Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Розробка локальної комп’ютерної мережі для КНП «Гусятинська комунальна лікарня» Гусятинської селищної ради.

Виконав: студент IV курсу, групи СНс-41
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Романюк М.Д.
(підпис) (прізвище та ініціали)

Керівник _____ Марценко С. В
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Липак Г. І.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ Стадник Н. Б.
(підпис) (прізвище та ініціали)

Тернопіль
2026

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«_8_» _червня_ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

Студенту Романюку Михайлу Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка локальної комп'ютерної мережі для КНП «Гусятинська комунальна лікарня» Гусятинської селищної ради.

Керівник роботи Марценко Сергій Володимирович, к.т.н., доц., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*14*» *травня* 20*26* року № *4/9-237*

2. Термін подання студентом завершеної роботи 22 червня 2026 р.

3. Вихідні дані до роботи Технічне завдання на розробку локальної комп'ютерної мережі для КНП «Гусятинська комунальна лікарня» Гусятинської селищної ради.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз використання локальних комп'ютерних мереж в медичні галузі 2. розробка проєкту локальної комп'ютерної мережі для КНП «Гусятинська КЛ» 3. Практична реалізація та віртуальне моделювання корпоративної мережі КНП «Гусятинська КЛ» 4. Безпека життєдіяльності, основи охорони праці. Висновки. Перелік джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема, мета та актуальність роботи. 2. Об'єкт проєктування та аналіз медичної галузі. 3. Структурована кабельна система та фізичне планування. 4. Сегментація мережі та розрахунок IP-адрес VLSM. 5 Обґрунтування вибору мережевого обладнання Cisco. 6. Логічна схема та налаштування безпеки мережі. 7. Віртуальне моделювання та тестування інфраструктури. 8. Висновки та практичне значення результатів.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці		01.06.2026	08.06.2026

7. Дата видачі завдання 26 січня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	26.01.2026	
2.	Підбір та опрацювання літературних джерел по темі кваліфікаційної роботи	27.01.2026-16.02.2026	
3.	Виконання дослідження щодо розробки локальної	17.02.2026-10.05.2026	
	комп'ютерної мережі для КНП "Гусятинська КЛ"»		
4.	Оформлення розділу Аналіз використання	11.05.2026-17.05.2026	
	локальних комп'ютерних мереж в медичні галузі		
5.	Оформлення розділу «розробка проєкту локальної	18.05.2026-24.05.2026	
	комп'ютерної мережі для КНП "Гусятинська КЛ"»		
6.	Оформлення розділу «Практична реалізація та	25.05.2026-31.05.2026	
	віртуальне моделювання корпоративної мережі КНП		
	"Гусятинська КЛ"»		
7.	Виконання завдання до підрозділу «Безпека життєдіяльності»	01.06.2026-08.06.2026	
8.	Виконання завдання до підрозділу «Основи охорони	01.06.2026-08.06.2026	
	праці»		
9.	Оформлення кваліфікаційної роботи	09.06.2026-11.06.2026	
10.	Нормоконтроль	12.06.2026-15.06.2026	
11.	Перевірка на плагіат	16.06.2026	
12.	Попередній захист кваліфікаційної роботи	18.06.2026	
13.	Захист кваліфікаційної роботи	28.06.2026	

Студент _____ Романюк М.Д
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценко С. В
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка локальної комп'ютерної мережі для КНП «Гусятинська комунальна лікарня» Гусятинської селищної ради. // Кваліфікаційна робота освітнього ступеня «Бакалавр» // Романюк Михайло Дмитрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНс-41 // Тернопіль, 2026 // С. 69 , рис. – 17 , табл. – 6 , кресл. – 8 , додат. – , бібліогр. – 35 .

Ключові слова: локальна комп'ютерна мережа, адреси, комутатор, маршрутизатор, топологія.

Кваліфікаційна робота присвячена дослідженню та розробці надійної і захищеної локальної мережі КНП «Гусятинська КЛ».

В першому розділі кваліфікаційної роботи описано вимоги до мережі КНП «Гусятинська КЛ». Висвітлено сучасні IT-тренди в медицині. Розглянуто топології та методи кібербезпеки. Проаналізовано методологію розробки Cisco PPDIOO.

В другому розділі кваліфікаційної роботи розроблено проєкт мережі. Досліджено інфраструктурні рішення. Подано фізичну топологію, план СКС, сегментацію VLAN, розрахунок IP-адрес (VLSM) та вибір обладнання для КНП «Гусятинська КЛ».

В третьому розділі кваліфікаційної роботи описано віртуальне моделювання в Cisco Packet Tracer. Проаналізовано налаштування маршрутизації, бездротової мережі та політик безпеки (ACL, IPsec VPN). Проведено комплексне тестування інфраструктури КНП «Гусятинська КЛ».

Об'єкт дослідження: телекомунікаційна інфраструктура КНП «Гусятинська КЛ».

Предмет дослідження: технології, протоколи та обладнання для побудови локальної мережі КНП «Гусятинська комунальна лікарня».

ANNOTATION

Development of a Local Computer Network for the Municipal Non-Profit Enterprise “Husiatyn Clinical Hospital” of the Husiatyn Settlement Council // Qualification work of the educational level “Bachelor” // Romanyuk Mykhailo Dmytrovych // Ternopil Ivan Pulyu National Technical University, Computer and Information Systems and Software Engineering Faculty, Computer Sciences Department, group SNs-41 // Ternopil, 2026 // P. 69 , fig. – 17 , tabl. – 6 , chair. – 8 , annexes. – , references – 35 .

Keywords: local computer network, ip addressing, switch, router, network topology, cybersecurity, vlan segmentation.

The qualification work is dedicated to researching and developing a reliable and secure local area network for the “Husiatyn Clinical Hospital”.

The goal of the work is to design an optimized and secure telecommunication infrastructure for the medical enterprise.

The first section of the qualification paper considered the network requirements, modern medical IT trends, network topologies, cybersecurity methods, and the Cisco PPDIOO methodology.

In the second section of the qualification work, the network project is developed, presenting the physical topology, structured cabling system plan, VLAN segmentation, VLSM IP addressing, and equipment selection.

The third section describes virtual modeling in Cisco Packet Tracer, configuring routing, wireless networks, and security policies (ACL, IPsec VPN), followed by comprehensive network testing.

Object of research: telecommunication infrastructure of the “Husiatyn Clinical Hospital”.

Subject of research: technologies, protocols, and equipment for building the local area network of the hospital.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AAA (англ. Authentication, Authorization, and Accounting) – автентифікація, авторизація та облік дій користувачів.

ACL (англ. Access Control List) – список контролю доступу.

CME (англ. Call Manager Express) – вбудована система управління IP-телефонією від Cisco.

DHCP (англ. Dynamic Host Configuration Protocol) – протокол динамічного налаштування вузла.

IP (англ. Internet Protocol) – міжмережевий протокол.

IPsec (англ. Internet Protocol Security) – набір протоколів для забезпечення безпеки передачі даних IP-мережею.

ISP (англ. Internet Service Provider) – постачальник інтернет-послуг (провайдер).

MAC (англ. Media Access Control) – унікальний ідентифікатор мережевого обладнання (управління доступом до середовища).

NAT (англ. Network Address Translation) – трансляція (перетворення) мережевих адрес.

NPS (англ. Network Policy Server) – сервер мережевих політик.

NVR (англ. Network Video Recorder) – мережевий відеореєстратор.

PAT (англ. Port Address Translation) – трансляція мережевих адрес на рівні портів.

PEAP (англ. Protected Extensible Authentication Protocol) – захищений протокол розширеної автентифікації.

PoE (англ. Power over Ethernet) – технологія передачі електричного живлення через кабель типу «вита пара».

PPDIOO (англ. Prepare, Plan, Design, Implement, Operate, Optimize) – багатокрокова методологія життєвого циклу мережі від компанії Cisco.

QoS (англ. Quality of Service) – технологія забезпечення якості обслуговування та пріоритезації трафіку.

RADIUS (англ. Remote Authentication Dial-In User Service) – протокол для реалізації централізованої автентифікації та авторизації.

SLA (англ. Service Level Agreement) – угода про рівень надання послуг (у контексті роботи – механізм Cisco IP SLA для моніторингу ліній).

SSID (англ. Service Set Identifier) – ідентифікатор (назва) бездротової мережі.

VLAN (англ. Virtual Local Area Network) – віртуальна локальна комп’ютерна мережа.

VLSM (англ. Variable Length Subnet Mask) – маска підмережі змінної довжини.

VPN (англ. Virtual Private Network) – віртуальна приватна мережа.

VTP (англ. VLAN Trunking Protocol) – протокол магістрального зв'язку для автоматизації налаштувань VLAN.

WLC (англ. Wireless LAN Controller) – апаратний контролер бездротової локальної мережі.

WPA2 (англ. Wi-Fi Protected Access 2) – протокол захищеного доступу до бездротових мереж.

ІТ – Інформаційні технології.

КЛ – Комунальна лікарня.

КНП – Комунальне некомерційне підприємство.

МІС – Медична інформаційна система.

СКС – Структурована кабельна система.

ЗМІСТ

ВСТУП

Актуальність теми. Внаслідок глобалізації цифрових процесів та активного реформування системи охорони здоров'я України, медична галузь переживає масштабну трансформацію, пов'язану з переходом до електронного документообігу (e-Health), масовим впровадженням хмарних медичних інформаційних систем (MIC) та розвитком телемедицини [1]. Операційне функціонування сучасного медичного закладу критично залежить від швидкості, стабільності та безпеки обміну даними. Генерація великих обсягів графічного трафіку (результати КТ, МРТ, цифрових рентгенограм), робота з електронними медичними картками (EHR) та функціонування чутливих до затримок сервісів (IP-телефонія) висувають жорсткі вимоги до телекомунікаційної інфраструктури. Окрім того, необхідність суворого дотримання лікарської таємниці та захисту персональних даних пацієнтів потребує впровадження комплексних засобів кібербезпеки [2]. Існуючі плоскі (flat) мережеві архітектури багатьох лікарень часто характеризуються низькою відмовостійкістю, наявністю великих широкомовних доменів та відсутністю резервування каналів зв'язку. Тому розробка проєкту та віртуальне моделювання сучасної, мультисервісної, відмовостійкої і захищеної локальної комп’ютерної мережі для медичних установ є актуальним напрямком сучасних досліджень в галузі комп'ютерних наук та телекомунікацій.

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Бакалавр» є підвищення якості надання медичних послуг, автоматизація внутрішніх процесів, забезпечення безперебійного доступу до хмарних платформ та підвищення рівня кібербезпеки інформаційного середовища установи шляхом проєктування і віртуального моделювання оптимальної телекомунікаційної інфраструктури для КНП «Гусятинська комунальна лікарня». Для досягнення поставленої мети потрібно виконати ряд завдань, зокрема:

– Проаналізувати сучасні інформаційні технології, IT-тренди у медичній галузі та особливості об'єкта проєктування для формування чітких технічних вимог до мережі.

– Дослідити теоретичні засади вибору мережевих топологій, методів кібербезпеки та системного підходу до управління життєвим циклем мережі за методологією Cisco PPDIOO [3].

– Проєктувати фізичну структуру та структуровану кабельну систему (СКС) лікарні відповідно до міжнародних галузевих стандартів TIA/EIA-568-B та ISO/IEC 11801.

– Розробить модель логічної сегментації мережі за допомогою віртуальних локальних мереж (VLAN) для надійної ізоляції робочих та гостьових потоків даних.

– Розрахувати оптимальний адресний простір методом масок змінної довжини (VLSM) для мінімізації втрат IP-адрес.

– Провести порівняльний аналіз інфраструктурних рішень, обґрунтувати вибір обладнання екосистеми Cisco та розробити структуру інтегрованої системи IP-телефонії.

– Створити віртуальну симуляційну модель спроєктованої мережі в середовищі Cisco Packet Tracer та реалізувати консольне налаштування базової комутації і маршрутизації (Inter-VLAN, NAT Overload).

– Впровадити комплекс політик безпеки канального та мережевого рівнів (Cisco Port Security, DHCP Snooping, розширені списки контролю доступу ACL) та налаштувати захищений віддалений доступ Remote Access IPsec VPN.

– Забезпечити високу відмовостійкість зовнішнього периметра шляхом налаштування схеми Dual-ISP з використанням механізмів Cisco IP SLA та Floating Static Route.

– Провести комплексне тестування кінцевих вузлів та верифікацію працездатності всієї змодельованої інфраструктури.

Практичне значення одержаних результатів. Практичне значення одержаних результатів полягає у створенні готового до практичного

впровадження технічного проєкту локальної комп’ютерної мережі для КНП «Гусятинська комунальна лікарня», що відповідає стандартам мультисервісності, безпеки та масштабованості. Розроблена в середовищі Cisco Packet Tracer симуляційна модель дозволяє наочно перевірити коректність конфігурації обладнання, оптимізувати маршрутизацію трафіку та верифікувати безпекові політики до початку реального монтажу, що мінімізує фінансові витрати та технічні ризики [4]. Створені інженерні скрипти налаштування пристроїв, схеми адресації VLSM, плани розподілу портів VLAN та архітектура безшовного бездротового роумінгу Wi-Fi Enterprise-рівня можуть бути безпосередньо використані під час модернізації телекомунікаційних систем КНП «Гусятинська КЛ».

РОЗДІЛ 1. АНАЛІЗ ВИКОРИСТАННЯ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ В МЕДИЧНІ ГАЛУЗІ

1.1 Аналіз сучасних інформаційних технологій та трендів у медичній галузі

На сучасному етапі розвитку світової системи охорони здоров'я спостерігається процес цифрової трансформації та глобального переходу від традиційного паперового документообігу до інтегрованих електронних рішень(e-Health) [5].

Гарантування операційного функціонування медичних закладів критично залежить від швидкості обміну даними, що робить автоматизацію ключових процесів обов'язковим стандартом для будь-якої установи. На основі аналізу загальних тенденцій цифровізації визначено, що впровадження новітніх технологій спрямоване на:

– прискорення міжлікарняної комунікації та координації медичних служб;

– оптимізацію збору, обробки та довготривалого зберігання конфіденційної інформації;

– мінімізацію людського фактора при веденні внутрішньої медичної документації.

Виходячи з цих міркувань, першочерговим інфраструктурним завданням для реалізації зазначених цілей є формування високонадійного телекомунікаційного середовища установи, спроможного витримувати сучасні операційні навантаження [6].

Розвиток світових технологій у медичній сфері також характеризується масовим впровадженням хмарних медичних інформаційних систем (МІС) на прикладі платформи Helsi або її аналогів. Ефективна інтеграція таких платформ потребує наявності постійного та відмовостійкого каналу зв'язку із

централізованими хмарними сховищами для запобігання втратам пакетів даних. Стабільне мережеве підключення є критично необхідним для гарантування таких повсякденних процесів:

– ведення та оновлення електронних медичних карток (EHR) пацієнтів;

– автоматизована генерація, верифікація та моніторинг використання електронних рецептів;

– цілодобове функціонування сервісів онлайн-запису громадян на прийом до спеціалістів.

Паралельно з хмаризацією процесів відбувається стрімке розширення сегмента телемедицини, що супроводжується впровадженням дистанційних консультацій та експлуатацією інноваційного цифрового діагностичного обладнання.

Особливістю цього етапу є генерація великих обсягів графічного трафіку, транспортування якого вимагає високої пропускної здатності комунікаційних ліній. Досліджено, що найбільше навантаження на внутрішню інфраструктуру закладу охорони здоров'я створюється під час передачі:

– високоякісних знімків комп'ютерної томографії (КТ);

– багатовимірних результатів магнітно-резонансної томографії (МРТ);

– цифрових рентгенограм та матеріалів ультразвукових досліджень.

Для усунення затримок при передачі таких даних та запобігання критичним колізіям, передбачено обов'язкове впровадження механізмів пріоритезації трафіку (QoS) та сегментації на віртуальні підмережі (VLAN) [7].

