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

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Карпенка Дениса Олеговича
(ПІБ)
академічної групи 123-20-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему "Комп'ютерна система Дніпропетровської обласної лікарні ім. І.І. Мечникова з детальним опрацюванням побудови IoT комплексу палати інтенсивної терапії та налаштуванням корпоративної мережі"
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
спеціальної частини	проф. Цвіркун Л.І.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"25" січня 2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Карпенка Д.О. **академічної групи** 123-20-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)

на тему "Комп'ютерна система Дніпропетровської обласної лікарні ім. І.І. Мечникова з детальним опрацюванням побудови IoT комплексу палати інтенсивної терапії та налаштуванням корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.05.2022 № 771-л

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2024
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2024
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2024
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2024

Завдання видано _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.01.2024

Дата подання до екзаменаційної комісії 23.06.2024

Прийнято до виконання _____ Карпенко Д.О.

РЕФЕРАТ

Пояснювальна записка: 97 с., 39 рис., 9 табл., 1 дод., 8 джерел.

КОМП'ЮТЕРНА СИСТЕМА, ІНТЕРНЕТ РЕЧЕЙ, ЛІКАРНЯ, МАРШРУТИЗАТОР, КОМУТАТОР, CISCO, CISCO PACKET TRACER, NAT, VPN, DHCP, VLAN.

Об'єкт дослідження - комп'ютерна система Дніпропетровської обласної лікарні ім. І.І. Мечникова, з акцентом на створенні IoT-комплексу для палати інтенсивної терапії та налаштуванні корпоративної мережі.

Мета роботи - розробка комп'ютерної системи для Дніпропетровської обласної лікарні ім. І.І. Мечникова.

Було створено гнучку та адаптивна комп'ютерну мережу, що може бути легко перепрограмована та модернізована, з урахуванням потреб лікарні ім. І.І. Мечникова.

Система дозволяє здійснювати як технічну, так і програмну модернізацію. Лікарня складається з декількох відділень: ІТ-відділ, бухгалтерія, відділ кадрів, відділ маркетингу, амбулаторні та лабораторні підрозділи, відділення інтенсивної терапії.

Розроблена комп'ютерна мережа виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Розроблена схема мережі виконана та перевірена за допомогою програми Cisco Packet Tracer.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках.

ЗМІСТ

ВСТУП

У сучасному світі комп'ютерні системи медичних установ відіграють ключову роль у забезпеченні якісної та ефективної медичної допомоги. Дніпропетровська обласна лікарня ім. І.І. Мечникова, як один із провідних медичних закладів України, активно впроваджує сучасні інформаційні технології для покращення рівня медичних послуг. У цьому контексті розробка та впровадження Інтернету речей (IoT) у палатах інтенсивної терапії та налаштування корпоративної мережі стають важливими кроками на шляху до модернізації лікарні та покращення якості медичної допомоги.

Сьогодні провідні наукові установи та організації по всьому світу активно досліджують та впроваджують IoT технології в медичній галузі. До таких установ належать Інститут інженерів з електротехніки та електроніки (IEEE), який проводить дослідження IoT для медицини, а також Массачусетський технологічний інститут (MIT), де ведуться передові дослідження в галузі медичних пристроїв та систем. Видатні вчені, такі як Кевін Ештон, який вперше ввів термін "Інтернет речей", та Раджів Гупта, відомий своїми дослідженнями в області IoT, зробили значний внесок у розвиток цієї сфери.

Глобальні тенденції в розвитку IoT технологій для медицини спрямовані на:

- підвищення точності діагностики;
- покращення моніторингу пацієнтів;
- оптимізацію роботи медичного персоналу.

Актуальність даної кваліфікаційної роботи обумовлена необхідністю вдосконалення медичних послуг в Україні та підвищення рівня безпеки пацієнтів у палатах інтенсивної терапії. Впровадження IoT комплексу дозволить забезпечити цілодобовий моніторинг стану пацієнтів, оперативне реагування на зміни їхнього стану та покращить взаємодію між медичними працівниками.

Метою роботи є розробка та впровадження IoT комплексу для палати інтенсивної терапії у Дніпропетровській обласній лікарні ім. І.І. Мечникова, а також налаштування корпоративної мережі для забезпечення ефективного та безпечного обміну даними. Реалізація даної системи сприятиме підвищенню якості медичних послуг, зниженню ризиків для пацієнтів та оптимізації роботи медичного персоналу.

Ця робота тісно пов'язана з іншими кваліфікаційними дослідженнями, що спрямовані на вдосконалення медичних технологій та інформаційних систем. Зокрема, вона може бути частиною більш широкого проекту, що включає розробку інтелектуальних систем діагностики, автоматизацію процесів обробки медичної інформації та інтеграцію різних медичних систем в єдину інформаційну мережу лікарні.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної мережі

Галузь комп’ютерних мереж, особливо в медичних установах, є однією з найважливіших і найбільш динамічних сфер сучасної інформатики. У медичній сфері комп’ютерні мережі виконують критично важливі функції, забезпечуючи оперативний обмін інформацією між різними підрозділами лікарні, моніторинг стану пацієнтів, управління медичними пристроями та захист медичних даних.

Мережеві технології дозволяють медичному персоналу безперервно відстежувати життєво важливі показники пацієнтів, отримуючи доступ до даних з датчиків та медичних пристроїв у режимі реального часу. Це дає можливість вчасно виявляти зміни в стані пацієнта та негайно реагувати на них, що рятує життя і покращує результати лікування.

Комп'ютерні мережі автоматизують багато рутинних завдань, звільняючи час медиків для більш важливих справ, таких як спілкування з пацієнтами та прийняття складних рішень. Наприклад, автоматизовані системи розподілу та зберігання медичних даних забезпечують швидкий доступ до необхідної інформації, що скорочує час на пошук і дозволяє медикам зосередитися на наданні допомоги пацієнтам.

Одним із важливих аспектів застосування комп’ютерних мереж у медицині є Інтернет речей (IoT). У відділеннях інтенсивної терапії IoT дозволяє здійснювати постійний моніторинг життєво важливих показників пацієнтів у реальному часі. Сенсори та медичні пристрої, підключені до мережі, забезпечують безперервний контроль за станом пацієнтів, що дозволяє швидко реагувати на будь-які зміни та запобігати критичним ситуаціям.

Застосування IoT в інтенсивній терапії включає використання різноманітних медичних сенсорів, які контролюють пульс, артеріальний тиск, рівень кисню в крові та інші важливі параметри. Дані з цих сенсорів

передаються в реальному часі на центральний сервер, де аналізуються за допомогою спеціалізованого програмного забезпечення. Це дозволяє медикам отримувати оперативні сповіщення про будь-які відхилення від норми і швидко приймати необхідні заходи.

Крім цього, мережі IoT дозволяють здійснювати дистанційний моніторинг пацієнтів, що є особливо актуальним у випадках, коли пацієнти перебувають вдома або у віддалених медичних установах. Це не тільки підвищує якість медичного обслуговування, але й знижує навантаження на лікарняний персонал та оптимізує використання медичних ресурсів.

Мережа повинна забезпечувати безперервний моніторинг стану пацієнтів, управління медичними пристроями та оперативний обмін інформацією між медичним персоналом. Вся медична інформація, що зберігається та передається в мережі, повинна бути захищена від несанкціонованого доступу, розголошення та інших загроз. Важливими аспектами є захист даних, управління доступом та забезпечення безперебійної роботи мережі.

Захист медичних даних здійснюється за допомогою сучасних методів шифрування, а також систем аутентифікації та авторизації користувачів. Це дозволяє забезпечити конфіденційність і цілісність інформації, зменшуючи ризики витоку даних та несанкціонованого доступу. Управління доступом включає визначення прав доступу для різних категорій персоналу, що дозволяє контролювати, хто і до яких даних має доступ.

Надійність і безперебійність роботи мережі досягаються завдяки використанню резервного копіювання даних, кластеризації серверів та регулярного моніторингу стану мережевого обладнання. Це дозволяє запобігати збоям у роботі системи та забезпечувати постійний доступ до медичної інформації.

Важливим трендом у розвитку медичних комп'ютерних мереж є використання хмарних технологій. Хмарні сервіси дозволяють зберігати та обробляти великі обсяги медичних даних, забезпечуючи їх доступність з будь-

якого місця та пристрою. Це особливо важливо для медичних установ, які мають обмежені ресурси для створення та підтримки власної IT-інфраструктури. Крім того, хмарні технології дозволяють швидко масштабувати систему відповідно до потреб лікарні, що є важливим фактором у випадку збільшення кількості пацієнтів або розширення спектру послуг.

Таким чином, сучасні комп'ютерні мережі в медичних установах є важливим інструментом для підвищення ефективності надання медичних послуг, забезпечення безпеки даних та оптимізації роботи медичного персоналу. Інтеграція IoT та інших передових технологій дозволяє значно покращити якість медичної допомоги та швидко реагувати на потреби пацієнтів.