Таким чином, виявлені глобальні IT-тренди висувають вимоги до швидкодії, надійності та пропускної здатності телекомунікаційного середовища лікувального закладу. Будь-які перебої у роботі інфраструктури або зниження швидкості передачі даних призводять до повного блокування роботи медичного персоналу та унеможливлюють оперативне надання допомоги пацієнтам.

1.2 Дослідження об’єкта проєктування та формування вимог до комп’ютерної мережі

Досліджено архітектурні особливості будівлі КНП «Гусятинська КЛ», яка являє собою типову дворівневу або багатозонну споруду з чітким просторовим розподілом робочих місць. З метою оптимізації маршрутизації трафіку в межах проєктування та розробки локальної комп’ютерної мережі було детально розглянуто специфіку руху даних у таких ключових секторах:

– адміністративно-господарська частина, що включає адміністрацію та бухгалтерію закладу, які здійснюють постійну взаємодію з державними реєстрами та потребують підвищеного рівня захисту інформації;

– клінічна частина, що охоплює лікарняне відділення та кабінети прийому пацієнтів, персонал яких потребує стабільного та швидкого доступу до медичної інформаційної системи (МІС).

На основі аналізу технічного завдання було визначено, що першочерговим кроком для автоматизації внутрішніх процесів установи є проєктування сучасної телекомунікаційної інфраструктури. У зв'язку з цим, майбутня розробка локальної комп’ютерної мережі орієнтована на виконання таких стратегічних завдань:

– створення єдиного інформаційного простору для узгодженої взаємодії всіх підрозділів установи;

– гарантування централізованого доступу до державних реєстрів;

– автоматизація обміну даними між різними ланками медичного і керівного персоналу;

– підвищення загальної безпеки та надійності.

У сучасній інженерній практиці побудова лікарняних мереж базується на принципах мультисервісності, що дозволяє інтегрувати різнорідні цифрові сервіси в межах спільної транспортної платформи [9]. Для гарантування оперативної комунікації та підвищення рівня фізичної безпеки об'єкта автоматизації виявлено потребу в розгортанні додаткових інженерних

підсистем. Це передбачає обов'язкову інтеграцію та підтримку таких технологічних рішень:

– надійної IP-телефонії для організації оперативної взаємодії між персоналом;

– системи мережевого відеоспостереження (NVR) для гарантування безпеки всього медичного закладу;

– механізмів якості обслуговування (QoS) для пріоритезації чутливого до затримок голосового та відеотрафіку;

– технології Power over Ethernet (PoE) для централізованого живлення кінцевих пристроїв інженерних систем.

Функціонування критично важливих сервісів КНП «Гусятинська КЛ» потребує забезпечення високої щільності інформаційного обміну без ризику втрати пакетів даних чи виникнення затримок. Виходячи з цього, під час безпосереднього практичного моделювання, було закладено конкретні параметри, що відповідають таким експлуатаційним критеріям:

– гарантування безперервного режиму функціонування в режимі 24/7/365 завдяки дублюванню магістральних ліній;

– використання гігабітних каналів зв'язку (стандарт 1000Base-T) для підвищення пропускної здатності підсистеми;

– логічне сегментування трафіку різних підрозділів за допомогою віртуальних мереж (VLAN) для підвищення безпеки;

– гарантування високого потенціалу масштабованості для легкого підключення нового медичного обладнання чи додаткових робочих місць без перебудови структури всієї мережі.

Забезпечення інтеграції великої кількості різнотипних периферійних пристроїв та швидкої обробки великих обсягів даних вимагає формування чітких технічних вимог до комутаційного обладнання. Для досягнення мети модернізації традиційної інфраструктури та підвищення взаємодії мережевих елементів визначено такі технологічні стандарти:

– впровадження гігабітних портів (1000Base-T) на рівні доступу для забезпечення необхідної пропускної здатності каналів;

– використання технології PoE/PoE+ (Power over Ethernet) для дистанційного живлення кінцевих пристроїв по витій парі;

– виключення необхідності прокладання додаткових силових кабелів для підключення IP-телефонів, бездротових точок доступу Wi-Fi та камер цифрового відеоспостереження.

З метою практичної реалізації логічного та фізичного рівнів локальної обчислювальної мережі розроблено базові вимоги до апаратного забезпечення та заплановано використання керованих комутаторів із підтримкою зазначених стандартів швидкісної передачі та розподілу живлення [10].

1.3 Теоретичний вибір мережевої топології та принципів побудови локальних мереж

Конфігурація фізичних зв'язків між вузлами базується на використанні базових архітектурних рішень, які визначають швидкість та надійність передачі даних. Для формування оптимальної структури комунікаційного середовища об'єкта було розглянуто такі фізичні топології:

– «Шина», передбачає підключення всіх робочих станцій до єдиного загального коаксіального каналу зв'язку;

– «Кільце», характеризується послідовним з'єднанням мережевих пристроїв у замкнений контур із маркерним принципом передачі даних;

– «Зірка», базується на радіальному підключенні всіх кінцевих абонентських вузлів до центрального комутаційного пристрою;

– «Повнозв’язна (деревоподібна)», забезпечує максимальну надлишковість каналів зв'язку шляхом безпосереднього з'єднання кожного елемента системи з усіма іншими [11].

З метою оптимізації структурних параметрів телекомунікаційної інфраструктури об'єкта автоматизації здійснено оцінювання зазначених конфігурацій.

При проєктуванні сучасних інформаційних систем для підприємств критичної інфраструктури, зокрема медичних закладів, першочергове значення має забезпечення високого рівня живучості та безперебійності функціонування систем. Проведення критичного аналізу технічних характеристик дозволило виявити невідповідність застарілих архітектурних рішень сучасним безпековим стандартам галузі. У результаті дослідження визначено такі основні недоліки топологій типу «шина» та «кільце»:

– низька відмовоустійкість, за якої пошкодження або обрив хоча б одного сегмента фізичного кабелю призводить до повної паралізації інформаційного обміну всієї установи;

– висока складність і тривалість інженерних процесів локалізації та пошуку точного місця виникнення несправності;

– обмеженість можливостей щодо масштабування та модернізації без зупинки роботи всієї мережі.

Виходячи з цього, для забезпечення стабільного функціонування медичної установи використання топологій «шина» та «кільце» було повністю відкинуто.

Тенденції розвитку мережевих технологій спрямовані на впровадження структур, які мінімізують вплив одиничних точок відмови на загальний стан системи та спрощують управління ресурсами. На основі аналізу та порівняння параметрів встановлено, що оптимальним рішенням для забезпечення безперебійного сервісу є використання топології «Зірка» або її модифікації у вигляді ієрархічної розширеної зірки [12]. Переваги впровадження даної конфігурації полягають у:

– ефективній локалізації несправностей, оскільки виникнення проблеми з окремим лінійним кабелем не впливає на працездатність інших користувачів;

– простоті здійснення централізованого адміністрування, обслуговування та моніторингу мережевого трафіку;

– високій гнучкості та адаптивності до розширення структури шляхом додавання нових абонентських вузлів.

Керуючись цими проєктними принципами, для реалізації проєктованої мережевої інфраструктури медичного об'єкта було обрано та теоретично обґрунтовано схему ієрархічної розширеної зірки.

1.4 Аналіз методів забезпечення кібербезпеки та ізоляції конфіденційних даних

Забезпечення кібербезпеки у медичних установах є критично важливим завданням через необхідність жорсткого дотримання законодавчих вимог щодо захисту персональних даних та гарантування лікарської таємниці. Виходячи з аналізу специфіки функціонування медичних об'єктів, вимоги до захисту інформації призначені для:

– безумовного гарантування конфіденційності медичних карток та облікових записів пацієнтів;

– унеможливлення витоків фінансової, господарської та клінічної інформації;

– запобігання атакам програм-шифрувальників, що можуть повністю заблокувати процеси надання невідкладної медичної допомоги [8].

Захист медичних даних потребує впровадження комплексних технічних рішень на рівні всієї мережевої інфраструктури об'єкта.

На сучасному етапі розвитку мережевих технологій для ізоляції конфіденційних потоків даних застосовується концепція логічного розподілу середовища передачі. Технологія віртуальних локальних мереж (VLAN) дозволяє розділити єдину фізичну інфраструктуру на кілька незалежних логічних зон без необхідності прокладання додаткових кабельних ліній. Для

гарантування безпеки проєктованого об'єкта було визначено необхідність створення таких ізольованих сегментів:

– VLAN гостьової мережі Wi-Fi для відвідувачів та пацієнтів;

– VLAN адміністративно-господарського сектору та бухгалтерії;

– VLAN медичної інформаційної системи (МІС) та серверних баз даних.

Шляхом такого логічного розподілу повністю виключається можливість несанкціонованого доступу користувачів із публічної чи гостьової зони до критично важливих комп'ютерів та інформаційних ресурсів установи [13].

Поряд із логічною сегментацією, критично важливим етапом є регламентація міжмережевої взаємодії та захист фізичного периметра підключень. Для контролю руху трафіку між створеними логічними зонами використовуються списки контролю доступу (ACL). Окрім контролю на мережевому рівні, захист безпосередніх точок доступу та роз'ємів обладнання забезпечується через:

– активацію функції захисту портів комутаторів (Port Security);

– жорстке обмеження кількості дозволених MAC-адрес на кожному фізичному порті;

– автоматичне деактивування порту при спробі підключення стороннього несанкціонованого пристрою;

– впровадження технології DHCP Snooping для формування ешелонованого захисту та протидії атакам типу підміни ідентифікаторів (MAC Spoofing).

Впровадженням цих засобів досягається повне обмеження нелегітимних переміщень трафіку всередині периметра медичного закладу.

На завершення побудови захищеної інфраструктури постає завдання організації безпечного дистанційного керування та адміністрування мережі. Створення віддаленого доступу для обслуговування систем здійснюється із використанням технології VPN (Virtual Private Network), що дозволяє організувати захищені шифровані тунелі через публічний Інтернет. Використання зазначеного підходу забезпечує:

– надійне криптографічне шифрування управлінського трафіку для запобігання перехопленню даних;

– строгу автентифікацію системного адміністратора при підключенні до внутрішніх ресурсів;

– повну ізоляцію сесії віддаленого доступу від загальних публічних каналів зв'язку.

Таким чином, на основі проведеного аналізу було обрано та реалізовано схему захищеного віддаленого доступу, яка гарантує стабільне та безпечне функціонування всієї інформаційної інфраструктури об'єкта [14].

1.5 Життєвий цикл розробки мережі

Використання стандартизованих інженерних концепцій проєктування дозволяє оптимізувати капітальні витрати, мінімізувати технічні ризики та забезпечити безперервність бізнес-процесів організації на всіх етапах функціонування системи. З огляду на це, у роботі було систематизовано та застосовано базову методологію Cisco PPDIOO, життєвий цикл якої трансформовано у такий перелік послідовних фаз:

– Prepare (Підготовка): здійснюється аналіз загальних бізнес-вимог, визначення стратегії розвитку архітектури, оцінювання фінансових можливостей та попереднє окреслення технологічних потреб замовника;

– Plan (Планування): проводиться комплексний аудит та дослідження існуючої інфраструктури, оцінка відповідності поточного середовища новим вимогам, визначення потенційних проблемних ділянок та формування базового плану керування проєктом;

– Design (Проєктування): розробляється детальна архітектурна та технічна специфікація мережі, що включає логічну й фізичну топології, детальні схеми IP-адресації, вибір апаратного гарантування та політики інформаційної безпеки;

– Implement (Впровадження): виконується безпосередній монтаж телекомунікаційного обладнання, конфігурування мережевих пристроїв згідно з проєктом, інтеграція нових компонентів у наявне середовище та проведення пусконалагоджувальних робіт;

– Operate (Експлуатація): забезпечується щоденний моніторинг функціонування мережі, оперативне управління інцидентами, резервне копіювання конфігурацій та підтримання заданого рівня доступності сервісів;

– Optimize (Оптимізація): здійснюється проактивне виявлення вузьких місць архітектури, модернізація налаштувань, усунення систематичних технічних помилок та планування подальшого масштабування системи до моменту їх критичного впливу на роботу установи [15].

Ефективна реалізація проєкту модернізації телекомунікаційної інфраструктури об'єкта автоматизації потребує високої чіткості формулювання технічного завдання та максимальної глибини попереднього збору вихідних даних. Згідно з методологічними положеннями концепції PPDIOO, первинне збирання інформації, аудит існуючого інженерного середовища та формалізація вимог дозволяють повністю усунути ризики проєктування неоптимальної топології на наступних етапах.

1.6 Висновок до першого розділу

В першому розділі роботи здійснено аналіз предметної області та технологій побудови мережі медичного закладу, який підтвердив необхідність впровадження новітніх інформаційних рішень для автоматизації процесів та гарантування швидкого обміну даними. На основі дослідження потреб щодо безперебійного доступу до хмарних платформ і електронних медичних карток (EHR), було сформовано технічні вимоги до мультисервісної комп'ютерної мережі КНП «Гусятинська КЛ». Ці вимоги передбачають інтеграцію IP-телефонії та систем відеоспостереження, використання гігабітних каналів зв'язку і технології дистанційного живлення PoE. Для забезпечення

максимальної відмовостійкості, ефективної локалізації несправностей та гнучкості інфраструктури теоретично обґрунтовано вибір мережевої топології ієрархічної розширеної зірки. Разом з тим, для захисту конфіденційної інформації визначено потребу впровадження комплексних заходів кібербезпеки: логічної сегментації середовища за допомогою VLAN, використання списків контролю доступу (ACL), захисту фізичних портів та організації віддаленого доступу через VPN-канали. Підсумовуючи, доведено доцільність використання стандартизованої методології життєвого циклу Cisco PPDIOO для системного проєктування, що дозволяє оптимізувати капітальні витрати та мінімізувати технічні ризики на всіх етапах розгортання мережі.

РОЗДІЛ 2. РОЗРОБКА ПРОЄКТУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ КНП «ГУСЯТИНСЬКА КЛ»

2.1 Проєктування фізичної топології та структурованої кабельної системи для КНП «Гусятинська КЛ»

Розробка локальної комп'ютерної мережі для КНП «Гусятинська КЛ» потребує впровадження надійної ієрархічної архітектури, оскільки застаріла плоска (flat) мережа є неефективною для потреб сучасного медичного закладу через неможливість гнучкого сегментування трафіку, наявність великих широкомовних доменів та відсутність резервування. Для вирішення цих проблем у межах технічного завдання для КНП «Гусятинська КЛ» було обрано дворівневу ієрархічну модель, що включає рівень згорнутого ядра (Collapsed Core) та рівень доступу (Access). Впровадження моделі зі згорнутим ядром дозволило об'єднати функції маршрутизації та розподілу політик в одному логічному вузлі, що забезпечує високу продуктивність, надійну ізоляцію підмереж та оптимізацію витрат на активне мережеве обладнання лікарні [16].

Логічна топологія побудована за принципом «Зірка», де кожний кінцевий пристрій КНП «Гусятинська КЛ» має виділене підключення до комутатора доступу. Таке рішення гарантує локалізацію можливих збоїв, при якій пошкодження кабельної лінії конкретного робочого місця медичного персоналу не призводить до зупинки функціонування всього відділення.

Проєктування структурованої кабельної системи (СКС) для КНП «Гусятинська КЛ» виконано з суворим дотриманням міжнародних галузевих стандартів TIA/EIA-568-B та ISO/IEC 11801. Основні вимоги до кабельної інфраструктури, що були враховані під час проєктування, включають:

– використання волоконно-оптичного кабелю для магістральних каналів між поверхами з метою забезпечення максимальної пропускної здатності та захисту від електромагнітних завад;

– застосування мідного кабелю типу «вита пара» категорії 6 (Cat6) для горизонтальної розводки, що дозволяє підтримувати гігабітні швидкості передачі даних на робочих місцях КНП «Гусятинська КЛ»;

– обов’язкове використання кабелів з негорючою оболонкою LSZH (Low Smoke Zero Halogen), що відповідає суворим вимогам пожежної безпеки медичного закладу [17].