1.2 Характеристика і структура об’єкта впровадження

Дніпропетровська обласна лікарня ім. І.І. Мечникова – це одна з провідних медичних установ України, що надає широкий спектр медичних послуг та має сучасну інфраструктуру для діагностики та лікування пацієнтів. Лікарня функціонує як багатопрофільний медичний центр, забезпечуючи пацієнтів висококваліфікованою медичною допомогою у різних напрямках.

Лікарня складається з різних відділень, включаючи стаціонарні та амбулаторні підрозділи, лабораторії, діагностичні центри та адміністративні приміщення. Відділення інтенсивної терапії (ВІТ) є одним з ключових підрозділів лікарні, де пацієнти потребують постійного моніторингу та інтенсивного догляду. Це відділення оснащене сучасним медичним обладнанням та системами моніторингу, що забезпечують високий рівень медичної допомоги.

Палати інтенсивної терапії є ключовим елементом лікарні, призначеним для надання невідкладної та критично важливої медичної допомоги пацієнтам у важкому стані. Кожна палата обладнана спеціальними медичними пристроями та моніторами, які слідкують за життєво важливими показниками

пацієнтів. Ці палати оснащені різноманітними датчиками та приладами для контролю за станом здоров'я пацієнтів, такими як кардіомонітори, оксиметри, апарати для штучної вентиляції легенів та інші життєво важливі системи.

Адміністративні приміщення включають кабінети управлінського персоналу, бухгалтерію, відділ кадрів та інші підрозділи, що забезпечують ефективне управління лікарнею. Ці приміщення є важливими для організації та координації роботи всіх підрозділів лікарні, забезпечуючи їх безперебійну роботу.

Амбулаторні підрозділи забезпечують первинну медичну допомогу та діагностику для пацієнтів, які не потребують госпіталізації. Вони включають кабінети лікарів різних спеціальностей, де проводяться консультації, огляди та первинні діагностичні процедури.

Централізований серверний центр є основою інформаційної інфраструктури лікарні, забезпечуючи зберігання, обробку та передачу медичних даних. Він включає сервери, мережеве обладнання, системи зберігання даних та інші компоненти, що забезпечують стабільну та безперебійну роботу всієї інформаційної системи лікарні.

Організаційна структура лікарні відображена на рисунку 1.1, що показує взаємозв'язок між різними підрозділами та їхніми функціями.

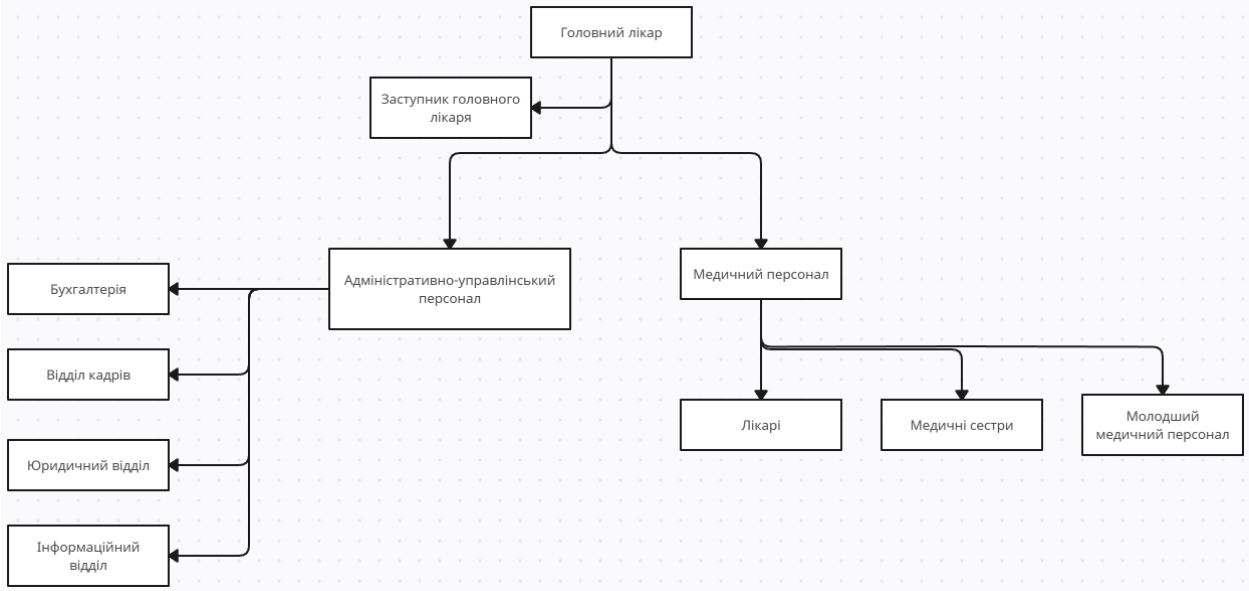

Рисунок 1.1 - Організаційна структура підприємства

Об’єкт впровадження комп’ютерної мережі знаходиться за адресом: 49005, м. Дніпро, пл. Соборна, 14. На рисунку 1.2 представлена схема гео-розміщення лікарні, що ілюструє розташування основних корпусів та відділень на території лікарні.

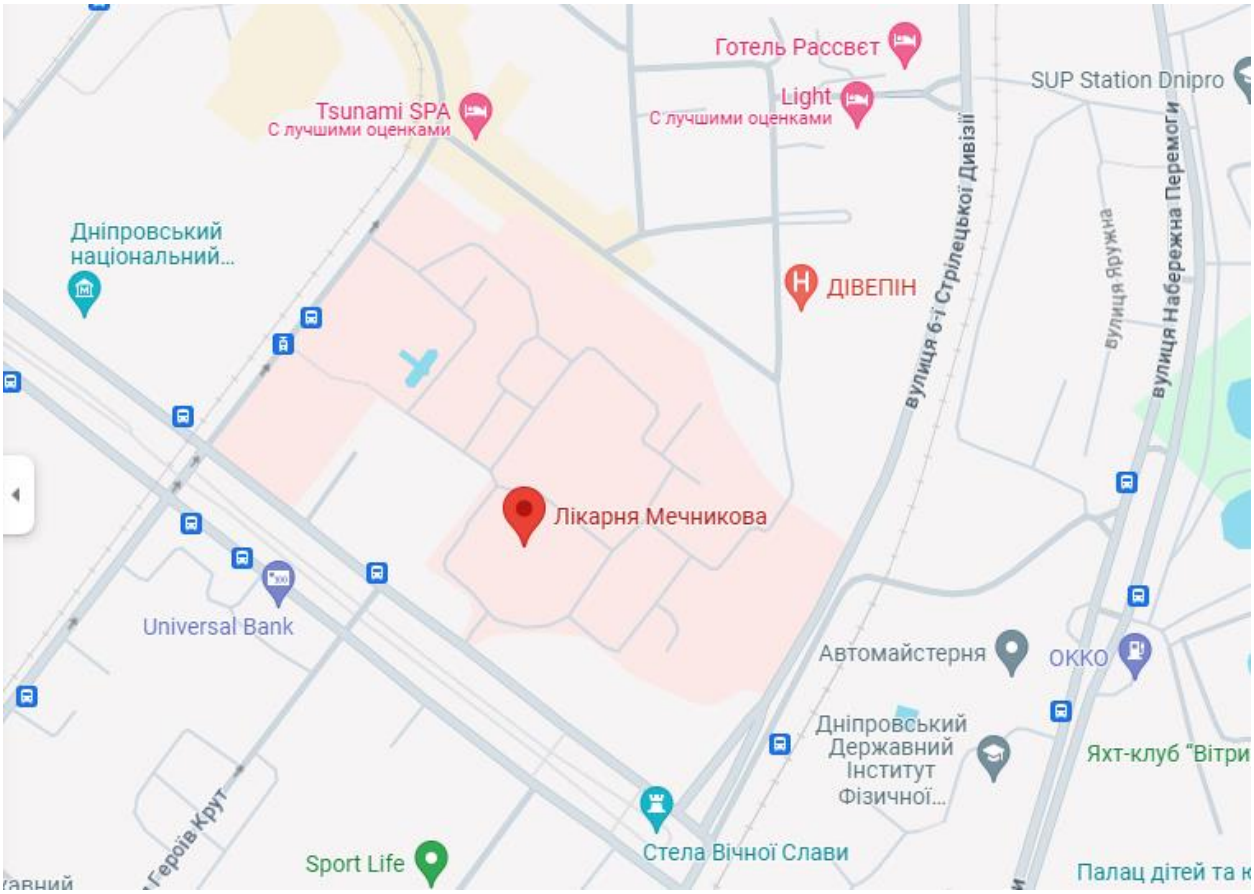

Рисунок 1.2 - Схема гео-розміщення

1.3 Стислі відомості про технологію керування для об’єкта впровадження.

Основна мета впровадження інформаційних технологій – створити надійну і безпечну інформаційну інфраструктуру, яка дозволить забезпечити безперервний збір, обробку та передачу даних. Це значно підвищить ефективність надання медичних послуг, забезпечить високий рівень моніторингу та догляду за пацієнтами, а також оптимізує управління всіма процесами в лікарні.