Для систематизації технічних параметрів обладнання, що використовується при побудові СКС для КНП «Гусятинська КЛ», було складено перелік, поданий у таблиці 2.1.

Таблиця 2.1 – Основні параметри кабельної системи та обладнання для КНП «Гусятинська КЛ»

Тип обладнання / лінії	**Технологія / Стандарт**	**Призначення**
Магістраль	Волокно (Fiber)	Зв’язок між поверхами
Горизонтальна розводка	Cat6 (UTP)	Робочі місця, БФП
Активне обладнання	PoE+	IP-телефони, Wi-Fi

Як видно з поданої таблиці, вибір стандартів та технологій дозволяє забезпечити повноцінне функціонування інформаційної інфраструктури. Прокладання кабельних трас здійснюється з використанням металевих та пластикових кабельних лотків із чітким дотриманням нормативного відступу від силових ліній електропередач: паралельне прокладання здійснюється на відстані не менше 200 мм, а перетин трас — виключно під кутом 90 градусів. Усі кабельні лінії підлягають обов'язковому двосторонньому маркуванню стандартом TIA/EIA-606, що спрощує експлуатацію та адміністрування системи персоналом лікарні.

Розміщення кабельних трас та мережевого обладнання на першому поверсі КНП «Гусятинська КЛ», та де розташовано центральний вузол (телекомунікаційна шафа з маршрутизатором, комутатором ядра та ДБЖ), представлено на рисунку 2.1.

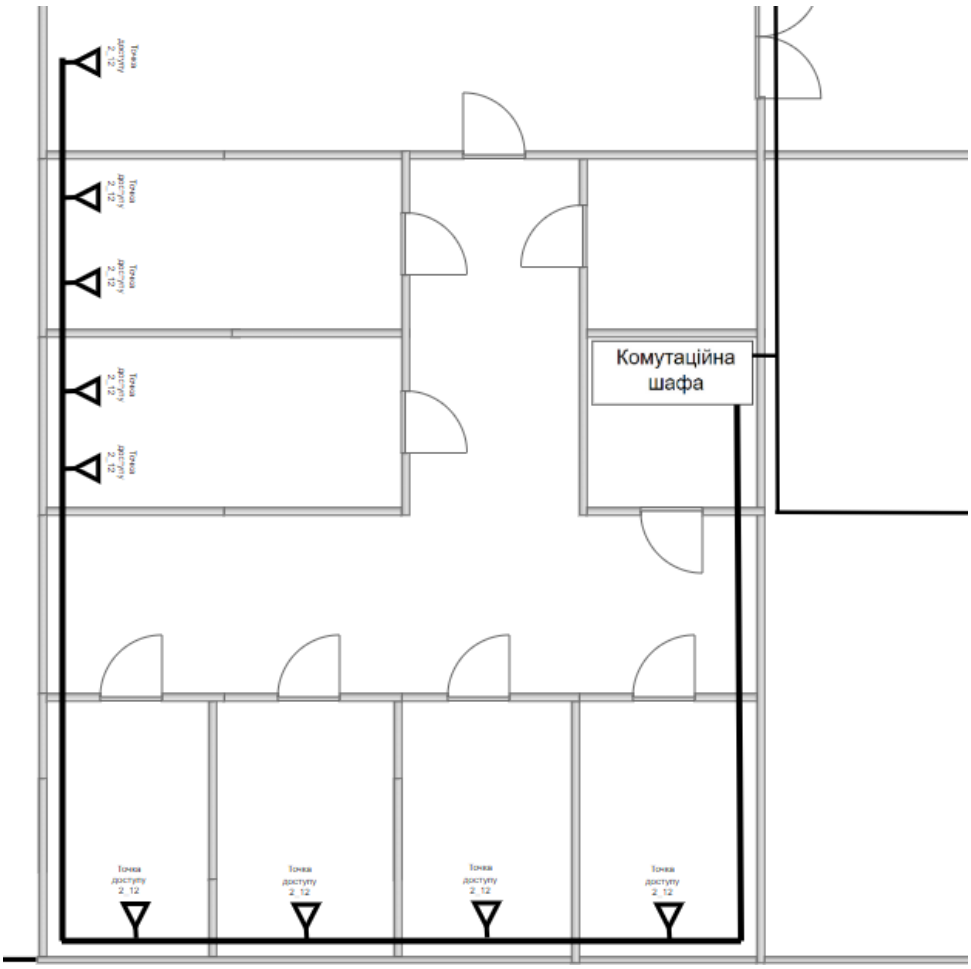

Рисунок 2.1 – Схема розташування кабель-каналів та мережевого обладнання на першому поверсі КНП «Гусятинська КЛ»

Як видно з поданого рисунка, розміщення центрального вузла в окремому приміщенні забезпечує фізичну безпеку та обмежений доступ до критичної інфраструктури лікарні. Топологія прокладання кабельних трас, зображена на схемі, демонструє оптимальне відгалуження магістралей до окремих кабінетів, що дозволяє раціонально використовувати ресурси кабельної системи та мінімізувати перешкоди. Прокладання здійснюється з використанням кабельних лотків із чітким дотриманням нормативного відступу від силових ліній електропередач, що гарантує цілісність сигналу в умовах медичного закладу.

Аналогічно, для другого поверху КНП «Гусятинська КЛ» було розроблено план розміщення комутатора рівня доступу (свіча), який забезпечує агрегацію даних та живлення кінцевих пристроїв, що подано на рисунку 2.2.

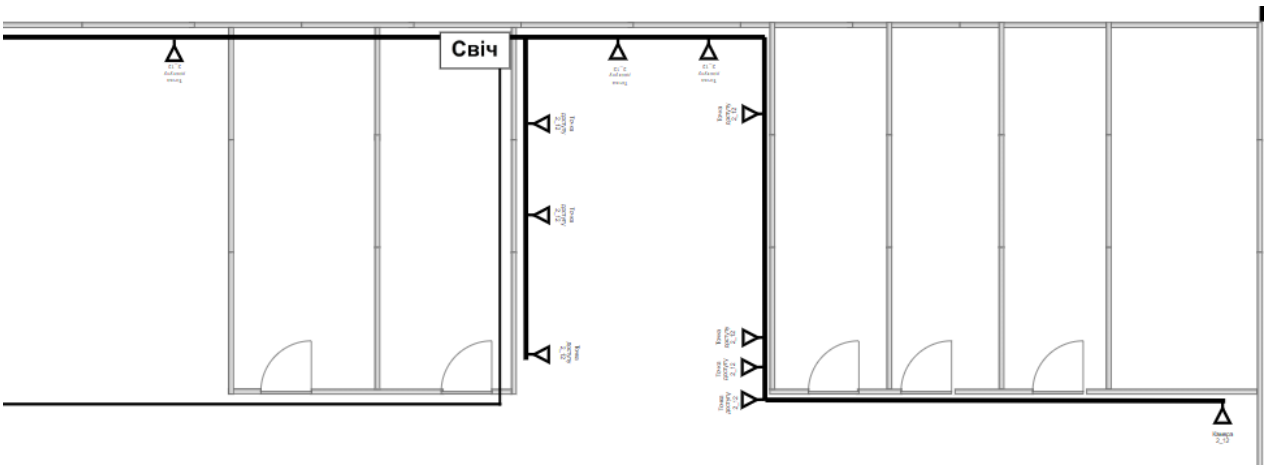

Рисунок 2.2 – Схема розташування кабель-каналів та мережевого обладнання на другому поверсі КНП «Гусятинська КЛ»

Як видно з поданого матеріалу, топологія мережі на другому поверсі передбачає чіткий розподіл активного та пасивного обладнання, що дозволяє масштабувати мережу за потреби.

Використання поверхового комутатора дозволяє ефективно інтегрувати всі робочі місця в єдину інформаційну мережу КНП «Гусятинська КЛ» без додаткових джерел живлення, що повністю відповідає технічним вимогам до сучасної медичної IT-інфраструктури.

Для спрощення подальшої експлуатації та адміністрування всі кабельні лінії, схематично зображені на рисунках 2.1 та 2.2, підлягають обов’язковому двосторонньому маркуванню.

2.2 Сегментація мережі та керування VLAN для КНП «Гусятинська КЛ»

Для мінімізації ризиків несанкціонованого доступу до конфіденційної інформації та забезпечення стабільної роботи критично важливих сервісів у межах функціонування КНП «Гусятинська КЛ» необхідно чітко розмежувати робочий трафік персоналу та гостьовий доступ. Особлива увага при розробці локальної комп’ютерної мережі приділяється захисту персональних медичних

даних, що обробляються через хмарну MIC Helsi, а також безпеці комерційної інформації підприємства, доступ до якої обмежений для бухгалтерії та керівництва [18]. Відповідно до поставлених вимог безпеки при розробці локальної комп'ютерної мережі для КНП «Гусятинська КЛ» було виділено такі віртуальні мережі:

– VLAN 10 (Адміністрація);
– VLAN 20 (Бухгалтерія);
– VLAN 30 (Медичний персонал);
– VLAN 40 (IP-відеокамери);
– VLAN 50 (Гостьова мережа);
– VLAN 60 (Сервери)
– VLAN 70 (IP-телефонія);
– VLAN 99 (Управління бездротовим обладнанням).
– VLAN 100 (Мережевий Адмін)

З метою забезпечення цілісності конфігурацій та автоматизації процесів синхронізації бази даних віртуальних мереж між комутаторами у застосовується протокол VLAN Trunking Protocol (VTP). Використання даного протоколу зумовлене необхідністю уникнення ручного налаштування параметрів VLAN на кожному комутаторі доступу, що дозволяє суттєво мінімізувати вплив людського фактора та ймовірність виникнення помилок під час адміністрування інфраструктури, тому було реалізовано централізовану модель керування базами даних VLAN [19].

У процесі впровадження розробки локальної комп'ютерної мережі для КНП «Гусятинська КЛ», головний комутатор рівня агрегації (ядра) буде переведено в режим VTP Server, що дозволить здійснювати авторизоване створення, видалення та модифікацію віртуальних мереж.

У свою чергу, комутатори доступу, розміщені на поверхах, налаштовані в режим VTP Client, завдяки чому забезпечується автоматичне отримання та оновлення бази VLAN через транкові (Trunk) з'єднання.

Для забезпечення ефективної маршрутизації та логічної ізоляції сегментів було виділено єдиний приватний блок IP-адрес 192.168.1.0/24. Використання класичного поділу на рівні підмережі з фіксованою маскою призвело б до неефективного використання адресного простору та його значного марнотратства, оскільки реальна кількість хостів у підрозділах лікарні суттєво відрізняється. З цих міркувань при розробці локальної комп'ютерної мережі для КНП «Гусятинська КЛ» було застосовано метод масок змінної довжини (Variable Length Subnet Mask, VLSM) [20].

Процес впровадження методу VLSM при проєктуванні інфраструктури базується на таких ключових принципах:

– мінімізація втрат адресного простору в умовах обмеженого діапазону;

– відповідність обсягу підмережі фактичній кількості хостів у відділеннях лікарні;

– ієрархічний розподіл сегментів від найбільшого (адміністративний та медичний персонал) до найменшого (мережі управління та технічні засоби).

З огляду на те, що формування адресного плану здійснюється автоматично за допомогою спеціалізованого програмного забезпечення, необхідність у ручному обчисленні параметрів кожного сегмента відсутня.

Результати розрахунку адресного простору за методом VLSM, необхідні для успішної реалізації розробки локальної комп'ютерної мережі КНП «Гусятинська КЛ», зведено у таблицю 2.2.

Таблиця 2.2 – Розрахунок адресного простору за методом VLSM

Назва підмережі (VLAN)	**Розрахункова кількість хостів**	**Адреса підмережі**	**Маска**	**Діапазон корисних адрес**
1	**2**	**3**	**4**	**5**
VLAN 50 (Гості)	50	192.168.1.0	/26	192.168.1.1 – 192.168.1.62

1	2	3	4	5
VLAN 30 (Медики)	50	192.168.1.64	/26	192.168.1.65 – 192.168.1.126
VLAN 20 (Бухгалтерія)	25	192.168.1.128	/27	192.168.1.129 – 192.168.1.158
VLAN 10 (Адміністрація)	25	192.168.1.160	/27	192.168.1.161 – 192.168.1.190
VLAN 70 (Voice / IP-Телефони)	10	192.168.1.192	/28	192.168.1.193 – 192.168.1.206
VLAN 40 (Камери спостереження)	5	192.168.1.208	/29	192.168.1.209 – 192.168.1.214
VLAN 99 (Wireless)	5	192.168.1.216	/29	192.168.1.217 – 192.168.1.222
VLAN 60 (Сервери)	10	192.168.1.224	/28	192.168.1.225 – 192.168.1.238
VLAN 100 (Мережевий Адмін)	2	192.168.1.240	/29	192.168.1.241 – 192.168.1.246
Резервний блок		192.168.1.248	/29	192.168.1.249 – 192.168.1.254

Як видно з поданої таблиці, розподіл адресного простору дозволяє забезпечити необхідну кількість вузлів для кожного сегмента мережі із мінімальним запасом, що відповідає вимогам до масштабованості та оптимізації при розробці локальної комп’ютерної мережі медичної установи КНП «Гусятинська КЛ».

2.3 Порівняльний аналіз інфраструктурних рішень та вибір обладнання для КНП «Гусятинська КЛ»

Для забезпечення безперебійної роботи інформаційних систем КНП «Гусятинська КЛ», підвищення обслуговування пацієнтів та захисту конфіденційних медичних даних, було проведено порівняльний аналіз інфраструктурних рішень. Перший варіант (рішення 1) передбачає створення екосистеми на основі обладнання Cisco, тоді як другий варіант (рішення 2) базується на гетерогенній структурі, що включає пристрої різних виробників. Результати технічного та функціонального зіставлення вказаних підходів систематизовано у таблиці 2.3.

Таблиця 2.3 – Порівняльний аналіз інфраструктурних рішень

Критерій оцінки	**Рішення 1 (Cisco)**	**Рішення 2 (гетерогенна мережа)**
Апаратна база	Маршрутизатор Cisco ISR 2911, комутатори Catalyst 2960-X / 2960-C	Маршрутизатор MikroTik RB4011, комутатори TP-Link JetStream
Централізація управління	Висока (єдина операційна система Cisco IOS)	Низька (різні інтерфейси: RouterOS, Web-CLI TP-Link)
Організація IP-телефонії	Вбудована платформа (Cisco Call Manager Express)	Потребує окремої апаратної АТС
Потреба у серверах	Не вимагається	Обов'язкова (для телефонії)
Підтримка мережевих протоколів	Повна підтримка пропрієтарних стандартів (VTP, PVST+)	Використання виключно відкритих стандартів

Як свідчать дані з таблиці 2.1, два представлені варіанти інфраструктурних рішень для КНП «Гусятинська КЛ» відрізняються за архітектурою та принципами адміністрування.

Рішення на базі обладнання Cisco, підтримує пропрієтарні протоколи (VTP, PVST+) та характеризується високим ступенем централізації завдяки використанню єдиної операційної системи Cisco IOS. Окрім того, організація IP-телефонії в цьому варіанті базується на вбудованій платформі, що не вимагає встановлення додаткових серверів [21].

Натомість гетерогенна мережа (на базі MikroTik та TP-Link) використовує відкриті мережеві стандарти, а її адміністрування передбачає роботу з різними інтерфейсами (RouterOS, Web-CLI). Для організації IP-телефонії у цьому варіанті необхідне розгортання окремої апаратної АТС.