Комп'ютерна мережа Дніпропетровської обласної лікарні ім. І.І. Мечникова – це не просто набір кабелів та комп'ютерів, а справжнє серце, що забезпечує безперебійну роботу всієї установи. Вона складається з 5 підрозділів.

Мережа організована так, щоб кожен відділ, кожен кабінет мав безперебійний доступ до інформації, необхідної для порятунку життів та надання якісної медичної допомоги.

Для ефективного управління цією складною мережею застосовуються різноманітні технології. Протоколи маршрутизації, такі як OSPF та BGP, визначають оптимальні шляхи передачі даних, забезпечуючи їх швидку та надійну доставку. Системи моніторингу та аналізу дозволяють відстежувати стан мережі в режимі реального часу, виявляти потенційні проблеми та аналізувати трафік для прийняття обґрунтованих рішень щодо її оптимізації.

Надійність та безперебійність роботи мережі є критично важливими, оскільки від цього залежить життя та здоров'я пацієнтів. Тому використовуються резервні канали зв'язку, системи безперебійного живлення та інші заходи, що забезпечують стабільну роботу мережі навіть у разі виникнення непередбачуваних ситуацій.

Крім того, особлива увага приділяється захисту медичних даних. Використання сучасних методів шифрування, систем аутентифікації та авторизації, а також міжмережевих екранів та систем виявлення вторгнень допомагає забезпечити конфіденційність та цілісність медичної інформації, мінімізуючи ризики несанкціонованого доступу та витоку даних.

Централізований серверний центр є критичним вузлом для зберігання та обробки всіх даних лікарні. Він повинен бути облаштований відповідно до вимог безпеки та надійності.

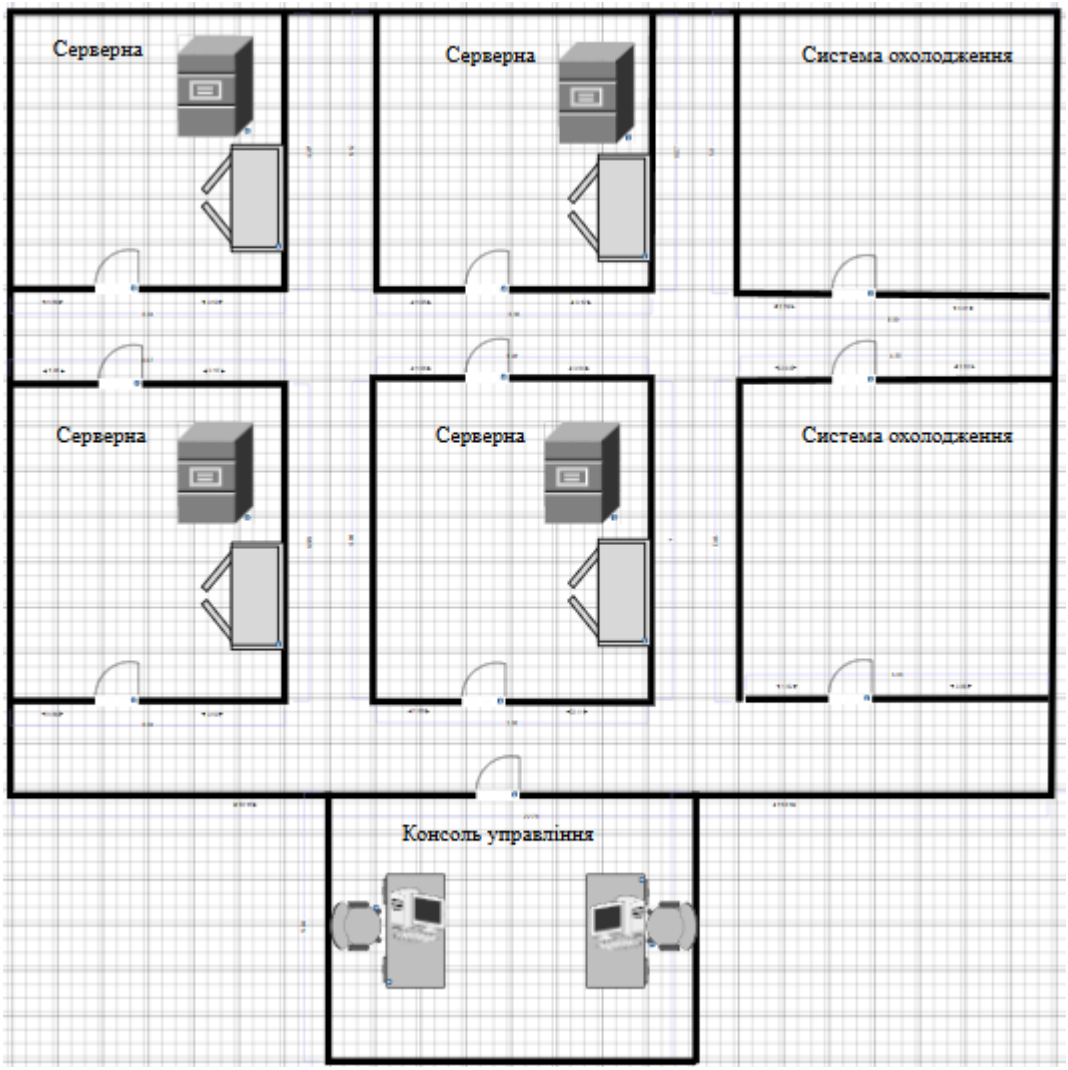

Рисунок 1.3 – схема централізованого серверного центру

Відділення інтенсивної терапії включає окремі палати для пацієнтів, обладнані сучасними медичними пристроями, та центральний пункт для медичного персоналу. Кожна палата оснащена датчиками та моніторами, які відстежують життєво важливі показники пацієнтів у режимі реального часу. Дані з цих пристроїв передаються до центрального сервера для подальшої обробки та аналізу.

Рисунок 1.4 – схема відділення інтенсивної терапії

Амбулаторні підрозділи забезпечують консультативну та діагностичну допомогу пацієнтам, які не потребують госпіталізації. Це включає поліклініки та спеціалізовані кабінети. Мережа забезпечує швидкий доступ до медичних записів пацієнтів, результатів діагностичних тестів та іншої важливої інформації, необхідної для надання якісної медичної допомоги.

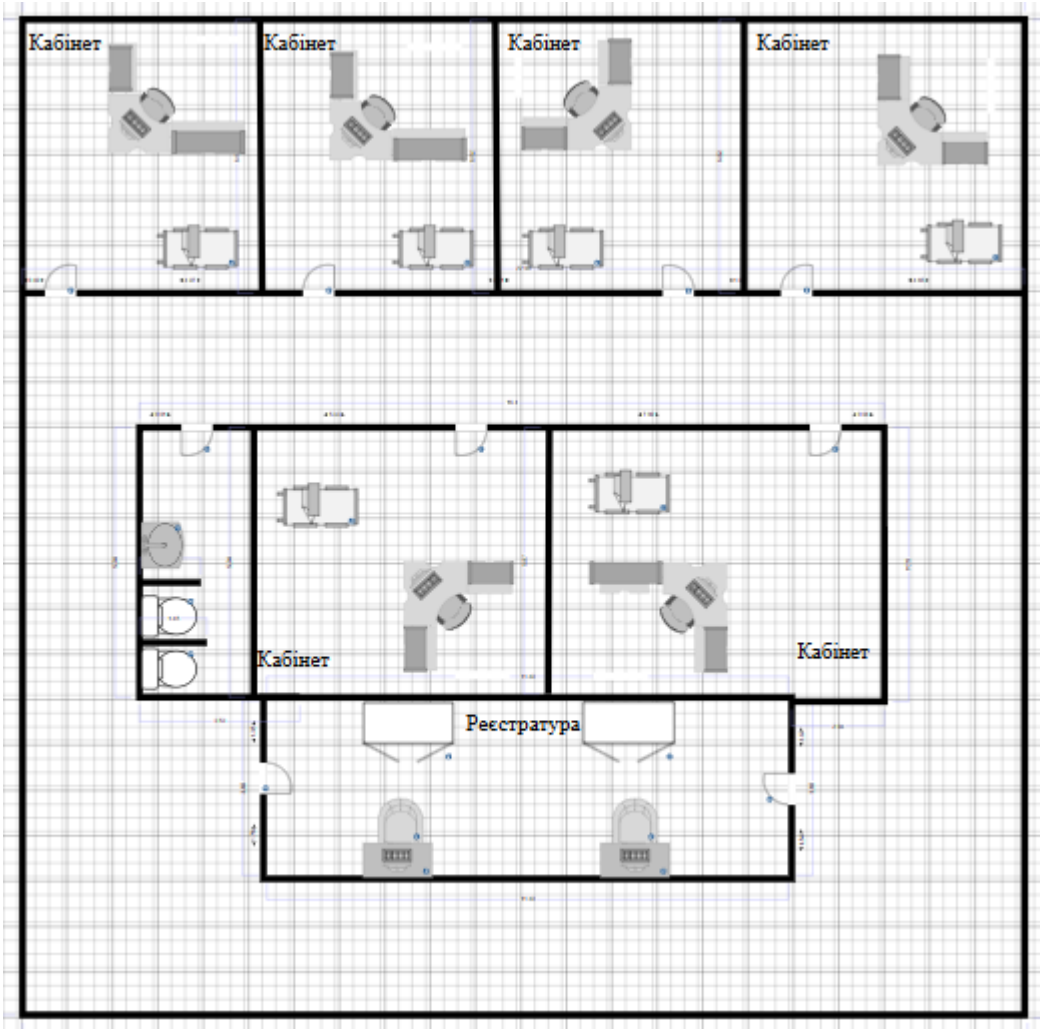

Рисунок 1.5 – схема приміщення амбулаторних підрозділів

Адміністративні приміщення включають офіси для управлінського персоналу, відділи кадрів, фінансові служби та інші підрозділи, що забезпечують ефективне функціонування лікарні. Інформаційна мережа в адміністративних приміщеннях підтримує управлінські процеси, фінансовий облік, управління персоналом та інші адміністративні функції, забезпечуючи при цьому високий рівень захисту даних.