Зважаючи на результати порівняння, для практичного впровадження обрано першу концепцію, оскільки реалізація розробки локальної комп’ютерної мережі на базі екосистеми Cisco забезпечує оптимізацію витрат та технічну досконаліть інфраструктури. Ключовим фактором цього вибору є інтегрована платформа Cisco Call Manager Express, розгорнута на маршрутизаторі ISR 2911, що дозволяє усунути потребу у закупівлі та підтримці окремої апаратної АТС. Переваги обраного підходу до розробки локальної комп’ютерної мережі для даного закладу включають:

– інтеграція сервісів IP-телефонії безпосередньо на рівні маршрутизації для забезпечення оперативного зв'язку між відділеннями;

– автоматизація процесів конфігурації та реплікації віртуальних мереж, що забезпечує стабільну роботу мережевої інфраструктури медичного закладу та мінімізує час простою сервісів [21].

Виходячи з цього, здійснена розробка локальної комп’ютерної мережі базується на концепції Cisco, що мінімізує експлуатаційні ризики та забезпечує гнучкість при подальшому масштабуванні інфраструктури КНП «Гусятинська КЛ».

Архітектура мережі доповнюється спеціалізованими інфраструктурними та периферійними пристроями.

Фундаментом безпеки та зберігання даних виступає серверна інфраструктура. До неї належить виділений Windows Server (NPS), який виконує функції AAA/RADIUS-сервера для автентифікації персоналу (за стандартом 802.1X) та слугує джерелом точного часу (NTP).

Для розгортання бездротової мережі використовується апаратний контролер Cisco WLC 2504. Він забезпечує централізоване управління чотирма точками доступу.

Для організації голосового зв'язку обрано IP-телефони Cisco 7960, робота яких керується вбудованою в маршрутизатор системою Cisco Call Manager Express (CME).

Окремим апаратним вузлом є мережевий відеореєстратор (NVR Dahua), призначений для централізованого збору та збереження відеопотоків із камер спостереження. Візуальний контроль приміщень забезпечується чотирма IP-камерами, які ізолюються в окремому сегменті мережі.

Для забезпечення автоматизованої адресації кінцевих вузлів у межах проєктування локальної комп’ютерної мережі КНП «Гусятинська КЛ» було обрано стратегію використання централізованого DHCP-сервера. З огляду на необхідність мінімізації витрат на підтримку окремого серверного обладнання та забезпечення високої доступності сервісів у медичному закладі, функцію надання IP-адрес покладено на головний маршрутизатор Cisco ISR 2911. Таке рішення дозволяє оптимізувати архітектуру та зменшити навантаження на інфраструктуру.

Динамічний розподіл адрес організовано за принципом логічної сегментації: для кожного віртуального сегмента (VLAN) створено окремий DHCP пул, прив’язаний до відповідного підінтерфейсу маршрутизатора.

При цьому конфігурація кожного пулу містить обов’язкові мережеві параметри, необхідні для стабільної роботи інформаційної системи лікарні:

– діапазон доступних IP-адрес, розрахований за методом VLSM;

– адреса шлюзу за замовчуванням (Default Gateway), що відповідає IP-адресі сабінтерфейсу;

– адреса сервера доменних імен (DNS) [23].

З метою уникнення конфліктів IP-адрес було реалізовано механізм виключення певних діапазонів із динамічного розподілу (команда ip dhcp excluded-address). Перелік інфраструктурного обладнання, що потребує стабільної статичної адресації та вилучається з пулів DHCP, наведено в таблиці 2.4.

Таблиця 2.4 – Перелік зарезервованих IP-адрес у мережі КНП «Гусятинська КЛ»

Тип пристрою	**Статус адресації**	**Шлюз (Subinterface)**	**Діапазон зарезервованих адрес**
Керовані комутатори мережі	Статична	192.168.1.241 (VLAN 100)	192.168.1.243 – 192.168.1.245
Контролер WLC та точки доступу Wi-Fi	Статична	192.168.1.217 (VLAN 99)	192.168.1.221 – 192.168.1.222
Мережевий (NVR) та IP-камери	Статична	192.168.1.209 (VLAN 40)	192.168.1.210 – 192.168.1.214
Сервер автентифікації (AAA/RADIUS)	Статична	192.168.1.225 (VLAN 60)	192.168.1.226 – 192.168.1.238
Робочі станції адміністрування	Статична	192.168.1.241 (VLAN 100)	192.168.1.242 – 192.168.1.246

Виключення цих діапазонів із пулів DHCP забезпечує стабільність роботи критично важливого інфраструктурного обладнання та систем відеоспостереження, виключаючи ризик збоїв через зміну IP-адрес.

2.4 Налаштування маршрутизації, безпеки трафіку та віддаленого доступу в КНП «Гусятинська КЛ»

У процесі проєктування було враховано, що внутрішня мережа КНП «Гусятинська КЛ» розрахована за методом VLSM з використанням приватного простору 192.168.1.0/24, через що прямий вихід в Інтернет для робочих станцій є неможливим у зв'язку з обмеженнями глобальної маршрутизації. З метою економії адресного простору та забезпечення прозорого виходу в зовнішнє середовище виникла необхідність трансляції множини внутрішніх IP-адрес в один пул з 5 або 6 публічних адресу активного провайдера. Для вирішення цієї проблеми на прикордонному пристрої Cisco ISR 2911 було успішно реалізовано механізм PAT (Port Address Translation або NAT Overload), завдяки чому забезпечується коректне функціонування та оптимальний розподів адресних просторів у поточній локальній комп’ютерноій мережі [24].

Взаємодія медичного персоналу КНП «Гусятинська КЛ» із віртуальної мережі VLAN 30 із хмарною медичною інформаційною системою Helsi потребує сувого дотримання політик безпеки периметра для запобігання потенційним зовнішнім загрозам. Застосований механізм PAT функціонує як базовий міжмережевий екран із контролем стану сесій, оскільки трансляція створюється динамічно лише для з'єднань, ініційованих зсередини периметра установи.

Завдяки такому підходу під час проєктування та розробки локальної комп’ютерної мережі було повністю заблоковано спроби несанкційонованого прямого підключення зловмисників до внутрішніх хостів лікарні, що гарантує цілісність конфіденційних даних пацієнтів.

Специфіка функціонування КНП «Гусятинська КЛ» вимагає цілодобового та безперервного доступу до хмари Helsi для оперативного внесення даних, тому раптове падіння одного каналу зв'язку не повинно зупиняти критично важливі процеси установи. Задля ліквідації ризиків повної втрати зв'язку в межах проєкту було обґрунтовано та впроваджено схему підключення будівлі лікарні до двох незалежних інтернет-провайдерів, де перший виступає як основний, а другий виконує роль резервного каналу через різні фізичні WAN-інтерфейси маршрутизатора. Дане рішення, інтегроване в загальну розробку локальної комп’ютерної мережі, дозволяє створити надійний фундамент для відмовостійкої інфраструктури закладу [25].

Для забезпечення автоматичного перемикання між каналами провайдерів без ручного втручання адміністратора виникла потреба в налаштуванні динамічної зміни маршрутів. Оптимальним інструментом для реалізації цієї інженерної логіки стало використання механізму Floating Static Route, де для основного провайдера задається статичний маршрут зі стандартною адміністративною відстанню, що дорівнює одиниці, а для резервного провайдера – аналогічний маршрут з вищою адміністративною відстанню, яка становить десять. Таким чином, резервний маршрут знаходиться в режимі очікування і автоматично інсталюється в таблицю маршрутизації лише у разі зникнення лінку на інтерфейсі основного провайдера.

Під час реалізації захисту на канальному рівні для КНП ”Гусятинська комунальна лікарня” виникає необхідність ефективної оптимізації топології та запобігання глобальним збоям, що становить базовий етап, на якому будується поточна розробка локальної комп’ютерної мережі. На відміну від стандартного протоколу RSTP, фірмовий протокол Cisco PVST+ (Per-VLAN Spanning Tree Plus) запускає окремий екземпляр (instance) безпетлевого дерева для кожного конкретного VLAN, що забезпечує балансування навантаження між магістральними зв'язками.

З метою забезпечення надійного захисту фізичних портів доступу на комутаторах від несанкціонованої зміни обладнання на робочих місцях

персоналу КНП «Гусятинська КЛ» було застосовано технологію Port Security. Суть методу Sticky MAC полягає в тому, що комутатор автоматично вивчає MAC-адресу першого підключеного пристрою, такого як ПК лікаря або IP-телефон, і динамічно «прив'язувати» її до конфігурації порту із збереженням в оперативній пам'яті. Виходячи з цього, на інтерфейсах доступу комутаторів лікарні було виконано повну активацію даного захисного режиму за допомогою введення відповідних інженерних команд конфігурації.

Для організації оперативного реагування на порушення встановленої політики безпеки в КНП «Гусятинська КЛ», у випадку якщо в порт доступу буде підключено сторонній апаратний засіб (наприклад, ноутбук пацієнта), передбачено автоматизоване блокування лінії зв'язку. При зафіксованій невідповідності зчитаної MAC-адреси комутатор негайно переводить інтерфейс у стан Error-Disable (режим shutdown), внаслідок чого передача пакетів даних повністю припиняється, а відновлення працездатності можливе лише вручну після втручання системного адміністратора через консоль управління.

З метою практичної реалізації концепції ешелонованого захисту (Defense in Depth) на комутаційному обладнанні доступу було впроваджено та скоординовано роботу технології Port Security. Для протидії складнішим векторам атак, зокрема підміні ідентифікаторів (MAC Spoofing) з метою обходу обмежень Port Security, додатково було налаштовано функціонал DHCP Snooping. Шляхом переведення користувацьких портів у статус недовірених (Untrusted) було повністю заблоковано можливість нелегітимної роздачі IP-адрес (пакети DHCP Offer) через випадково чи навмисно підключені сторонні роутери, що дозволило гарантувати цілісність адресного простору [26].

Для організації керованого обміну даними між логічно ізольованими сегментами мережі на третьому рівні моделі OSI було застосовано технологію Inter-VLAN Routing за архітектурним принципом Router-on-a-Stick. У межах цього рішення єдиний фізичний інтерфейс головного маршрутизатора, було розподілено на декілька логічних субінтерфейсів, кожен з яких виступає в ролі шлюзу за замовчуванням (Default Gateway) для конкретного VLAN. На

кожному з налаштованих субінтерфейсів було активовано інкапсуляцію трафіку за загальноприйнятим стандартом IEEE 802.1Q, що забезпечило чітке тегування кадрів, надійне розмежування широкомовних доменів та оптимізацію використання фізичних портів маршрутизатора.

Застосування розширених списків контролю доступу (Extended ACL) на інтерфейсах маршрутизатора забезпечує гнучке керування пакетами на основі адрес та портів призначення, повністю реалізуючи концепцію «найменших привілеїв», було здійснено налаштування правил фільтрації, структуру яких наведено в таблиці 2.5.

Таблиця 2.5 – Структура списків доступу КНП «Гусятинська КЛ»

Назва списку доступу	**Тип ACL**	**Точка застосування**	**Функціональне призначення**
1	Standard	Внутрішній процес роутера	Відбір трафіку мережі для трансляції NAT Overload
GUEST_SECURITY	Extended	GigabitEthernet0/0.50 (VLAN 50)	Ізоляція гостей від внутрішніх підмереж лікарні
CAMERA_SECURITY	Extended	GigabitEthernet0/0.40 (VLAN 40)	Обмеження доступу IP-камер лише до сервера NVR
INTERNAL_ISOLATION	Extended	Gi0/0.10, Gi0/0.20, Gi0/0.30	Захист серверної зони від звичайних користувачів

Таблиця містить інформацію про правила фільтрації, точки застосування та обмеження доступу між окремими технологічними зонами закладу. Як видно з поданого матеріалу, детальна логіка обмежень найсуворіше реалізується через розширений список доступу для гостьової мережі (VLAN 50) КНП «Гусятинська КЛ», де згідно з адресним планом вимагається ізоляція підмережі 192.168.1.0/26 від робочих ресурсів компанії. Для впровадження цієї політики безпеки на відповідному віртуальному субінтерфейсі маршрутизатора було активовано систему фільтрації, яка забезпечує покрокове виконання таких умов:

– суворе блокування будь-яких пакетів у напрямку підмережі медичних працівників (192.168.1.64/26);

– заборону передачі даних до службових сегментів бухгалтерії (192.168.1.128/27) та загальної адміністрації (192.168.1.160/27);

– повний дозвіл на маршрутизацію та подальшу динамічну трансляцію адрес (NAT/PAT) у глобальну мережу інтернет для всіх інших незаборонених запитів від локальних вузлів.

Окремими розширеними списками контролю сувора ізоляція мережі камер спостереження (VLAN 40, підмережа 192.168.1.208/29), що обмежує їхню взаємодію суворо внутрішнім периметром моніторингу та реєстрації. Одночасно з цим, розширений список доступу реалізує глибоку ізоляцію серверної інфраструктури: він дозволяє легітимний обмін даними між серверами автентифікації AAA/RADIUS (VLAN 60) та контролером WLC (VLAN 99), але при цьому жорстко відсікає будь-які спроби несанкціонованого доступу до них з боку звичайних користувацьких підмереж [27].

Для забезпечення захищеного віддаленого керування цифровою інфраструктурою КНП «Гусятинська КЛ» на маршрутизаторі Cisco ISR 2911 було розгорнуто технологію віддаленого доступу Remote Access IPsec VPN. Реалізація захищеного віртуального тунелю базується на дворівневій архітектурі безпеки: на першому етапі (IKE Phase 1) за допомогою політики ISAKMP узгоджуються параметри автентифікації сесії, де застосовано стійкий

алгоритм симетричного кодування та функцію контролю цілісності даних, а перевірка справжності вузлів виконується через попередньо розподілений ключ (Pre-Shared Key). Безпосередній криптографічний захист корисного навантаження здійснюється на другому етапі шляхом конфігурування набору трансформації (Transform Set) у суворому тунельному режимі Encapsulating Security Payload (ESP), який інтегрується у динамічну криптографічну карту (Dynamic Crypto Map).

Процедура автентифікації самого системного адміністратора делегується локальній базі підсистеми AAA (Authentication, Authorization, and Accounting) з призначенням найвищого рівня привілеїв керування, а після успішного встановлення сесії віддаленому пристрою динамічно виділяється IP-адреса зі спеціалізованого віртуального пулу адресації. Прив'язка сформованої крипто-карти до обох зовнішніх інтерфейсів маршрутизатора гарантує постійну доступність шлюзу безпеки та стабільність захищеного каналу адміністрування навіть у режимі аварійного перемикання трафіку між двома незалежними магістральними провайдерами.

2.5 Побудова бездротової інфраструктури та IP-телефонії для КНП «Гусятинська КЛ»

Забезпечення безперервної комунікації медичного персоналу під час виконання щоденних клінічних обов'язків є критично важливою технологічною вимогою для успішного функціонування КНП «Гусятинська КЛ». Оскільки лікарі з планшетами та мобільними телефонами постійно переміщуються між поверхами або палатами закладу, виникає потреба у стабільній роботі з медичною інформаційною системою (МІС) без ризику втрати пакетів чи розриву поточних сесій.

Для вирішення цієї проблеми завдяки контролеру WLC було спроєктовано технологію безшовного роумінгу, що забезпечує безперервну взаємодію клієнтських пристроїв в умовах переміщення корпусами лікарні [28].

Перемикання клієнтського терміналу між суміжними точками доступу відбувається непомітно для користувача, а втрата пакетів під час транзиту пристрою між зонами покриття лікарні повністю відсутня.

Організація стабільного радіопокриття у двоповерховій будівлі лікарні вимагає усунення «сліпих зон» та мінімізації взаємного перекриття сигналів у суміжних частотних діапазонах. Ручне регулювання параметрів є неефективним через динамічну зміну завадової обстановки, тому під час створення проєкту була виконана всебічна оцінка середовища, завдяки якій мережі для КНП «Гусятинська КЛ» було надано високий рівень завадостійкості шляхом активації технології RRM (Radio Resource Management). Завдяки постійному автоматичному скануванню радіоефіру алгоритм WLC самостійно регулює потужність передавачів кожної з 4 точок доступу та динамічно змінює частотні канали задля усунення інтерференції.