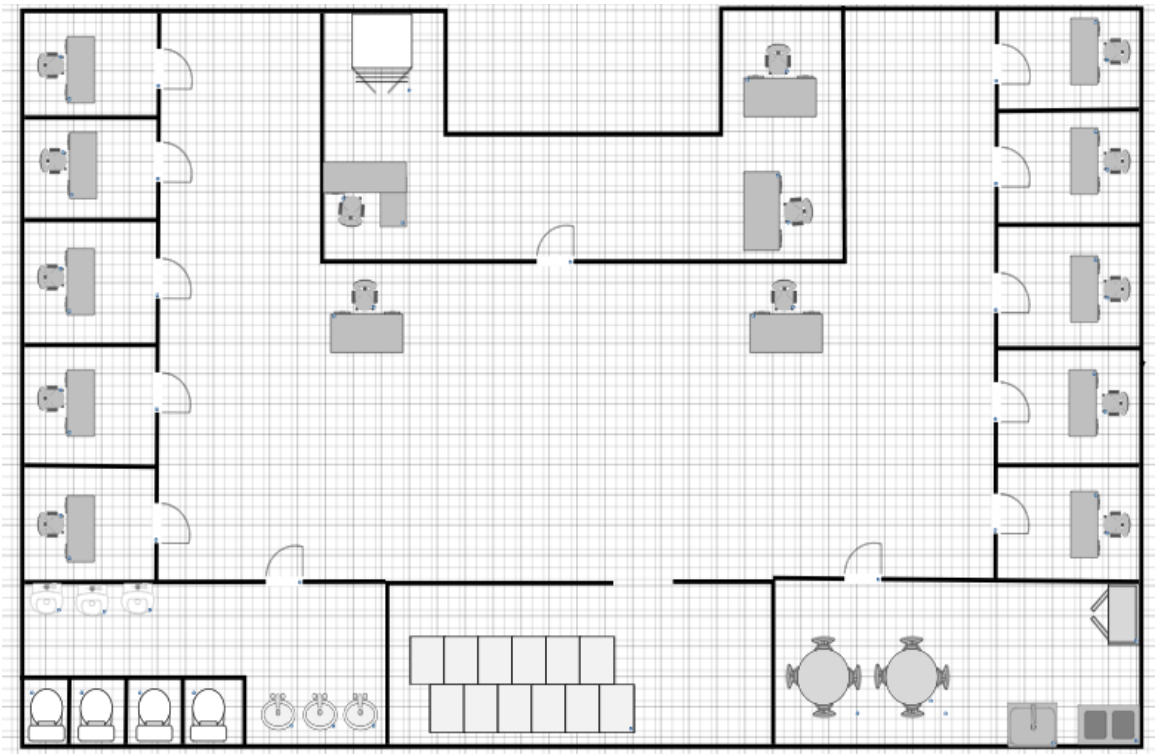

Рисунок 1.6 – схема приміщення адміністративних підрозділів

Комп'ютерна мережа лікарні забезпечує не тільки зручний доступ до даних для медичного персоналу, але й високий рівень захисту медичної інформації. Використовуються сучасні методи шифрування, системи аутентифікації та авторизації, що забезпечують конфіденційність і цілісність медичних даних. Завдяки цьому можна запобігти несанкціонованому доступу до інформації та забезпечити її безпеку.

1.4 Принципи та технічні методи керування об’єкта впровадження

Ефективне функціонування лікарні ґрунтується на сучасних принципах та технічних методах управління, що забезпечують злагоджену роботу всієї системи. Основними аспектами цього процесу є автоматизація, інтеграція, безпека та безперервний моніторинг:

Інтеграція: Всі підсистеми лікарні, включаючи медичні пристрої, інформаційні системи, бази даних та комунікаційні мережі, об'єднуються в єдину платформу. Це гарантує безперебійну взаємодію між відділами та оптимізує загальну роботу. Наприклад, інтеграція лабораторних інформаційних систем з електронними медичними записами дозволяє лікарям

швидко отримувати результати аналізів та ухвалювати обґрунтовані рішення щодо лікування.

Автоматизація: Рутинні завдання, такі як моніторинг стану пацієнтів, ведення медичних записів, управління ресурсами та комунікація між відділами, автоматизуються. Це зменшує навантаження на медичний персонал та мінімізує людський фактор у цих процесах. Автоматизація також сприяє більш точному та швидкому обробленню даних, що є критично важливим у медичних умовах.

Безпека даних: Захист медичної інформації є пріоритетним завданням. Використовуються сучасні методи шифрування, аутентифікації та авторизації для гарантування конфіденційності та цілісності даних. Наприклад, впровадження багатофакторної аутентифікації (MFA) забезпечує додатковий рівень захисту при доступі до критичних систем та даних.

Безперервний моніторинг: Постійне спостереження за станом системи дозволяє вчасно виявляти та усувати проблеми, а також гарантувати високу якість медичних послуг. Це стосується як моніторингу стану пацієнтів, так і контролю за роботою технічних систем. Наприклад, система моніторингу мережевої інфраструктури дозволяє оперативно виявляти збої та запобігати простою медичних інформаційних систем.

Технічними методами керування є:

- системи управління базами даних: Вони забезпечують зберігання, організацію та доступ до великого обсягу медичних даних. СУБД дозволяють проводити складні запити та аналізувати інформацію, що є важливим для медичного обслуговування та управління лікарнею;
- мережеві технології: Високошвидкісні та надійні мережеві технології забезпечують обмін даними між різними підрозділами лікарні. Використання Wi-Fi, Ethernet та інших мережевих протоколів дозволяє забезпечити постійний доступ до необхідної інформації;

- інтернет речі (IoT): IoT-пристрої забезпечують збір даних у режимі реального часу з медичних приладів, сенсорів та моніторів. Ці дані передаються через мережу для подальшої обробки та аналізу. Наприклад, IoT-пристрої у палатах інтенсивної терапії дозволяють безперервно моніторити життєво важливі показники пацієнтів;
- хмарні технології: Хмарні сервіси забезпечують зберігання та резервне копіювання даних, доступ до яких можливий з будь-якого місця. Використання хмарних технологій також дозволяє масштабувати ресурси в залежності від потреб лікарні, забезпечуючи гнучкість та надійність інформаційної системи.

Всі перелічені методи та принципи інтегруються в єдину систему, що гарантує комплексне управління лікарнею. Наприклад, дані з IoT-пристроїв передаються через мережу до СУБД, де вони обробляються та зберігаються. Хмарні технології забезпечують резервне копіювання цих даних, гарантують їх доступність та захист. Інтеграція різних технологій та систем дозволяє створити ефективну, надійну та безпечну інформаційну інфраструктуру, що підвищує якість медичних послуг та покращує результати лікування пацієнтів.

1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об’єкта проектування, відомих рішень у галузі, що розглядається, або в інших галузях

У сучасному світі медицина все більше покладається на інформаційні технології. Різноманітні системи та методи використовуються для збору, обробки та передачі важливих медичних даних, що значно підвищує ефективність медичних послуг та полегшує роботу медичного персоналу.

Традиційні бази даних SQL, такі як MySQL, PostgreSQL та Microsoft SQL Server, ідеально підходять для зберігання структурованої інформації, наприклад, електронних медичних карток пацієнтів. Вони дозволяють

зберігати великі обсяги даних, забезпечують швидкий доступ до інформації та можливість виконувати складні запити для аналізу медичних даних.

Завдяки Amazon Web Services, Microsoft Azure та іншим хмарним платформам, медичні установи отримують гнучкі та масштабовані рішення для зберігання та обробки даних. Хмарні технології дозволяють легко масштабувати ресурси, забезпечують високу доступність даних та надійний захист інформації.

Інструменти на кшталт Hadoop та Apache Spark допомагають виявляти важливі закономірності в медичних даних, що сприяє розвитку досліджень та покращенню лікування. Вони дозволяють обробляти великі обсяги даних, проводити аналітику в реальному часі та отримувати цінні інсайти для прийняття медичних рішень.

Для передачі інформації використовують:

- провідні мережі (Ethernet): Забезпечують швидку та надійну передачу даних між різними пристроями в лікарні. ;
- бездротові мережі (Wi-Fi): Дозволяють медичному персоналу бути мобільним та мати доступ до інформації з будь-якого місця;
- віртуальні приватні мережі (VPN): Гарантують безпечний доступ до лікарняної мережі ззовні, що особливо важливо для віддаленої роботи та консультацій;
- мобільні мережі (5G): Відкривають нові можливості для передачі даних з мобільних пристроїв та медичних датчиків у режимі реального часу. VPN технології забезпечують шифрування даних та захищають інформацію від несанкціонованого доступу під час її передачі через Інтернет.

Проектування медичних систем базується на кількох ключових принципах. Модульність забезпечує можливість легко оновлювати або замінювати окремі частини системи без впливу на інші компоненти. Це дозволяє інтегрувати нові технології та розширювати функціональні можливості.

Інтероперабельність гарантує сумісність всіх компонентів системи та їхню здатність до взаємодії незалежно від виробника. Це забезпечує ефективний обмін даними між різними підсистемами, такими як лабораторні інформаційні системи, електронні медичні записи та системи управління медичними пристроями.

Безпека є критично важливою складовою, що включає шифрування даних, контроль доступу, аудит та моніторинг безпеки, забезпечуючи високий рівень захисту даних на всіх етапах їх обробки та передачі. Важливість безпеки особливо актуальна для медичних закладів, де конфіденційність медичних даних є критично важливою.

Масштабованість дозволяє системі зростати разом з потребами лікарні, забезпечуючи ефективну роботу без зниження продуктивності. Надійність досягається за рахунок резервування, кластеризації та регулярного резервного копіювання даних, що забезпечує високу доступність і стійкість до збоїв.

Надійність досягається за рахунок резервування, кластеризації та регулярного резервного копіювання даних, що забезпечує високу доступність і стійкість до збоїв. Надійні системи гарантують безперервну роботу медичних інформаційних систем та мінімізують ризик втрати даних.

У медичних установах світу вже успішно впроваджуються сучасні інформаційні системи, що базуються на перерахованих вище принципах та методах. Наприклад, в США використовуються системи електронних медичних записів (EHR) такі як Епіс та Cerner, які інтегрують різноманітні медичні дані та забезпечують доступ до них у режимі реального часу.

У Європі багато лікарень впроваджують телемедичні рішення, що дозволяють проводити дистанційні консультації та моніторинг пацієнтів. Це особливо актуально в умовах пандемії COVID-19, коли дистанційне надання медичних послуг стало необхідністю.

Сучасні технології обробки та передачі інформації відкривають нові горизонти для розвитку медицини. Впровадження таких рішень, як у Дніпропетровській обласній лікарні ім. І.І. Мечникова, може значно

покращити якість медичної допомоги та зробити її більш доступною для пацієнтів.

1.6 Аналіз ризиків та обмежень

Впровадження комплексної комп'ютерної системи неминуче пов'язане з певними технічними ризиками. Насамперед, це можливість виникнення проблем сумісності між різними компонентами обладнання та програмного забезпечення. Необхідно враховувати, що медичне обладнання часто має специфічні вимоги до підключення та взаємодії з інформаційними системами.

Для мінімізації цього ризику необхідно провести ретельний аналіз сумісності всіх компонентів системи ще на етапі проектування. Використання відкритих стандартів та протоколів, а також проведення тестування сумісності допоможуть уникнути проблем під час впровадження.

Крім того, існує ризик відмов та збоїв у роботі системи, які можуть призвести до втрати даних або порушення функціонування медичних приладів. Важливо також передбачити можливість масштабування та розширення системи у майбутньому, щоб вона могла адаптуватися до зростаючих потреб лікарні.

Для забезпечення безперебійної роботи системи необхідно передбачити резервування критичних компонентів (серверів, комунікаційного обладнання), а також розробити плани аварійного відновлення. Регулярне технічне обслуговування та моніторинг стану системи також допоможуть запобігти відмовам та збоям.

Впровадження нових технологій завжди вимагає змін у робочих процесах та адаптації персоналу. Тому існує ризик опору з боку співробітників, які можуть бути не готові до навчання та використання нових інструментів.

Недостатня кваліфікація персоналу також може стати перешкодою для ефективного використання системи. Крім того, впровадження та підтримка

комплексної комп'ютерної системи потребує значних фінансових та ресурсних вкладень, що може створити певні труднощі для лікарні.

Для подолання опору персоналу необхідно провести інформаційну кампанію, яка пояснить переваги нової системи та її вплив на роботу співробітників. Важливо також забезпечити навчання персоналу та надати їм необхідну підтримку під час впровадження.

Необхідно розробити програми навчання для персоналу, які охоплюватимуть всі аспекти роботи з новою системою. Також важливо забезпечити постійну підтримку та консультації для співробітників, щоб вони могли ефективно використовувати нові інструменти.

При роботі з медичними даними особливо важливо дотримуватися вимог законодавства щодо їх захисту. Необхідно забезпечити конфіденційність, цілісність та доступність персональних даних пацієнтів, а також вжити заходів для запобігання їх несанкціонованому використанню. Крім того, використання IoT технологій у медичній сфері піднімає ряд етичних питань, таких як право пацієнта на приватність та контроль над своїми даними.

1.7 Критерії оцінки ефективності

Успішна реалізація проекту неможлива без ретельного аналізу потенційних ризиків та обмежень. Технічні ризики, такі як проблеми сумісності обладнання та програмного забезпечення, ризики відмов та збоїв у роботі системи, а також труднощі з її масштабуванням у майбутньому, вимагають особливої уваги. Для їх мінімізації необхідно вже на етапі проектування провести ретельний аналіз сумісності всіх компонентів, використовувати відкриті стандарти та протоколи, а також передбачити резервування критичних елементів системи.

Організаційні ризики, пов'язані з опором персоналу до впровадження нових технологій, недостатньою кваліфікацією співробітників та проблемами з фінансуванням, також потребують вирішення. Для подолання цих труднощів необхідно провести інформаційну кампанію серед персоналу, організувати

навчання та забезпечити постійну підтримку користувачів. Крім того, важливо розробити детальний бізнес-план, який обґрунтує економічну ефективність проекту та дозволить залучити необхідні фінансові ресурси.

Не менш важливим є врахування законодавчих та етичних обмежень. При роботі з медичними даними необхідно суворо дотримуватися вимог законодавства щодо їх захисту, забезпечуючи конфіденційність, цілісність та доступність інформації. Розробка політики безпеки даних та впровадження відповідних технічних заходів є невід'ємною частиною проекту. Крім того, необхідно враховувати етичні аспекти використання IoT технологій у медичній сфері, забезпечуючи прозорість та інформованість пацієнтів щодо використання їхніх даних.

Для оцінки ефективності впровадження комплексної комп'ютерної системи необхідно використовувати як кількісні, так і якісні критерії. Кількісні показники, такі як зниження рівня смертності, скорочення часу на обробку даних та зменшення кількості помилок, дозволять об'єктивно оцінити вплив системи на роботу лікарні. Якісні критерії, такі як підвищення задоволеності пацієнтів та персоналу, покращення якості медичного обслуговування та рівня безпеки даних, допоможуть зрозуміти, наскільки система відповідає очікуванням користувачів та сприяє досягненню стратегічних цілей лікарні.

Очікувані результати від впровадження проекту включають як наукові, так і практичні аспекти. З наукової точки зору, це може бути розробка нових методів та підходів до проектування медичних інформаційних систем, а також аналіз ефективності використання IoT технологій. З практичної точки зору, результатом стане створення готового до впровадження проекту, який дозволить підвищити конкурентоспроможність лікарні, покращити якість медичного обслуговування та забезпечити більш ефективне використання ресурсів.

1.8 Визначення основних етапів реалізації проекту

Реалізація проекту з впровадження комплексної комп'ютерної системи в Дніпропетровській обласній лікарні ім. І.І. Мечникова передбачає кілька послідовних етапів.

На першому етапі, етапі проектування, здійснюється детальна розробка технічного завдання, яке включає в себе визначення функціональних вимог до системи, розробку її архітектури, забезпечення необхідного рівня безпеки та створення зручного інтерфейсу користувача. На цьому етапі також проводиться вибір та обґрунтування технологічних рішень, які будуть використовуватися для реалізації проекту.

Після завершення проектування розпочинається етап впровадження. Він включає закупівлю та встановлення необхідного обладнання, налаштування програмного забезпечення та його інтеграцію з існуючими інформаційними системами лікарні. Важливим аспектом цього етапу є навчання персоналу роботі з новою системою, щоб забезпечити її ефективне використання.

Наступним кроком є етап тестування та налагодження. На цьому етапі проводиться комплексне тестування системи в реальних умовах роботи лікарні. Виявляються та усуваються можливі помилки та недоліки, а також оптимізується робота системи для досягнення максимальної ефективності.

Після успішного завершення тестування система переходить в етап експлуатації та підтримки. На цьому етапі забезпечується безперебійна робота системи, проводиться регулярне технічне обслуговування та оновлення програмного забезпечення. Важливим аспектом є збір та аналіз відгуків користувачів, що дозволяє виявляти потенційні проблеми та вносити необхідні корективи для подальшого покращення системи.