Захист конфіденційних медичних даних та внутрішніх ресурсів установи вимагає створення суворо ізольованого бездротового середовища для співробітників. Оскільки циркулююча інформація містить лікарську таємницю та персональні дані пацієнтів КНП «Гусятинська КЛ», виникає потреба у застосуванні найсучасніших методів криптографічного захисту та авторизації. Виходячи з цього, для корпоративного сегменту лікарні було створено окремий SSID з ідентифікатором Hospital_Staff, де реалізовано протокол шифрування WPA2-Enterprise з логічним прив'язуванням трафіку до робочої підмережі VLAN 30. На основі аналізу схеми логічного розподілу встановлено, що трафік персоналу повністю відокремлений від публічного сегменту на рівні тегування кадрів стандарту 802.1Q, що унеможливлює несанкціонований доступ до серверів автоматизації закладу.

Надання бездротового доступу до мережі Інтернет для пацієнтів та відвідувачів не повинно створювати додаткових векторів атак на внутрішні сервери шпиталю чи призводити до неконтрольованого споживання ресурсів КНП «Гусятинська КЛ». З огляду на це, публічний трафік потребує обов'язкової ізоляції, а користувачі – ознайомлення з правилами надання послуг

перед автентифікацією. Завдяки комплексній інженерній роботі над розробкою локальної комп’ютерної мережі для КНП «Гусятинська КЛ» було зорієнтовано конфігурацію на створення відкритого SSID з ідентифікатором Hospital_Guest, де реалізовано авторизацію через спеціалізовану веб-сторінку Captive Portal. У межах цього було зафіксовано суворе логічне розмежування широкомовних доменів, відповідно до якого гостьовий сегмент функціонує у межах VLAN 50 із виділеною IP-підмережею 192.168.1.0 з маскою двадцять шість, тоді як в корпоративний сегмент Hospital_Staff впроваджено технологію динамічного призначення віртуальних мереж (Dynamic VLAN Assignment) на базі стандарту 802.1X та RADIUS-сервера. Завдяки цьому контролер WLC, спираючись на облікові дані працівника, автоматично ізолює підключення у відповідний профільний сегмент. Виходячи з цих параметрів, забезпечується високий рівень безпеки внутрішнього периметру КНП «Гусятинська КЛ» та повна ізоляція незахищених клієнтських терміналів відвідувачів.

У межах розробленої архітектури функцію безпосередньої перевірки облікових даних було делеговано централізованому RADIUS-серверу, роль якого виконує служба NPS (Network Policy Server) на базі Windows Server. При цьому контролер бездротової мережі (WLC) налаштовано як транзитний автентифікатор, що ізолює прямий доступ і лише безпечно перенаправляє запити від клієнтських пристроїв до сервера. Для захисту процесу перевірки персональних логінів медичного персоналу було застосовано протокол PEAP (Protected Extensible Authentication Protocol), завдяки якому весь обмін даними інкапсулюється у зашифрований TLS-тунель, що повністю унеможливлює перехоплення облікових записів у радіоефірі.

Для підключення Smart TV в їдальні КНП «Гусятинська КЛ» використано дротове з’єднання (кручена пара) до порту комутатора доступу в ізольованому VLAN 50. Це дозволило уникнути перевантаження бездротової мережі (Wi-Fi) та звільнити радіоефір для критично важливих завдань медперсоналу.

На базі головного за рахунок інтеграції вбудованого функціоналу архітектури Call Manager Express (CME) маршрутизатора Cisco ISR 2911 було розгорнуто та налаштовано централізований сервіс телефонії.

Для реалізації вимоги у надійному захисті медіапотоків від критичних затримок та мінімізації кількості кабельних ліній, під час передачі даних під час розробки локальної комп'ютерної мережі лікарні було впроваджено такі технологічні рішення:

– підключення IP-телефонів до портів комутаторів із підтримкою стандарту PoE+, що дозволило відмовитися від зовнішніх блоків живлення;

– тегування голосового трафіку в окремому VLAN 70 з метою логічного розподілу та ізоляції мережевих потоків;

– застосування спеціалізованих політик якості обслуговування (QoS) для забезпечення безумовної пріоритезації голосу над звичайними даними.

Організація ефективної та швидкої комунікації між медичним персоналом КНП «Гусятинська КЛ» потребує створення чіткої, структурованої системи внутрішньої адресації з обов'язковим врахуванням потенційного розширення штату установи. Було сформовано та впроваджено логічний 4-значний план внутрішньої нумерації, використання якого повністю гарантує необхідну масштабованість на випадок розширення закладу. Весь комплекс розроблених діапазонів із прикладами призначення номерів подано в таблиці 2.6.

Таблиця 2.6 – План внутрішньої нумерації IP-телефонії КНП «Гусятинська КЛ»

Відділення	**Діапазон номерів**	**Приклад використання**
1	**2**	**3**
Адміністрація	1000 – 1099	1001 – Головний лікар, 1002 – Секретар
Бухгалтерія	2000 – 2099	2001 – Бухгалтер

1	2	3
Лікарняне відділення	3000 – 3099	3001 – Пост медсестри
Технічні служби	9000 – 9099	9001 – Системний адміністратор

Як видно з наведеної таблиці, весь номерний ресурс чітко сегментовано за підрозділами, що значно спрощує подальшу маршрутизацію викликів всередині закладу. Автоматичне налаштування апаратів забезпечує DHCP Option 150. Під час увімкнення телефон автоматично отримує від маршрутизатора IP-адресу та дізнається координати маршрутизатора для завантаження налаштувань.

2.6 Висновок до другого розділу

В другому розділі кваліфікаційної роботи здійснено всебічний аналіз предметної області та технічного завдання на проєктування локальної комп'ютерної мережі для КНП «Гусятинська КЛ», у результаті чого було детально вивчено специфіку функціонування сучасного медичного закладу та виявлено ключові недоліки існуючої плоскої мережевої архітектури, зокрема низьку відмовостійкість, відсутність гнучкого сегментування трафіку й обмежені можливості масштабування. На основі критичного огляду сучасних мережевих технологій, стандартів структурованих кабельних систем та засобів захисту інформації було науково обґрунтовано доцільність впровадження дворівневої ієрархічної моделі мережі із виділеним згорнутим ядром, логічним розділенням сервісів за допомогою віртуальних мереж (VLAN), а також інтеграцією сучасної системи IP-телефонії з підтримкою політик якості обслуговування (QoS), що дозволило сформувати чіткі технічні вимоги для подальшої практичної реалізації та розрахунку логічної структури проєктованої мережі лікарні.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ВІРТУАЛЬНЕ МОДЕЛЮВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ КНП «ГУСЯТИНСЬКА КЛ»

3.1 Консольне налаштування базової комутаційної інфраструктури та маршрутизації

Для перевірки розробленого проєкту мережі, підтвердження теоретичних розрахунків та аналізу працездатності інфраструктури КНП «Гусятинська КЛ» зручно використати середовище моделювання Cisco Packet Tracer [29]. Загальний вигляд побудованої візуальної моделі представлено на рисунку 3.1.

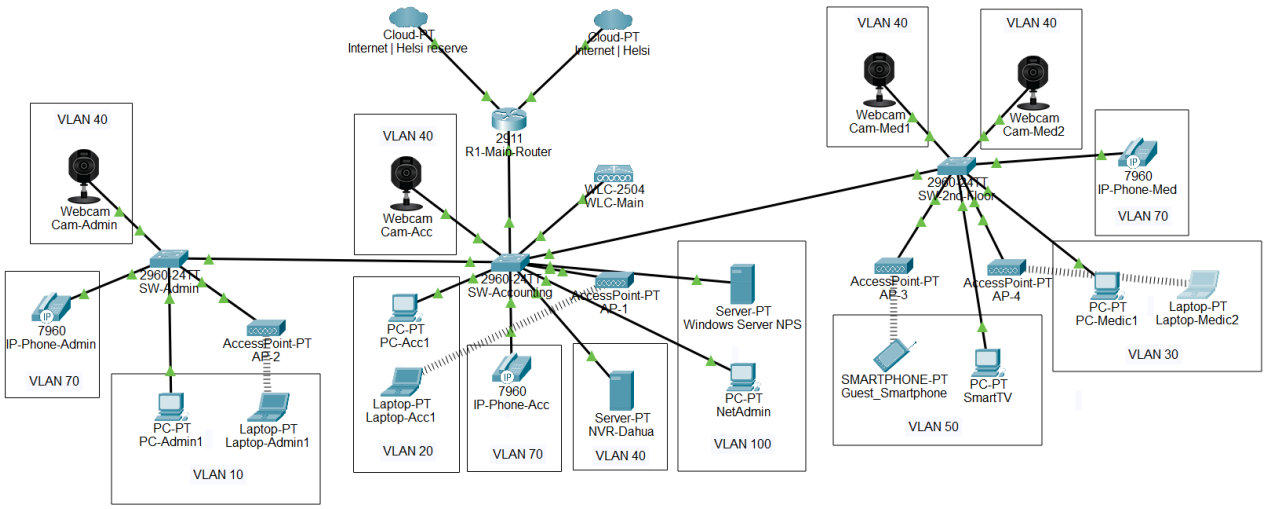

Рисунок 3.1 – Схема логічної топології мережі

Як видно з поданого рисунку, на схемі відображено ключові вузли комутації та маршрутизації. Свідоме спрощення моделі за кількістю кінцевих пристроїв зроблено для уникнення ускладнення наочності роботи мережі, але без втрати основних компонентів, що потребують перевірки у тестуванні інженерних рішень.

Для перевірки результатів налаштування маршрутизації між віртуальними мережами КНП «Гусятинська КЛ» необхідно проаналізувати

поточний стан інтерфейсів на головному маршрутизаторі, який відображено на рисунку 3.2.

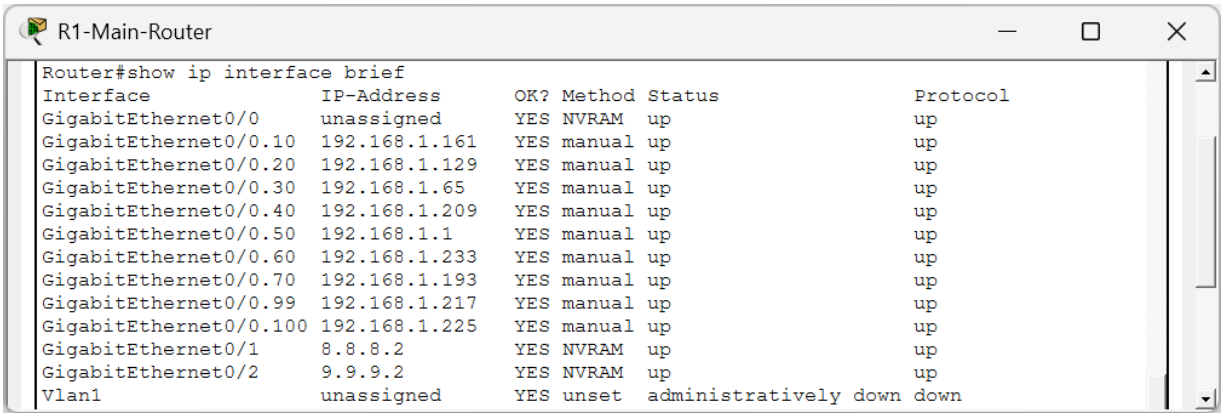

Рисунок 3.2 – Верифікація IP-адрес підінтерфейсів маршрутизатора

Згідно з рисунком, всі створені підінтерфейси переведені в режим up, а протокол сигналізує про їхню повну активність. Демонструє коректність конфігурації інкапсуляції 802.1Q та успішний запуск маршрутизації Inter-VLAN для всіх сегментів лікарні [30].

Для розмежування зон безпеки, логічного розподілу користувачів та ізоляції широкомовного трафіку проведемо закріплення фізичних інтерфейсів за певними доменами. Процес розподілу кінцевих портів комутаторів рівня доступу між створеними VLAN для різних відділів лікарні підтверджується виводом бази даних, який продемонстровано на рисунку 3.3.

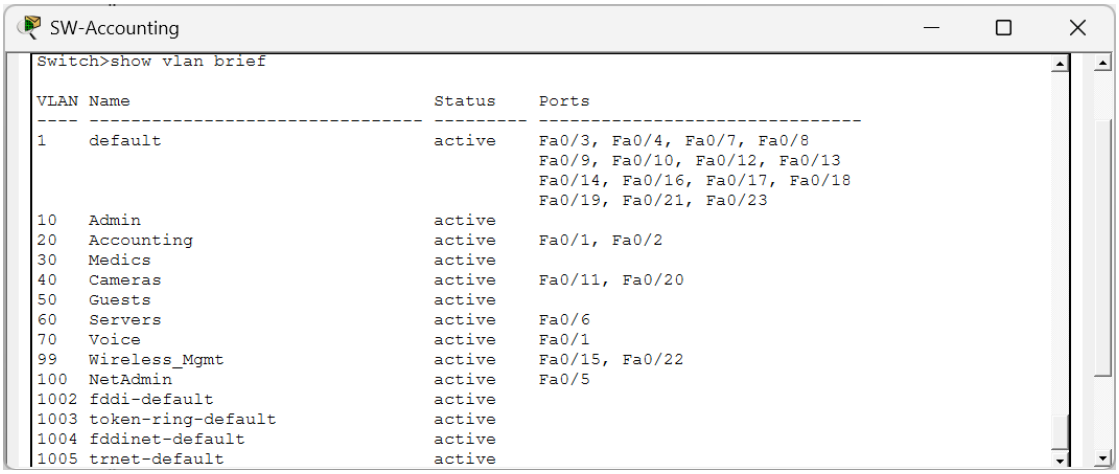

Рисунок 3.3 – Конфігурація та розподіл портів VLAN на комутаторі

Як видно з поданого рисунку, кожен інтерфейс комутатора чітко закріплений за відповідним ідентифікатором мережі підрозділу. Таке налаштування пристроїв виконано вірно та згідно розроблених схем, що повністю ізолює інформаційні потоки відділів медичного закладу на другому рівні [31].

В цілях перевірки коректності роботи служби DHCP та доказу її правильного функціонування на маршрутизаторі медичного закладу звернемося до поточної таблиці прив'язки IP-адрес до MAC-адрес (DHCP Binding), яку зображено на рисунку 3.4.

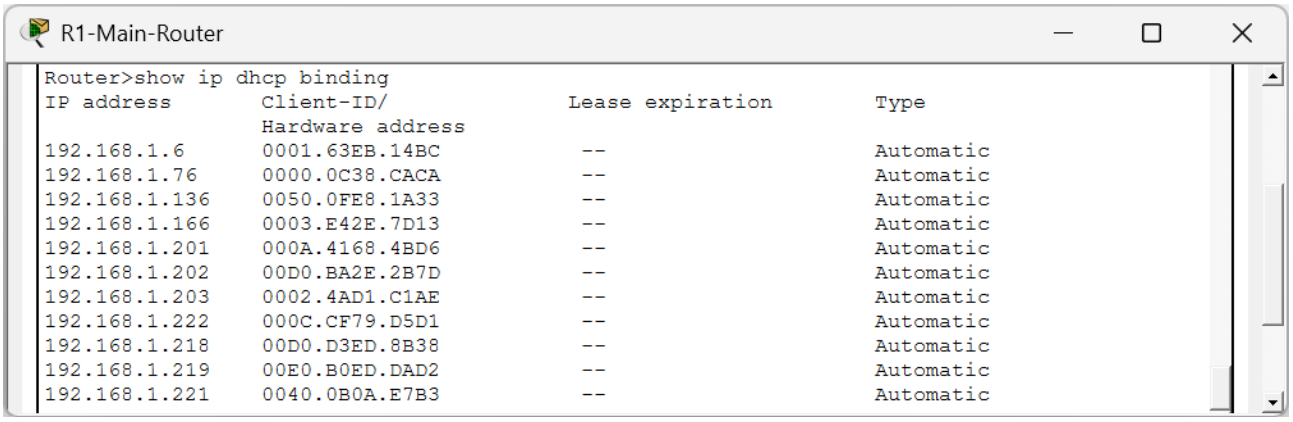

Рисунок 3.4 – Таблиця розподілу та прив'язки IP-адрес до MAC-адрес пристроїв у базі даних DHCP-сервера

Як видно з поданого рисунку, в базі даних пристрою чітко зафіксовано відповідність динамічно виділених IP-адрес унікальним фізичним MAC-адресам хостів медичного та адміністративного персоналу. Спостерігається успіх динамічного розподілу параметрів, що доводить працездатність налаштованої служби [32].