1.9 Завдання і мета роботи

Мета роботи - створити сучасну комп'ютерну систему для Дніпропетровської обласної лікарні ім. І.І. Мечникова, яка зробить життя лікарів та пацієнтів кращим.

Завдяки швидкому збору та аналізу важливих медичних даних система дозволить лікарям приймати обґрунтовані рішення в найкоротші терміни. Автоматизовані системи моніторингу в режимі реального часу забезпечать своєчасне виявлення критичних змін у стані пацієнтів.

Автоматизація рутинних процесів, таких як ведення медичних записів та управління ресурсами, дозволить лікарям зосередитись на наданні медичної допомоги та спілкуванні з пацієнтами, що підвищить загальну якість медичних послуг.

Використання сучасних методів шифрування, аутентифікації та авторизації гарантуватиме конфіденційність та цілісність медичної інформації. Це забезпечить доступ до даних тільки уповноваженим особам, мінімізуючи ризик несанкціонованого доступу.

Для досягнення мети, потрібно провести огляд та аналіз наявних комп'ютерних систем у медичних установах, визначення їхніх сильних сторін та недоліків. Це допоможе виявити найкращі практики та області, які потребують покращення.

Розробка структури комп'ютерної системи, включаючи визначення її компонентів та їх взаємодії. Система повинна включати централізований серверний центр, мережу для відділень інтенсивної терапії, амбулаторних підрозділів та адміністративних приміщень.

Підключення всіх медичних приладів у палатах до комп'ютерної системи для автоматичного збору та аналізу даних. Це дозволить здійснювати постійний моніторинг стану пацієнтів у режимі реального часу.

Об'єднання всіх комп'ютерів у лікарні в єдину мережу, що забезпечить швидкий та безпечний обмін інформацією. Впровадження можливості віддаленої роботи для лікарів через захищені канали зв'язку, такі як VPN.

Ретельне тестування всіх компонентів системи на сумісність та надійність. Навчання персоналу користуванню новою системою та поетапне впровадження її у роботу лікарні.

Запропоновані рішення сприятимуть підвищенню ефективності медичних процесів, що дозволить лікарні вийти на новий рівень якості медичних послуг. Це також покращить імідж лікарні та сприятиме залученню нових пацієнтів.

Успішна реалізація цих завдань забезпечить сучасний рівень медичного обслуговування, що відповідатиме найвищим стандартам. Нова комп'ютерна система допоможе лікарні стати провідним медичним закладом у регіоні, забезпечуючи пацієнтів високоякісною та персоналізованою медичною допомогою.

1.10 Можливі напрямки рішення поставлених завдань

Першочерговим кроком є ретельне проектування та розробка IoT комплексу палати інтенсивної терапії. Це включає вибір оптимальних технологій, таких як датчики, мікроконтролери та протоколи зв'язку, які забезпечать надійний збір, передачу та аналіз медичних даних пацієнтів у режимі реального часу. Важливим аспектом є розробка детальної архітектури комплексу, яка відображатиме взаємодію всіх його компонентів, а також забезпечення надійних механізмів захисту медичної інформації.

Перш за все, необхідно обрати датчики, мікроконтролери, такі як Arduino або Raspberry Pi, вони забезпечать обробку даних з датчиків та їхню передачу на центральний сервер через надійні протоколи зв'язку. Створити схеми взаємодії всіх компонентів IoT комплексу, включаючи датчики, контролери, мережеве обладнання та сервери для обробки та зберігання даних. Особлива увага приділяється питанням масштабованості та відмовостійкості системи. Впровадження сучасних засобів захисту даних, таких як шифрування при передачі та зберіганні, двофакторна аутентифікація для доступу до системи та регулярний аудит безпеки.

Після цього потрібно налаштувати корпоративну мережу лікарні. Розробити сегментацію мережі та налаштувати VLAN, це забезпечить розподіл трафіку між різними підрозділами лікарні, підвищуючи безпеку та

продуктивність мережі. Використання резервних каналів зв'язку, кластеризації серверів та інших методів для гарантування безперебійної роботи мережі. Впровадження рішень для постійного моніторингу мережевої інфраструктури та своєчасного виявлення та усунення проблем.

Потрібно розробити інтерфейси для обміну даними між IoT комплексом та існуючими системами електронних медичних записів (EMR). Використання зібраних даних для автоматизації процесів моніторингу стану пацієнтів, оповіщення медичного персоналу про критичні ситуації та ведення електронних медичних записів.

Зробити аналіз фективності впровадження IoT комплексу. Оцінити показники роботи комплексу, включаючи точність і надійність збору даних, швидкість передачі та обробки інформації. Проаналізувати, як нова система вплинула на ефективність лікування, своєчасність надання медичної допомоги та загальну задоволеність пацієнтів.

1.8 Обґрунтування вибраного напрямку інженерного рішення

Вибір напрямку цієї роботи не випадковий. Він продиктований гострою необхідністю впровадження сучасних технологій у медичну сферу, зокрема у Дніпропетровську обласну лікарню ім. Мечникова. Зростаюча складність медичних процесів і потреба у високоточному та оперативному обміні інформацією вимагають застосування інноваційних підходів, які відповідають сучасним стандартам і викликам.

Створення палати інтенсивної терапії з використанням IoT – це не данина моді, а реальний крок до покращення якості лікування пацієнтів у критичному стані. Безперервний моніторинг життєво важливих показників, миттєве оповіщення лікарів про будь-які відхилення – все це дозволить вчасно реагувати на зміни стану хворого та підвищити шанси на його одужання.

Не менш важливою є і модернізація корпоративної мережі лікарні. Адже надійна та безпечна передача медичних даних – це основа конфіденційності та ефективної роботи всього медичного закладу. Відділення зможуть швидко та

ефективно обмінюватися даними, що сприятиме кращій координації роботи. Лікарі зможуть оперативно отримувати всю необхідну інформацію про пацієнта, що є критично важливим для прийняття обґрунтованих медичних рішень. Автоматизація рутинних завдань звільнить медичний персонал для виконання більш важливих і складних обов’язків, таких як спілкування з пацієнтами та розробка лікувальних планів.

Об'єднання IoT комплексу палати інтенсивної терапії та модернізованої корпоративної мережі в єдину інтегровану систему дозволить створити справжній інформаційний центр лікарні. Кожен лікар матиме під рукою всі необхідні дані, що дозволить приймати більш обґрунтовані рішення. Завдяки точному та оперативному доступу до даних медичний персонал зможе швидко реагувати на зміни стану пацієнтів, що сприятиме покращенню результатів лікування.

Таким чином, обраний напрямок роботи – це не просто технічне завдання, а реальний внесок у розвиток медицини регіону. Впровадження сучасних інформаційних технологій у Дніпропетровську обласну лікарню ім. Мечникова сприятиме підвищенню ефективності медичного обслуговування, зменшенню часу реакції на критичні ситуації та забезпеченню більш високого рівня безпеки пацієнтів. Це можливість зробити лікування в обласній лікарні більш сучасним, ефективним та безпечним для пацієнтів, що в кінцевому рахунку підвищить якість медичних послуг і задоволеність пацієнтів.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонування Системи

2.1.1.1.1 Перелік Підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації Системи

Мережа Дніпропетровської обласної лікарні ім. І.І. Мечникова розділена на п'ять локальних сегментів (підмереж) для оптимізації управління, безпеки та продуктивності:

- LAN_1: амбулаторні підрозділи (51 вузол);
- LAN_2: відділення інтенсивної терапії з детальним опрацюванням побудови IoT комплексу (83 вузла);
- LAN_3: адміністративні підрозділи (90 вузлів);
- LAN_4: віддалена мережа (8 вузлів);
- LAN_5: лабораторні підрозділи (6 вузлів).

В підмережі амбулаторних підрозділів (LAN_1) розташований HTTP сервер, який використовується для розміщення веб-сторінок і надання доступу до них через Інтернет або локальну мережу.

У відділенні інтенсивної терапії (LAN_2) розташовано DNS сервер, о використовується для перетворення доменних імен на IP-адреси і навпаки. Також буде розгорнуто комплекс Інтернету речей (IoT), що об'єднує датчики (диму, вологості, температури), зчитувачі ID-карток та різноманітні пристрої. Це забезпечить:

- безперервний моніторинг стану пацієнтів та параметрів навколишнього середовища;
- автоматизацію процесів управління мікрокліматом та безпекою;
- оперативне реагування на критичні ситуації.

В віддаленій мережі (LAN_4), розташовано TFTP сервер, який використовується для простої і швидкої передачі файлів між пристроями в мережі.

Перевагами сегментованої мережі є:

– Оптимізоване управління: Адміністрування кожної підмережі здійснюється незалежно, що спрощує обслуговування та підвищує ефективність роботи мережі;
– Підвищений рівень безпеки: Можливість застосування індивідуальних політик безпеки для кожної підмережі (брандмауери, VPN) знижує ризики несанкціонованого доступу та витоку даних;
– Збільшена пропускна здатність: Локалізація трафіку в межах підмереж зменшує навантаження на магістральні канали зв'язку та забезпечує швидку передачу даних;
– Масштабованість: Архітектура мережі дозволяє легко додавати нові вузли та підмережі відповідно до потреб лікарні.

LAN_1: забезпечує комунікацію 51 вузла в амбулаторних підрозділах.

LAN_2: забезпечує комунікацію 83 вузлів у відділенні інтенсивної терапії.

LAN_3: забезпечує комунікацію 90 вузлів в адміністративних підрозділах.

LAN_4: віддалена мережа, яка забезпечує комунікацію 8 вузлів.

LAN_5: забезпечує комунікацію 6 вузлів у лабораторних підрозділах.

Загалом Підсистема головного офісу налічує 230 вузлів, а віддалена мережа 8 вузлів.

2.1.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами Системи

LAN_1 (Амбулаторні підрозділи): Застосування технології EtherChannel для об'єднання фізичних каналів зв'язку між комутаторами в єдиний логічний

канал. Це забезпечить збільшення пропускної здатності та підвищення відмовостійкості мережі.

LAN_3 (Адміністративні підрозділи): Впровадження VLAN для логічного розділення фізичної мережі на ізольовані сегменти. Це дозволить підвищити безпеку, оптимізувати управління трафіком та спростити адміністрування мережі.

LAN_4 (Віддалена мережа): Організація захищеного з'єднання з основною мережею за допомогою VPN. Це забезпечить конфіденційність та цілісність даних, що передаються між віддаленими підрозділами та головним офісом.

Використання протоколу динамічної маршрутизації OSPF для автоматичного визначення та оновлення маршрутів між підмережами. Це забезпечить оптимальну доставку пакетів та підвищить ефективність роботи мережі.

Використання технології NAT для забезпечення доступу до Інтернету через провайдера. Це дозволить приховати внутрішні IP-адреси лікарні та підвищити рівень безпеки.

Середовище передачі даних:

– внутрішні мережі: Вита пара для забезпечення гнучкості та економічності підключення;
– між підмережами та віддаленою мережею: оптичне волокно для забезпечення високої швидкості та надійності передачі даних на великі відстані.

Використання бездротової технології Wi-Fi для об'єднання датчиків та пристроїв IoT. Це забезпечить гнучкість розгортання та зручність управління системою.

2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної Системи із суміжними системами

Створена система забезпечує обмін інформацією з іншими медичними системами (Медстар, простоМед, Apteka24, Medcore) шляхом використання поширених форматів медичних даних, таких як: DICOM, HL7, CDA, PDF, XML.

2.1.1.1.4 Вимоги до режимів функціонування Системи

Режими функціонування системи:

- стандартний: Підтримує повноцінну роботу лікарні протягом робочих годин;
- екстрений: Активується у випадку масового надходження пацієнтів або надзвичайних ситуацій, підтримуючи пріоритетне надання невідкладної допомоги;
- резервний: Гарантує безперервну роботу критичних функцій системи навіть при відключенні електроенергії;
- нічний: Зменшує активність системи, обмежуючи або автоматизуючи деякі функції для оптимізації ресурсів;
- обслуговування: Дозволяє проводити технічне обслуговування, ремонт та налаштування компонентів системи з можливим обмеженням функціональності;
- аварійного відновлення: Підтримує відновлення працездатності системи після збоїв або критичних подій.

2.1.1.1.5 Вимоги до діагностування Системи

Процедура діагностування:

- перевірка фізичних підключень (кожні 6 місяці): Візуальний огляд та тестування кабельної системи, перевірка надійності з'єднань мережевих пристроїв;
- аналіз IP-адресації та мережевих налаштувань (кожні 3 місяці): Верифікація коректності присвоєння IP-адрес, перевірка налаштувань мережевих протоколів (TCP/IP, DHCP, DNS тощо);

– тестування пропускної здатності (кожні 3 місяці): Вимірювання швидкості передачі даних у різних сегментах мережі для виявлення вузьких місць та потенційних перевантажень;
– аудит безпеки (раз на рік): Перевірка наявності та актуальності антивірусного програмного забезпечення, налаштувань брандмауерів та інших засобів захисту на всіх комп'ютерах;
– моніторинг мережевих служб (кожен місяць): Тестування доступності та працездатності веб-серверів, серверів баз даних, служб електронної пошти та інших критичних сервісів.

Планове діагностування проводиться фахівцями ІТ-відділу не рідше одного разу на півроку. Позапланове діагностування здійснюється у разі виникнення непередбачуваних збоїв або несправностей.

Метою діагностування є:

– забезпечення стабільної та безперебійної роботи комп'ютерної системи лікарні;
– своєчасне виявлення та усунення потенційних проблем та вразливостей;
– оптимізація продуктивності мережі;
– підвищення рівня захисту інформації та забезпечення кібербезпеки.

2.1.1.1.6 Перспективи розвитку Системи

Напрямки розвитку комп'ютерної системи можуть бути наступними:

– масштабування та адаптація: Забезпечення гнучкості та масштабованості системи для підтримки зростання лікарні та впровадження нових технологій;
– впровадження розумних технологій: Установка датчиків забруднення повітря, витоку води та інших інтелектуальних пристроїв для створення більш безпечного та комфортного середовища для пацієнтів та персоналу;

2.1.1.3 Вимоги до експлуатації

2.1.1.3.1 Умови і регламент (режим) експлуатації, що повинні забезпечувати використання технічних засобів (ТЗ) Системи з заданими технічними показниками

Вимоги до працездатності системи в різних кліматичних умовах:

– температура: від +10°C до +45°C;
– вологість: від 40% до 80% (при +10°C);
– атмосферний тиск: від 84 кПа до 107 кПа.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Вимоги до електроживлення комп'ютерної системи:

– мережа повинна відповідати стандартам. Напруга в мережі повинна бути 220 В ± 5%, а частота 50 Гц ± 0,2 Гц;
– електропостачання має бути безперебійним для забезпечення стабільної роботи системи.

2.1.1.3.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи

Для забезпечення безперебійної роботи комп'ютерної системи, IT-відділ, що складається з 1 фахівців електротехніків, забезпечує цілодобову підтримку.

Графік роботи IT-відділу розроблений таким чином, щоб завжди на місці були спеціалісти. Співробітники працюють за 8-годинним графіком, чергуючись у змінному режимі для забезпечення цілодобової підтримки.

Понеділок - П'ятниця:

– Денна зміна (9:00 - 17:00): на робочому місці завжди присутні 6 співробітників.
– Вечірня зміна (17:00 - 1:00): на робочому місці завжди присутні 4 співробітники.

– Нічна зміна (1:00 - 9:00): на робочому місці завжди присутні 2 співробітники.

Субота - Неділя:

– Денна зміна (9:00 - 17:00): на робочому місці завжди присутні 4 співробітники.
– Вечірня зміна (17:00 - 1:00): на робочому місці завжди присутні 2 співробітники.
– Нічна зміна (1:00 - 9:00): на робочому місці завжди присутні 2 співробітники.

2.1.1.3.4 Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів

Для забезпечення безперервної роботи комп'ютерної системи лікарні необхідно мати резерв обладнання, що включає два маршрутизатори, два комутатори, один сервер, один IoT-шлюз та п'ять персональних комп'ютерів. Крім того, важливо мати запас кабелю витої пари UTP (не менше 30 метрів) та конекторів RJ-45 (не менше 20 штук).

Зберігання резервного обладнання здійснюється в окремому приміщенні з контрольованим мікрокліматом (температура 18-24 °C, вологість 40-60%), доступ до якого мають лише відповідальні співробітники IT-відділу.

2.1.1.3.5 Вимоги до регламенту обслуговування

Регламент обслуговування комп'ютерної системи лікарні включає наступні види робіт:

– усунення несправностей компонентів системи, яке може бути плановим або невідкладним;
– заміна компонентів на більш сучасні та продуктивні, що здійснюється за необхідності та наявності фінансування;
– постійний контроль за роботою системи, що дозволяє виявляти потенційні проблеми на ранніх стадіях та запобігати збоям.

– регулярні перевірки та профілактичні роботи, що включають зовнішній та внутрішній огляд технічних засобів, перевірку контактних з'єднань, налаштувань та взаємодії елементів системи.

2.1.1.4 Вимоги до патентної чистоти

Забезпечена патентна чистота на території України.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до активного обладнання

Активне обладнання комп'ютерної системи лікарні повинно бути сумісним з іншими компонентами системи та мати пропускну здатність не менше 1 Гбіт/с для швидкого обміну даними без перевантажень.

Для забезпечення безпеки мережі, активне обладнання має базуватися на платформі Cisco IOS, яка надає широкий спектр засобів захисту, а саме шифрування, VPN, брандмауер та контроль доступу.

2.1.1.5.2 Вимоги до кабель-каналів, інформаційним та електричним розеткам

Електричні розетки, встановлені у приміщеннях з підвищеною вологістю, повинні мати клас захисту IP44 або вище, що гарантує їх вологостійкість.

Матеріали, з яких виготовлені розетки, також повинні бути вологостійкими та корозійностійкими, наприклад, ударостійкий пластик. Обов'язковим є заземлення розеток та наявність захисту від перенапруги для мінімізації ризику ураження електричним струмом та пошкодження обладнання.