Для забезпечення виходу локальної корпоративної мережі КНП «Гусятинська КЛ» до глобальної мережі інтернет необхідно реалізувати чітку логіку трансляції адрес та забезпечити безперебійність зв'язку. Приклад реалізації трансляції адрес (NAT Overload), механізму активного моніторингу

віддалених вузлів (IP SLA) та відмовостійкого резервування провайдерів (Dual-ISP) наведено у лістингу 3.1.

Лістинг 3.1 – Конфігурація відмовостійкого Dual-ISP NAT Overload на базі PAT та IP SLA

```
ip nat inside source route-map MAP_ISP1 interface gigabitEthernet 0/1 overload
ip nat inside source route-map MAP_ISP2 interface gigabitEthernet 0/2 overload

interface gigabitEthernet 0/0.10
ip nat inside

interface gigabitEthernet 0/0.20
ip nat inside

interface gigabitEthernet 0/1
ip nat outside

interface gigabitEthernet 0/2
ip nat outside

ip access-list extended NAT_TRAFFIC
permit ip 192.168.0.0 0.0.255.255 any

route-map MAP_ISP1 permit 10
match ip address NAT_TRAFFIC
match interface gigabitEthernet 0/1

route-map MAP_ISP2 permit 10
match ip address NAT_TRAFFIC
match interface gigabitEthernet 0/2

ip sla 1
icmp-echo 8.8.8.8 source-interface gigabitEthernet 0/1
timeout 2000
frequency 5
ip sla schedule 1 start-time now life forever
track 1 ip sla 1 reachability

ip route 0.0.0.0 0.0.0.0 8.8.8.1 track 1
ip route 0.0.0.0 0.0.0.0 9.9.9.1 50
```

Як видно з наведеного лістингу, для економії публічного адресного простору застосовано механізм NAT Overload, який дозволяє внутрішнім хостам виходити в інтернет через одну зовнішню IP-адресу. Водночас

технологія Dual-ISP гарантує відмовостійкість завдяки підключенню до двох незалежних провайдерів [33].

Щоб забезпечити автоматичне перемикання на резервного провайдера у разі аварії на лінії зв'язку, застосовано механізм плаваючого маршруту (Floating Static Route) та технологію Cisco IP SLA. Параметри конфігурації та стан цього маршруту наведено на рисунку 3.5.

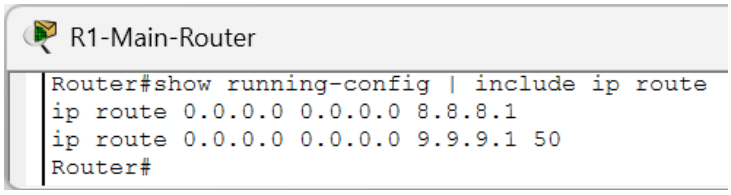

Рисунок 3.5 – Конфігурація основного та плаваючого маршрутів

Як видно з рисунку, для плаваючого маршруту через резервного провайдера задано вищу адміністративну відстань (метрику) порівняно з основним маршрутом. Завдяки зміні цього параметра шлях залишається в режимі очікування і з'явиться в активній таблиці маршрутизації лише у разі падіння головного лінку.

Використаєно протокол VTP, з автентифікацією, для захисту від ризиків. Поточний статус роботи цього протоколу на головному комутаторі ілюструє рисунок 3.6.

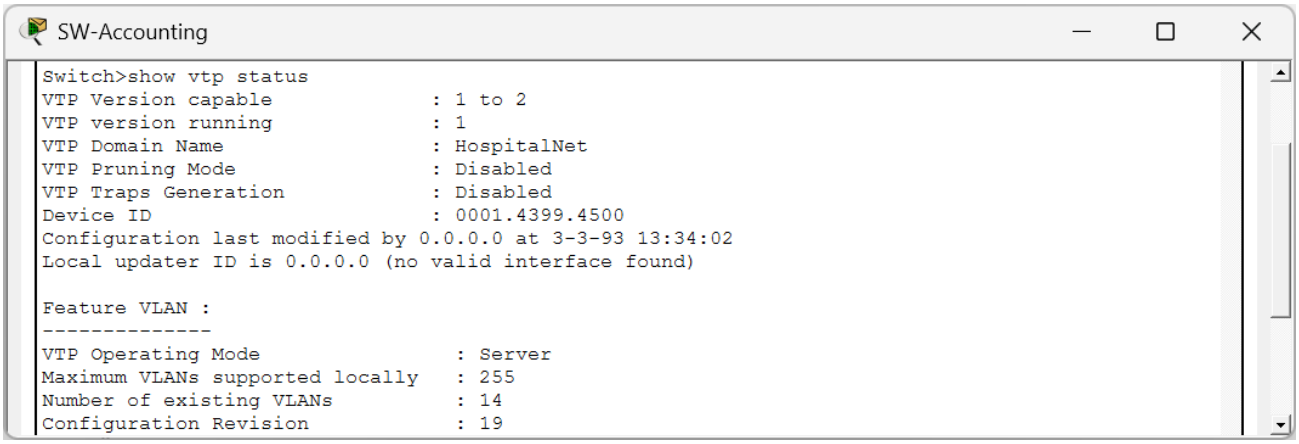

Рисунок 3.6 – Верифікація статусу протоколу VTP на комутаторі

На рисунку показано успішне функціонування пристрою в режимі сервера. Як видно з поданого матеріалу, центральний комутатор автоматично транслює базу даних віртуальних мереж на підпорядковані комутатори рівня доступу КНП «Гусятинська КЛ», що унеможливлює виникнення помилок при ручному конфігуруванні.

3.2 Налаштування політик безпеки, віддаленого доступу та бездротових мереж

Для забезпечення безпеки корпоративної інфраструктури КНП «Гусятинська КЛ» необхідно реалізувати надійний захист мережевих пристроїв від несанкціонованого фізичного підключення стороннього обладнання. Для захисту на фізичному рівні комутаторів виконано налаштування функції прив'язки MAC-адрес до портів (Sticky MAC) із застосуванням жорстких санкцій за порушення у вигляді автоматичного вимкнення порту (Shutdown), як показано у лістингу 3.2.

Лістинг 3.2 – Система апаратного захисту портів Cisco Port Security

```
interface range fastEthernet 0/2 - 20
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown

interface fastEthernet 0/1
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

Як видно з поданого лістингу, конфігурування механізму Port Security забезпечує динамічне запам'ятовування легітимних адрес, а у разі фіксації невідомого індивідуального ідентифікатора інтерфейс миттєво переходить у стан Error-Disabled.

Для перевірки коректності функціонування розгорнутих політик безпеки на комутаційному обладнанні медичного закладу проаналізовано глобальний статус системи Port Security на комутаторі адміністрації, дані якого відображено на рисунку 3.7.

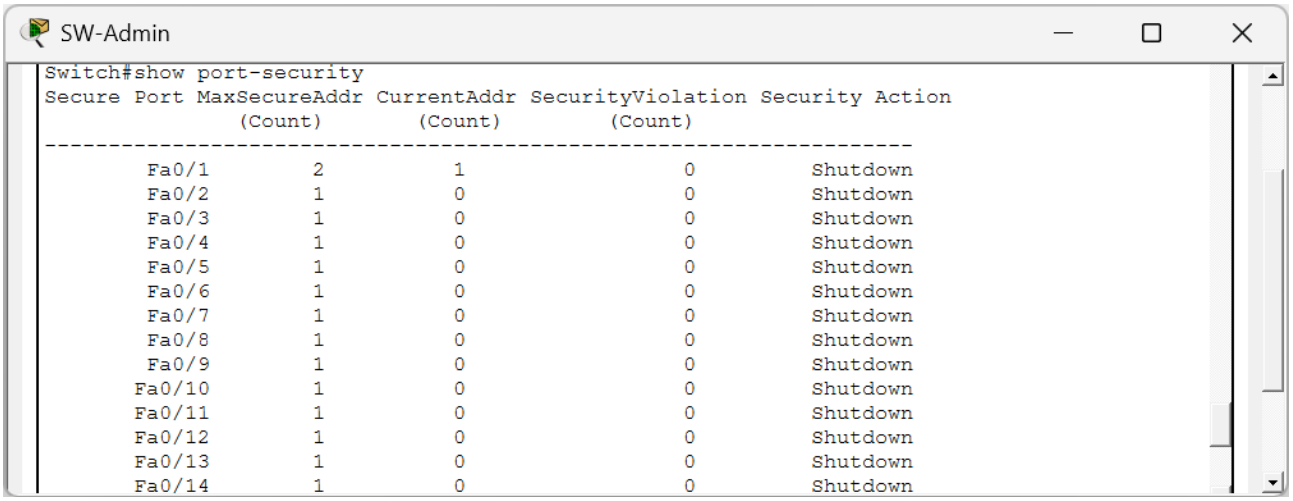

Рисунок 3.7 – Верифікація глобальної активації та параметрів системи Port Security на комутаторі SW-Admin

Як видно з поданого рисунку, механізм захисту периферійних ліній зв'язку перебуває в активному стані, що підтверджує готовність комутатора до блокування потенційних загроз на рівні доступу.

Необхідність повної ізоляції гостьової мережі та мережі IP-камер від головних серверів КНП «Гусятинська КЛ» за допомогою розширених списків контролю доступу (Extended ACL), наведено у лістингу 3.3.

Лістинг 3.3 – Списки контролю доступу ACL

```
access-list 1 permit 192.168.1.0 0.0.0.255

ip access-list extended GUEST_SECURITY
deny ip 192.168.1.0 0.0.0.63 192.168.1.64 0.0.0.63
deny ip 192.168.1.0 0.0.0.63 192.168.1.128 0.0.0.31
deny ip 192.168.1.0 0.0.0.63 192.168.1.160 0.0.0.31
permit ip any any

ip access-list extended CAMERA_SECURITY
permit ip 192.168.1.208 0.0.0.7 192.168.1.0 0.0.0.255
```

```
deny ip any any

ip access-list extended INTERNAL_ISOLATION
permit ip 192.168.1.224 0.0.0.7 192.168.1.216 0.0.0.7
permit ip any 192.168.1.224 0.0.0.7
deny ip any 192.168.1.0 0.0.0.255
permit ip any any
```

Як видно з наведеного лістингу, розроблені правила чітко розмежовують права доступу підмереж, повністю блокуючи проходження IP-пакетів від гостьових клієнтів та систем відеоспостереження до серверного сегмента.

Для підтвердження працездатності розгорнутих безпекових інструментів та аналізу застосованих правил фільтрації безпосередньо в консолі маршрутизатора ядра звернемося до даних рисунка 3.8.

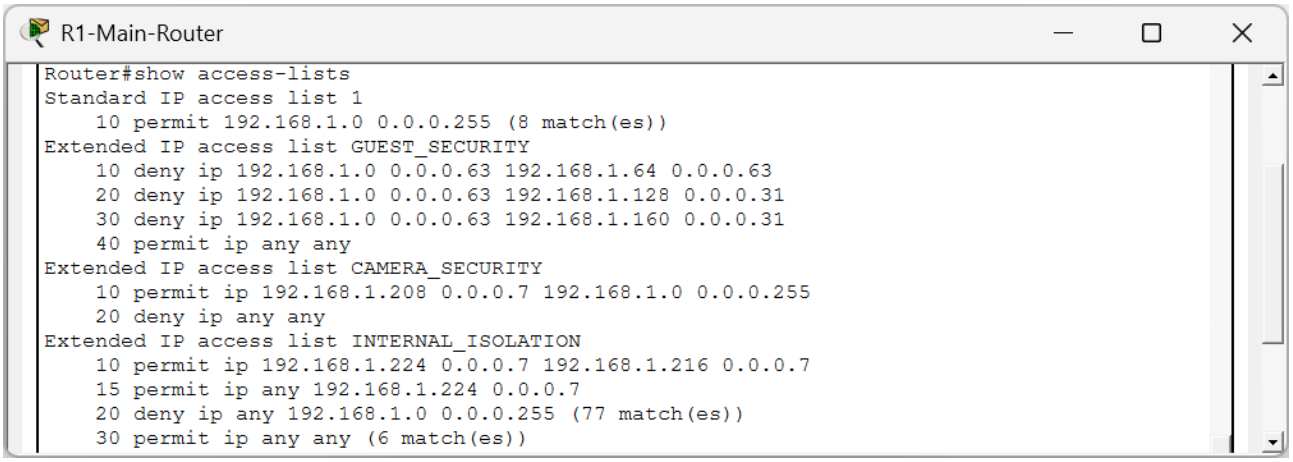

Рисунок 3.8 – Структура та правила функціонування розширених списків контролю доступу Extended ACL на головному маршрутизаторі

Як видно з поданого рисунку, налаштування пристроїв виконано вірно та згідно розроблених схем. На інтерфейсах пристрою чітко зафіксовано лічильники спрацьовування відповідних розширених ACL-правил, а з’єднання між ізольованими зонами функціонує без втрат легітимних даних, демонструючи успіх блокування забороненого трафіку [34].

Розгорнено захищене з'єднання за технологією Remote Access IPsec VPN. Спочатку активація криптографічного ліцензійного пакета операційної системи. Далі побудова безпечного тунелю, що включає активацію ліцензії,

створення пулу локальних адрес, визначення політик ISAKMP та формування криптокарт для відповідних інтерфейсів наведено у лістингу 3.4.

Лістинг 3.4 – Налаштування захищеного віддаленого доступу (Remote Access IPsec VPN) та активація криптографічного модуля

```
license boot module c2900 technology-package securityk9

aaa new-model
aaa authentication login vpn_auth local
aaa authorization network vpn_author local

ip local pool VPN_POOL 10.10.10.1 10.10.10.5
username remoteadmin privilege 15 secret AdminVpnPass2026

crypto isakmp policy 10
encryption aes
hash sha
authentication pre-share
group 2

crypto isakmp client configuration group HospitalRemoteVPN
key SecretVpnKey2026
pool VPN_POOL

crypto ipsec transform-set ESP_AES_SHA esp-aes esp-sha-hmac

crypto dynamic-map DYN_VPN_MAP 10
set transform-set ESP_AES_SHA
reverse-route

crypto map VPN_MAP client authentication list vpn_auth
crypto map VPN_MAP client configuration address respond
crypto map VPN_MAP 10 ipsec-isakmp dynamic DYN_VPN_MAP
```

Як видно з поданого лістингу, після успішної активації відповідного рівня ліцензування (securityk9) маршрутизатор відкриває можливість встановлення шифрованих сесій. Усі параметри віртуальної приватної мережі сконфігуровано в повному обсязі: задано стійкі алгоритми шифрування та хешування.

Для перевірки коректності ініціалізації та активації параметрів шифрування другої фази звернемося до поточного стану пристрою. Успішність активації набору параметрів безпеки (Transform Set) підтверджується виводом з консолі маршрутизатора, який представлено на рисунку 3.9.

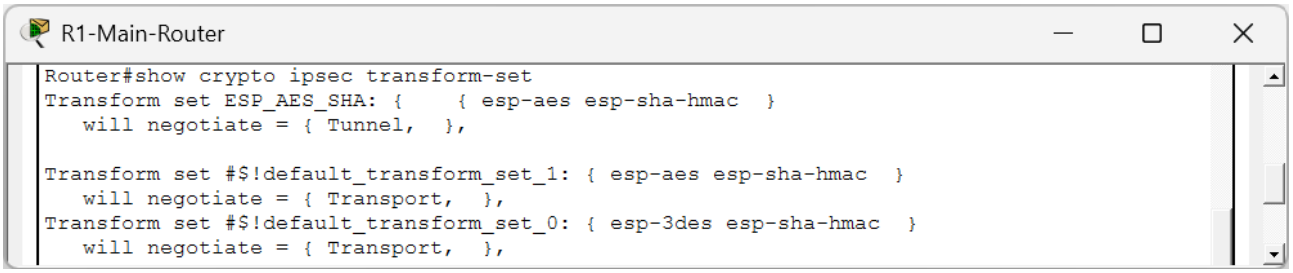

Рисунок 3.9 – Верифікація параметрів ініціалізації набору трансформації Transform Set для криптографічного захисту IPsec

Як видно з рисунку, ініціалізація параметрів шифрування відбулася успішно, а статус фази Transform Set підтверджує готовність обладнання до інкапсуляції трафіку.

Для переходу до бездротового сегмента лікарняної мережі та забезпечення Enterprise-рівня безпеки необхідно впровадити сувору політику контролю доступу. Для реалізації централізованої автентифікації, авторизації та обліку дій користувачів розгорнемо виділений RADIUS-сервер, налаштування якого відображено на рисунку 3.10.

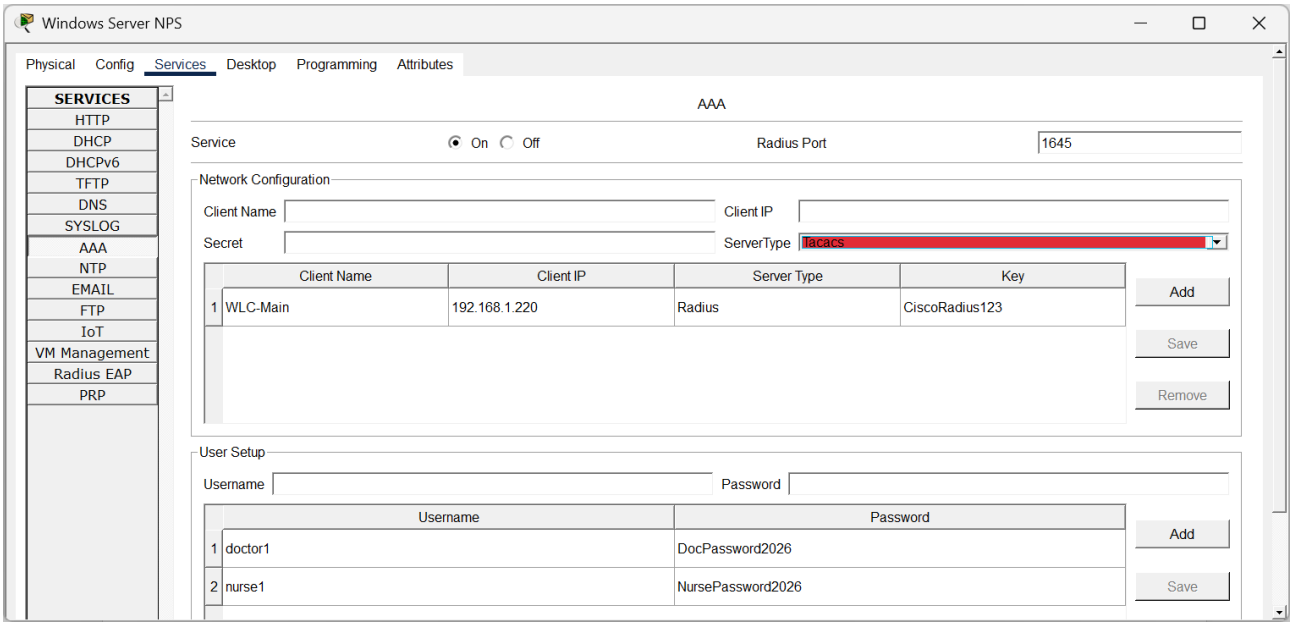

Рисунок 3.10 – Налаштування бази даних та параметрів AAA на корпоративному RADIUS-сервері Windows Server NPS

Як видно з рисунку, конфігурування служби автентифікації виконано вірно, що дозволяє перейти до розгортання бездротових профілів на контролері бездротової локальної мережі (WLC).

Для логічного розділення користувачів у межах КНП «Гусятинська КЛ» та забезпечення належного рівня захисту інформації необхідно створити окремі бездротові мережі. Процес розгортання профілів для медичної та гостьової мереж клініки, а також аналіз їхнього поточного статусу подано на рисунку 3.11.

Рисунок 3.11 – Перелік створених бездротових мереж WLANs та верифікація їхнього активного статусу в інтерфейсі контролера

Встановлено параметри захисту відповідно до сучасних стандартів кібербезпеки. Фінальні налаштування безпеки бездротової мережі 802.1X на контролері, які забезпечують використання індивідуальних зашифрованих сесій для персоналу КНП «Гусятинська КЛ».

3.3 Перевірка працездатності інфраструктури та тестування кінцевих вузлів

Для перевірки автентифікації користувачів опишемо процес підключення клієнта до робочої Wi-Fi мережі. Налаштування протоколу шифрування (PEAP/WPA2 Enterprise) з боку користувача наведено на рисунку 3.12.

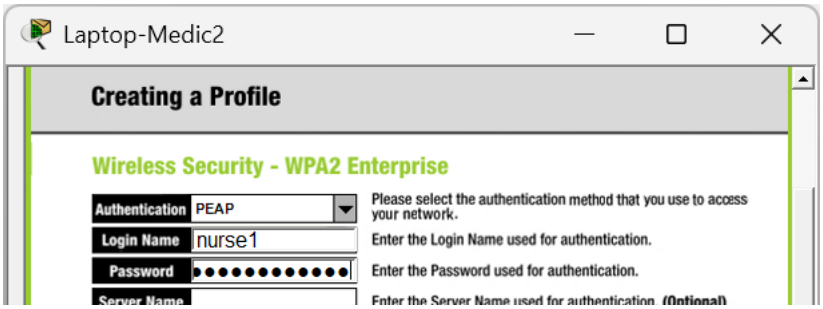

Рисунок 3.12 – Налаштування протоколу шифрування та верифікації облікових даних на клієнтському пристрої

Як видно з поданого рисунку, SSID та корпоративні реквізити користувача задано коректно. Конфігурація за протоколом PEAP забезпечує надійний захист та демонструє правильну інтеграцію клієнта із сервером автентифікації.

Для підтвердження бездротової асоціації перевіримо статус підключення обладнання до інфраструктури КНП «Гусятинська КЛ». Успішне встановлення з'єднання з точкою доступу ілюструє рисунок 3.13.

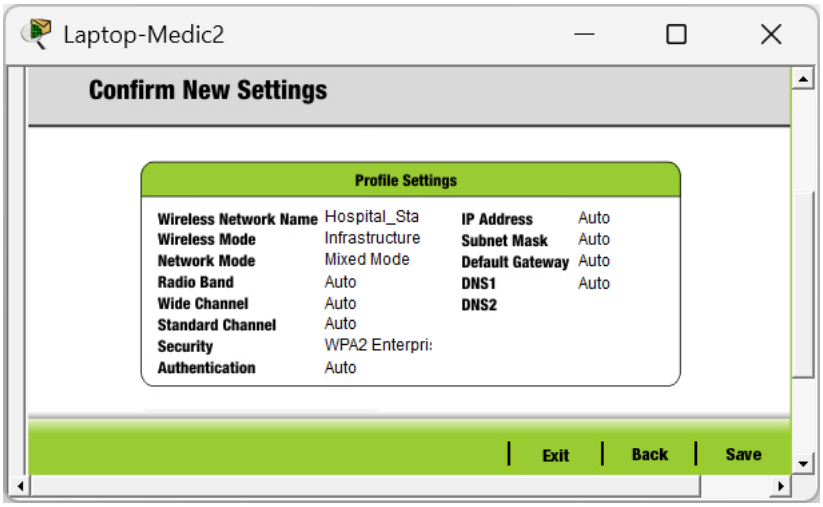

Рисунок 3.13 – Верифікація фінальних параметрів створюваного бездротового профілю безпеки на робочій станції

Як видно з поданого рисунку, клієнт успішно авторизувався та встановив з'єднання з точкою доступу. Результати тестування показують, що налаштування виконано вірно, а захищений профіль безпеки функціонує.

В цілях перевірки політик безпеки продемонстровано роботу налаштованих списків доступу (ACL). Проведемо тестування з'єднання до забороненого сегмента мережі, результати якого показано на рисунку 3.14.

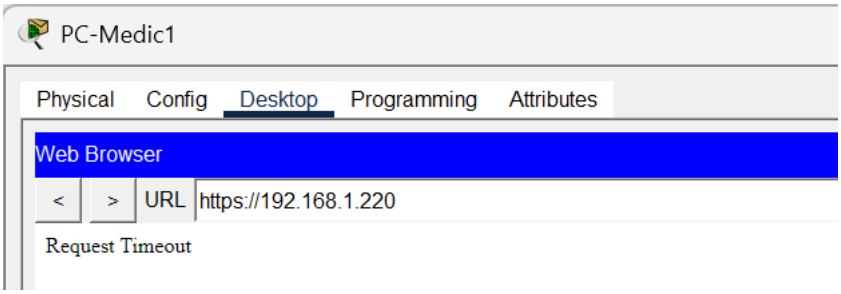

Рисунок 3.14 – Верифікація ефективності дії міжмережевих списків контролю доступу ACL для користувацьких підмереж

Як видно з поданого рисунку, підключення до приладу управління бездротовими мережами було заблоковане. Це констатує ізоляцію сегментів і підтверджує працездатність застосованих правил ACL.

Для фінальної верифікації виконано практичний тест встановленого голосового з'єднання між двома IP-телефонами. Стан апаратів із фіксацією активного сеансу зв'язку наведено на рисунку 3.15.

Рисунок 3.15 – Верифікація встановлення двостороннього голосового з'єднання між абонентами мережі клініки

Як видно з поданого рисунку, на екранах відображається статус «Connected», що свідчить про успішну комутацію абонентів. Загальний підсумок випробувань доводить, що моделювання повністю підтвердило працездатність спроєктованої архітектури КНП «Гусятинська КЛ» та її відповідність технічним вимогам.

3.4 Висновок до третього розділу

У третьому розділі кваліфікаційної роботи виконано практичну реалізацію та віртуальне моделювання спроєктованої архітектури корпоративної мережі КНП «Гусятинська КЛ» у середовищі Cisco Packet Tracer. У ході симуляції успішно верифіковано коректність конфігурування базової комутаційної інфраструктури, зокрема запуск міжмережевої маршрутизації (Inter-VLAN) за стандартом 802.1Q, динамічний розподіл адресних параметрів через службу DHCP, а також автоматизацію централізованого управління віртуальними мережами за допомогою протоколу VTP. Високий рівень відмовостійкості та зв'язності з глобальною мережею було досягнуто завдяки успішному впровадженню технології Dual-ISP із механізмами PAT (NAT Overload), активного моніторингу ліній через IP SLA та плаваючих статичних маршрутів для автоматичного перемикання на резервного провайдера у разі аварії. Комплексний захист медичної інфраструктури забезпечено шляхом апаратного захисту ліній зв’язку Cisco Port Security із прив'язкою Sticky MAC, суворої ізоляції гостьового сегмента й систем відеоспостереження від серверів за допомогою розширених списків контролю доступу (Extended ACL), організації шифрованих каналів Remote Access IPsec VPN, а також розгортання бездротової мережі Enterprise-рівня з централізованою RADIUS-автентифікацією за протоколом PEAP/WPA2. Тестування кінцевих вузлів, що включало перевірку ефективності міжмережевої фільтрації та успішне встановлення двостороннього сеансу голосового зв'язку в сегменті IP-телефонії, повністю підтвердило надійність.

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Аварії з викидом радіоактивних речовин та заходи безпеки в КНП «Гусятинська КЛ»

Аварії з викидом радіоактивних речовин належать до техногенних надзвичайних ситуацій [36]. Вони супроводжуються порушенням нормального функціонування об'єктів, радіоактивним зараженням місцевості та ураженням населення [37].

Причини таких аварій умовно поділяють на аварії мирного та воєнного характеру [38]. У сучасних умовах найбільш актуальною причиною аварій воєнного характеру є регулярні ракетні та дронові удари по об'єктах критичної інфраструктури України. Руйнування об'єктів атомної енергетики чи промисловості із застосуванням звичайних засобів ураження здатне спричинити небезпечні вторинні наслідки: масштабний викид радіоактивних речовин у довкілля.

Радіаційне ураження організму відбувається внаслідок як зовнішнього опромінення (гамма- та бета-променями), так і внутрішнього через потрапляння радіонуклідів в організм людини з повітрям, водою чи їжею.

Для захисту персоналу, який розробляє, налаштовує та обслуговує комп'ютерну мережу Комунального некомерційного підприємства «Гусятинська комунальна лікарня» у разі виникнення загрози або безпосереднього факту аварії з викидом радіоактивних речовин впроваджено комплексний план заходів цивільного захисту.

Основні організаційні та інженерно-технічні заходи включають:

– Забезпечено оперативний доступ працівників до підготовленого сховища в приміщеннях з мінімальною проникністю іонізуючого випромінювання (підвальні приміщення лікарні, які належним чином обладнані як споруди цивільного захисту).

– Передбачено обов'язкове використання засобів індивідуального захисту органів дихання (респіраторів класу FFP3, протигазів) та шкірних покривів для мінімізації внутрішнього опромінення.

– Впроваджено постійний контроль радіаційної обстановки на території та всередині медичного закладу за допомогою штатних побутових і професійних дозиметрів.

– Організовано проведення герметизації серверних приміщень, а також переведення систем вентиляції в режим повної рециркуляції або їх повне вимкнення для уникнення потрапляння радіоактивного пилу на чутливе комутаційне обладнання, оптичні порти та системи охолодження.

Під час проєктування та налаштування локальної мережі інженери тривалий час перебувають безпосередньо у робочих приміщеннях КНП «Гусятинська КЛ». При отриманні сигналу повітряної тривоги або спеціального сповіщення про радіаційну загрозу розроблено чіткий та автоматизований алгоритм дій:

– Системний адміністратор оперативно зберігає поточні конфігураційні дані комутаторів і маршрутизаторів.

– Активуються заздалегідь підготовлені скрипти автоматизованого критичного резервного копіювання (backup) медичних баз даних та електронних карток пацієнтів на віддалені хмарні сервери.

– Адміністратор блокує робочу станцію та негайно прямує до визначеного укриття.

Для гарантування безпеки критично важливих даних пацієнтів та стабільної підтримки життєво важливих систем лікарні в умовах можливого пошкодження зовнішніх електромереж, уся серверна інфраструктура та головні комутаційні вузли підключені до потужних джерел безперебійного живлення (UPS) з можливістю тривалої автономної роботи.

Після офіційного відбою тривоги, проведення дезактиваційних заходів (за потреби) та отримання підтвердженої інформації щодо безпечного рівня

радіаційного фону, повне обслуговування та адміністрування мережі відновлюється у штатному режимі.

4.2 Вимоги ергономіки до організації робочого місця адміністратора мережі КНП «Гусятинська КЛ»

Проєктування, модернізація та щоденне адміністрування комп'ютерної мережі сучасної лікарні належить до категорії напруженої розумової праці. Основне функціональне навантаження припадає на центральну нервову систему, що безпосередньо виражається у тривалому зоровому та стійкому нервово-емоційному напруженні.

Системні адміністратори керують складними мережевими процесами дистанційно, безперервно сприймаючи та аналізуючи текстову й графічну інформацію через екранні пристрої моніторів. Відповідно, у даному проєкті детально узгоджено організацію робочого місця з фізіологічними, анатомічними й психологічними можливостями та характеристиками людини [39].

Робоче місце адміністратора мережі КНП «Гусятинська КЛ« організовано з суворим дотриманням чинних вимог ДСанПіН 3.3.2.007-98 [40]. Для поліпшення загальних умов праці, збереження високої працездатності та підтримання належної терморегуляції організму ІТ-спеціаліста враховано оптимальний мікроклімат приміщення:

– Площа, що припадає на одне робоче місце, становить не менше 6,0 м², а загальний повітряний об'єм приміщення не менше 20,0 м³.

– Температура повітря в робочій зоні впродовж року підтримується в межах 21–23 °С, а відносна вологість становить 40–60%.

– Приміщення обов'язково оснащено автоматичною системою кондиціонування, припливно-витяжною вентиляцією та сертифікованою аптечкою першої медичної допомоги.

Виробниче штучне та природне освітлення спроєктовано згідно з вимогами ДБН В.2.5-28:2018. Воно забезпечує рівномірний розподіл яскравості в полі зору та повну відсутність засліпленості чи прямих відблисків. Обладнано комбіновану систему освітлення: загальне та місцеве. Область столу, де розміщуються документи та клавіатура, має рівень освітленості не менше 400 лк, а коефіцієнт пульсації штучного світла не перевищує 5%. Робочі столи ІТ-персоналу орієнтовані та розміщені так, щоб природне світло з вікон падало переважно з лівого боку, що мінімізує появу дзеркальних відблисків на захисних покриттях моніторів.

Ергономічні рішення щодо облаштування робочого місця:

– Має спеціальну матову поверхню з низьким коефіцієнтом відбиття світла для запобігання стомлюваності очей; висота столу зафіксована на рівні 720 мм, а під стільницею забезпечено достатній простір для ніг.

– Використовується сучасне підйомно-поворотне крісло з анатомічною підтримкою хребта, що легко регулюється за висотою сидіння, кутом нахилу та висотою спинки. Це дозволяє працівнику періодично змінювати позу тіла, знижуючи статичне навантаження на опорно-руховий апарат.

– Екран монітора розташовано на оптимальній та безпечній відстані 600–700 мм від очей користувача (кут зору становить 15–20° нижче горизонталі). Клавіатура та миша відокремлені від екрана і розміщені так, щоб лікті та кисті рук адміністратора мали опору, що запобігає розвитку хронічного синдрому зап'ястного каналу (тунельного синдрому).

Для надійного захисту інженерів від постійного підвищеного шумового навантаження, все активне та гучне мережеве обладнання (магістральні маршрутизатори, сервери, дискові масиви, комутатори ядра) винесено за межі робочого кабінету у відокремлену серверну кімнату з обмеженим доступом та додатковою звукоізоляцією стін.

Режим праці та відпочинку адміністраторів передбачає обов'язкові регламентовані перерви. При стандартній 8-годинній робочій зміні призначено короткочасні перерви тривалістю 15 хвилин через кожну годину безперервної

інтенсивної роботи за монітором. Під час цих перерв рекомендується виконувати легкі фізичні вправи для зняття загального тонусу та спеціальну гімнастику для очей.Комплексне дотримання розроблених санітарно-гігієнічних, інженерних та ергономічних вимог мінімізує загальну втомлюваність ІТ-фахівців, запобігає розвитку професійних захворювань, підвищує концентрацію уваги та гарантує загальну надійність і безпеку функціонування комп'ютерної мережі КНП «Гусятинська КЛ».

4.3 Висновки до четвертого розділу

В цьому розділі кваліфікаційної роботи детально розглянуто актуальні питання безпеки життєдіяльності та основи охорони праці персоналу КНП «Гусятинська КЛ», який безпосередньо задіяний у розробці та адмініструванні запроєктованої локальної комп'ютерної мережі.

Проаналізовано ризики виникнення техногенних надзвичайних ситуацій воєнного характеру, пов'язаних із можливими аваріями з викидом радіоактивних речовин у довкілля через удари по критичній інфраструктурі.

На основі проведеного аналізу розроблено комплексний план інженерно-технічних та організаційних заходів цивільного захисту, а також чіткий покроковий алгоритм дій системного адміністратора під час отримання сигналів оповіщення про радіаційну небезпеку, що спрямований на збереження життя працівників та захист важливих медичних даних лікарні.

Окрім цього, визначено та обґрунтовано основні ергономічні й санітарно-гігієнічні вимоги до організації робочого місця адміністратора мережі відповідно до ДСанПіН 3.3.2.007-98 та ДБН В.2.5-28:2018.

Запропоновані комплексні рішення щодо оптимізації параметрів мікроклімату, штучного й природного освітлення, зниження шумового навантаження та впровадження раціонального режиму праці й відпочинку дозволяють суттєво знизити зорову та нервово-емоційну втому, запобігти виникненню професійних захворювань ІТ-спеціалістів.

ВИСНОВКИ

У кваліфікаційній роботі вирішено актуальне науково-практичне завдання, яке полягає у розробці та моделюванні сучасної, відмовостійкої і захищеної локальної комп’ютерної мережі для потреб КНП «Гусятинська комунальна лікарня». Запропоновані інфраструктурні рішення дозволяють оптимізувати процеси обміну даними, забезпечити безперебійний доступ до медичних інформаційних систем (e-Health) та гарантувати високий рівень кібербезпеки конфіденційної інформації пацієнтів.

У першому розділі кваліфікаційної роботи освітнього рівня «Бакалавр»:

– Подано ґрунтовний аналіз актуальності впровадження сучасних ІТ-рішень, хмарних сервісів (e-Health) та телемедицини у медичній галузі, що підтвердило необхідність модернізації мережі для стабільної обробки великих масивів конфіденційних даних та забезпечення оперативної взаємодії персоналу.

– Розглянуто ключові проблеми наявної інфраструктури (низька відмовостійкість, відсутність ізоляції та резервування) та обґрунтовано вибір ієрархічної топології типу «розширена зірка» для гарантування гнучкості та масштабованості системи.

– Висвітлено базові принципи побудови захищеного корпоративного середовища, включно з методами логічної сегментації та контролем доступу для ізоляції чутливого трафіку.

– Проаналізовано стандартизовану методологію життєвого циклу мережі Cisco PPDIOO, яка стала основою для систематизованого підходу до збору вимог, проєктування, впровадження та підтримки мережевої інфраструктури об'єкта.

У другому розділі кваліфікаційної роботи:

– Досліджено специфіку приміщень і робочих місць КНП «Гусятинська КЛ» та розроблено проєкт фізичної топології і структурованої кабельної

системи (СКС) з урахуванням сучасних стандартів пропускної здатності та пожежної безпеки (використання оптоволокна, кабелів Cat6 та ізоляції LSZH).

– Обґрунтовано модель логічної сегментації мережі, що передбачає виділення окремих VLAN для адміністрації, бухгалтерів, медичного персоналу, гостьового доступу, відеоспостереження та IP-телефонії.

– Сформовано план IP-адресації з використанням методу масок змінної довжини (VLSM), що дозволило оптимізувати використання адресного простору; проведено порівняльний аналіз та обрано обладнання екосистеми Cisco для апаратної реалізації проєкту, включаючи впровадження системи Cisco Call Manager Express (CME) для внутрішньої телефонії.

У третьому розділі кваліфікаційної роботи:

– Розроблено віртуальну симуляційну модель спроєктованої мережі в середовищі Cisco Packet Tracer.

– Запропоновано та успішно налаштовано схеми міжмережевої маршрутизації (Inter-VLAN), механізми трансляції адрес (NAT Overload) та динамічного розподілу параметрів через локальний DHCP-сервер.

– Спроєктовано та імплементовано комплекс політик безпеки (включно із Port Security, DHCP Snooping, розширеними списками контролю доступу ACL) і технологію віддаленого доступу Remote Access IPsec VPN; інтегровано захищену бездротову мережу Enterprise-рівня з RADIUS-авторизацією за протоколом PEAP/WPA2.

– Протестовано працездатність та відмовостійкість інфраструктури (зокрема, запуск резервних ліній через Dual-ISP та IP SLA, успішне проходження телефонних дзвінків та блокування несанкціонованого доступу), що повністю підтвердило відповідність розробленої моделі поставленим технічним вимогам [35].

У розділі «Безпека життєдіяльності, основи охорони праці»:

– Висвітлено питання цивільного захисту, зокрема розроблено алгоритм дій адміністратора мережі у випадку надзвичайних ситуацій воєнного

характеру (аварії з викидом радіоактивних речовин) для забезпечення безпеки персоналу та збереження критичних медичних даних.

– Проаналізовано та сформовано комплекс санітарно-гігієнічних та ергономічних вимог до робочого місця ІТ-спеціаліста (мікроклімат, освітлення, зниження шуму, правильна організація простору) відповідно до чинних стандартів для збереження працездатності та профілактики професійних захворювань.

ПЕРЕЛІК ДЖЕРЕЛ

1 Електронна система охорони здоров'я (eHealth) в Україні: офіційний портал. [Електронний ресурс]. – Режим доступу: https://ehealth.gov.ua/ – Назва з екрану. – Дата звернення: 10.05.2026.

2 Global strategy on digital health 2020-2025. World Health Organization. [Електронний ресурс]. – Режим доступу: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf – Назва з екрану. – Дата звернення: 10.05.2026.

3 Олійник О. В. Інформаційні технології в медицині та організація захисту медичних даних. Журнал медичної інформатики, 2023. № 2. С. 45-51.

4 The digital transformation of healthcare. [Електронний ресурс]. – Режим доступу: https://www.mckinsey.com/industries/healthcare/our-insights – Назва з екрану. – Дата звернення: 10.05.2026.

5 Healthcare Information Network Architecture: Reference Design Guide [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/healthcare/healthcare_architecture.pdf – Назва з екрану. – Дата звернення: 10.05.2026.

6 Бідюк, О., & Марценко, С. (2025). Методи та засоби інформаційної безпеки іт інфраструктур. Herald of Khmelnytskyi National University. Technical Sciences, 347(1), 47-58. https://doi.org/10.31891/2307-5732-2025-347-6.

7 The information system for planning the parameters of telecommunication operator networks / S. Martsenko et al. 2019 IEEE 14th international scientific and technical conference on computer sciences and information technologies (CSIT), Lviv, Ukraine, 17–20 September 2019. 2019. URL: https://doi.org/10.1109/stc-csit.2019.8929747 (date of access: 12.05.2026).

8 Smart city: a review of model architecture and technology / N. Martsenko et al. 2021 IEEE 16th international conference on computer sciences and information technologies (CSIT), LVIV, Ukraine, 22–25 September 2021. 2021. URL: https://doi.org/10.1109/csit52700.2021.9648606 (date of access: 12.05.2026).

9 Марценко С. В., Круглик Ю. Методи та засоби оптимізації роботи мереж різного призначення. Актуальні задачі сучасних технологій : Матеріали IX міжнар. науково-техн. конф. молодих уч. та студентів «Акт. задачі сучас. технологій» Терноп. нац. техн. ун-ту ім. Ів. Пулюя,, м. Тернопіль, 25–26 листоп. 2020 р. Тернопіль, 2020. С. 48.

10 Information technology platform for the selection and analytical processing of information on COVID-19 / S. Martsenko et al. 2021 IEEE 16th international conference on computer sciences and information technologies (CSIT), LVIV, Ukraine, 22–25 September 2021. 2021. URL: https://doi.org/10.1109/csit52700.2021.9648839 (date of access: 12.05.2026).

11 Марценко С. В., Федина В., Шоцький М. Дослідження процесів автоматизації керування мережевими пристроями. Актуальні задачі сучасних технологій : Матеріали X міжнар. науково-практ. конф. молодих уч. та студентів «Акт. задачі сучас. технологій», м. Тернопіль, 24–25 листоп. 2021 р. Тернопіль, 2021. С. 140.

12 Network functionality [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/topics/computer-science/network-functionality – Назва з екрану. – Дата звернення: 12.05.2026.

13 Functionality of computer networks [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/functionality-of-computer-network/ – Назва з екрану. – Дата звернення: 12.05.2026.

14 Wlan security [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html – Назва з екрану. – Дата звернення: 12.05.2026.

15 Understand web authentication on wireless LAN. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html. – Назва з екрану. – Дата звернення: 12.05.2026.

16 What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 12.05.2026.

17 Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 12.05.2026.

18 Cyber-security-architecture [Електронний ресурс]. – Режим доступу: https://thecyphere.com/blog/cyber-security-architecture/. – Назва з екрану. – Дата звернення: 12.05.2026.

19 «Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco.» [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nacappliance-cleanaccess/product_data_sheet0900aecd802da1b5.html. – Назва з екрану. – Дата звернення: 12.05.2026.

20 Cisco-security-reference-architecture [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/security/cisco-security-reference-architecture.html. – Назва з екрану. – Дата звернення: 12.05.2026.

21 Passwordless authentication [Електронний ресурс]. – Режим доступу: https://www.onelogin.com/learn/passwordless-authentication / – Назва з екрану. – Дата звернення: 12.05.2026.

22 Internet-of-things [Електронний ресурс]. – Режим доступу: https://www.wi-fi.org/discover-wi-fi/internet-of-things – Назва з екрану. – Дата звернення: 12.05.2026.

23 Solution brief vmware cloud packs [Електронний ресурс]. – Режим доступу: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmw-solution-brief-vmware-cloud-packs.pdf – Назва з екрану. – Дата звернення: 12.05.2026.

24 NSX [Електронний ресурс]. – Режим доступу: https://www.vmware.com/products/nsx.html – Назва з екрану. – Дата звернення: 12.05.2026.

25 Industry 5.0 – Towards a sustainable, human-centric and resilient European inustry [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en – Назва з екрану. – Дата звернення: 12.05.2026.

26 What is SD-WAN (Software-Defined Wide Area Network)? [Електронний ресурс]. – Режим доступу: https://www.sdxcentral.com/networking/sd-wan/definitions/software-defined-sdn-wan/ – Назва з екрану. – Дата звернення: 12.05.2026.

27 Cisco Software-Defined WAN (SD-WAN) FAQ [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sw-defined-wan-faq-cte-en.html?dtid=osscdc000283 – Назва з екрану. – Дата звернення: 12.05.2026.

28 Computing theory. [Електронний ресурс]. – Режим доступу: https://www.schoolsofkingedwardvi.co.uk/ks2-computing-computing-theory-5-computer-networks/. – Назва з екрану. – Дата звернення: 10.05.2026.

29 Types of area networks - LAN, MAN and WAN [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/. – Назва з екрану. – Дата звернення: 10.05.2026.

30 What is LAN. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html. – Назва з екрану. – Дата звернення: 10.05.2026.

31 Planning a New Local Area Network: From Start to Finish [Електронний ресурс]. – Режим доступу: https://www.networkcablinglosangeles.com/computer-network-cabling/. – Назва з екрану. – Дата звернення: 10.05.2026.

32 T. King et al., “BLACKHOLE Community,” Internet Engineering Task Force (IETF), 2016. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7999. – Назва з екрану. – Дата звернення: 12.05.2026.

33 A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/.

34 Wieclaw L.; Pasichnyk V.; Kunanets N.; Duda O.; Matsiuk O.; Falat P. Cloud computing technologies in «smart city» projects. In Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Bucharest: Romania, 21–23 September 2017. pp. 339–342.

35 Karnaukhov, O., Duda, O., Martsenko, S., & Yatsyshyn, V. (2023). Cyber-physical systems at “Digital University”. In ITTAP (pp. 306-314).

36 Желібо Є. П., Зацарний В. В. Безпека життєдіяльності : підручник. Київ : Каравела, 2023. 344 с.

37 Атаманчук П. С. Безпека життєдіяльності : навч. посіб. Київ : Центр учбової літератури, 2020. 276 с.

38 Кодекс цивільного захисту України : Закон України від 01.07.2013 р. № 5403-VII (із змінами та доповненнями). [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17 – Назва з екрану. – Дата звернення: 15.06.2026.

39 Фізіологія, гігієна та психологія праці. Електронна система дистанційного навчання ТНТУ [Електронний ресурс]. – Режим доступу: https://dl.tntu.edu.ua/content.php?cid=289144 – Назва з екрану. – Дата звернення: 15.06.2026.

40 Жидецький В. Ц. Охорона праці користувачів комп'ютерів : підручник. Львів : Афіша, 2020. 176 с.