Кабель-канали, що використовуються для прокладання інформаційних кабелів, повинні забезпечувати надійний захист кабелів від фізичних пошкоджень, бути легкодоступними для монтажу, обслуговування та заміни

кабелів, а також виготовлятися з вогнестійких матеріалів для забезпечення пожежної безпеки.

2.1.1.5.3 Вимоги до комунікаційного обладнання і його розташування

Комунікаційне обладнання комп'ютерної системи лікарні має бути розміщено у спеціальних комутаційних шафах, які забезпечують захист від вологості, пилу та інших зовнішніх впливів. Ці шафи повинні знаходитись у спеціально відведеному технічному приміщенні, оснащеному системами вентиляції, кондиціонування та регулювання вологості для підтримання оптимальних умов роботи обладнання (температура 18-24 °C, вологість 40-60%).

IP-адреси комутаційних шаф знаходяться в діапазоні 10.1.5.1/30 - 10.1.5.18/30.

Кабельні траси, що підводяться до шаф, повинні мати правильну організацію кабелів та бути захищені від зовнішніх впливів. Для запобігання електромагнітних перешкод, кабельні траси повинні бути ізольовані від силових кабелів.

Обладнання в шафах повинно бути надійно закріплене та логічно розташоване для зручної ідентифікації та обслуговування. Корпус комутаційної шафи повинен бути заземлений для забезпечення електричної безпеки. Між пристроями необхідно забезпечити достатній простір для вентиляції та легкого доступу.

2.1.1.5.4 Вимоги до однорідності

Для забезпечення єдності та сумісності компонентів комп'ютерної системи лікарні необхідно дотримуватися таких вимог до однорідності:

- кабелі: у всій мережі використовувати єдиний тип кабелів: виту пару категорії 6A для Ethernet-з'єднань та оптоволоконний кабель OS1 для магістральних ліній;

- з'єднувачі: для підключення Ethernet-кабелів використовувати стандартні конектори типу RJ-45;
- мережеве обладнання: використовувати обладнання одного виробника, наприклад, Cisco, для забезпечення сумісності та спрощення управління мережею;
- протоколи: використовувати стандартні мережеві протоколи, такі як TCP/IP для передачі даних, Ethernet для локальних мереж та Wi-Fi для бездротових з'єднань.

2.1.1.5.5 Вимоги до резервування

Резервні копії даних повинні зберігатися на зовнішніх сховищах, розташованих за межами лікарні. Це дозволить зберегти інформацію у разі фізичного пошкодження будівлі лікарні внаслідок стихійних лих або крадіжки.

Для реалізації такого резервування рекомендується використовувати хмарні сервіси, які забезпечують високий рівень безпеки та доступності даних.

Важливо забезпечити апаратне резервування даних, тобто створення копій на фізичних пристроях, таких як резервні сервери. Це дозволить швидко відновити роботу системи у разі відмови основного сервера.

2.1.2 Вимоги до функцій (задач), виконуваним Системою

Структура мережі:

- LAN_1: амбулаторні підрозділи;
- LAN_2: відділення інтенсивної терапії;
- LAN_3: адміністративні підрозділи;
- LAN_4: віддалена мережа;
- LAN_5: лабораторні підрозділи

Кількість вузлів: 58, 93, 80, 9 та 91 відповідно.

Використовувати адресу 10.23.60.0/22 для підмереж, та 10.1.5.0/24 для маршрутизаторів.

Розрахувати, щоб середня інтенсивність трафіку дорівнювала 145 кадрів/с, а середня довжина повідомлення - 650 байт. Затримка передачі пакету повинна бути не більше 6 мс.

При розробці адресації пристроїв слід враховувати наступні вимоги:

- інтерфейси та підінтерфейси маршрутизаторів: перші можливі адреси;
- комутатори: другі можливі адреси;
- сервери: перша можлива адреса у мережі + 9 + 12.

Базове налаштування конфігурації пристроїв:

- назви пристроїв повинні виглядати як Прізвище студента_тип пристрою_номер пристрою.
- для доступа до консолі та vty використати пароль cisco;
- для доступа до привілейованого режиму використати пароль class;
- розробити індивідуальний банер motd;
- налаштувати протокол ssh;
- при шифруванні даних використовувати ключ rsa завдовжки 1024 біт;
- призначити частоту 128000 на DCE-інтерфейсах маршрутизаторів;
- налаштувати аудит та відправку повідомлень про початок і завершення процесу exec;
- об'єднати фізичні лінії на комутаторах у LAN_1.

При налаштуванні динамічної маршрутизації OSPF необхідно активувати оголошення безпосередньо підключених мереж, але вимкнути автоматичне поширення оновлень маршрутизації у локальні мережі, такі як VLAN. Для спрощення таблиць маршрутизації слід створити та оголосити сумарні маршрути для VLAN мереж іншим маршрутизаторам OSPF.

Важливо встановити еталонну пропускну спроможність 1000 для інтерфейсів Gigabit Ethernet.

На serial-інтерфейсах, що з'єднують з провайдером, пропускна спроможність має бути 128 Кб/с, а вартість метрики – 7500. Це дозволить OSPF враховувати швидкість каналів при виборі оптимальних маршрутів.

На маршрутизаторі, який має пряме підключення до інтернет-провайдера (ISP), потрібно налаштувати статичний маршрут за умовчанням та поширити його через оновлення OSPF. Крім того, на цьому маршрутизаторі слід налаштувати ручне підсумовування маршрутів для зменшення розміру таблиць маршрутизації та спрощення їх обробки.

Налаштування служби AAA:

- використовувати локальну базу даних користувачів дял vty;
- налаштувати RADIUS-аутентифікацію;
- при налаштуванні аутентифікація використати Ключове слово "radius123", обліковий запис "ім'я пристрою" з паролем "admin123".

Налаштування Інтернет-доступу

- використати один провайдер ISP;
- налаштувати на маршрутизаторі динамічний NAT на (пул "Internet", адреси 209.165.200.5-209.165.200.30, список доступу 5);
- налаштувати сервер HTTP для відображення веб-сайту з інформацією про проект при вводі в рядку браузера http://123.dnipro.ua (http://209.165.200.4);
- налаштувати site-to-site IPsec VPN між підмережею підприємства та віддаленою мережею.

Налаштування VLAN та маршрутизації:

- для LAN_3 розробити мережі VLAN з номерами 25, 35, 45, 99, 100.
- присвоїти кожній мережі VLAN відповідну назву Accounting, Resources Department, Guest, Management, Native;

– налаштувати транкові та порти доступу, вимкнути невикористовувані;
– налаштувати на комутаторах з IPv4-адресами з Management VLAN SVI-інтерфейси;
– налаштувати маршрутизацію між мережами VLAN.

Налаштування DHCP:

– налаштувати DHCP-сервер для маршрутизатора між VLAN;
– налаштувати DHCP-пули під назвою "pollvlan№" (№ - номер VLAN), виключити перші 10 адрес, вказати DNS-сервер та шлюз.

Безпека портів:

– надати доступ тільки для двох унікальних пристроїв;
– виконати динамічне розпізнавання та додавання MAC-адреси;
– при порушенні безпеки системи, порт залишається включеним та з’являється повідомлення.

2.1.3 Вимоги до видів забезпечення

2.1.3.1 Вимоги до математичного забезпечення

Вимоги у цьому розділі відсутні.

2.1.3.2 Вимоги до інформаційного забезпечення

Система повинна забезпечувати надійний захист медичних даних пацієнтів, використовуючи контроль доступу.

2.1.3.3 Вимоги до лінгвістичного забезпечення

Для зручності користувачів комп'ютерна система лікарні має бути налаштована на українську мову як основну мову взаємодії з технічним забезпеченням. Проте, враховуючи можливу присутність іноземних пацієнтів та співробітників, система повинна також надавати можливість перемикання на англійську мову.

Сайт клініки, як важлива складова інформаційної системи, також буде доступний українською мовою, що відповідає вимогам законодавства та забезпечує зручність для більшості пацієнтів. Однак, для іноземних відвідувачів сайту буде передбачена можливість перемикання на англомовну версію, що сприятиме доступності інформації для широкої аудиторії.

2.1.3.4 Вимоги до технічного забезпечення

Кожне робоче місце повинно бути оснащене комп’ютером із наступною конфігурацією:

- процесор: мінімум 4 ядра, не менше 2 ГГц;
- оперативна пам'ять: більше 8 ГБ;
- накопичувач: не менше 256 ГБ;
- операційна система: Windows 10 або Windows 11;

Сервер:

- процесор: не менше 1,5 ГГц;
- оперативна пам'ять: більше 8 ГБ.

Комутатор:

- порти: 24 FastEthernet + 1 GigabitEthernet;
- підтримка: Etherchannel, VLAN.

Маршрутизатор:

- порти: 2 GigabitEthernet + 4 EHWIC слоти;
- підтримка: DHCP, NAT, VPN, AAA.

Підтримка Wi-Fi та дистанційного управління для IoT Шлюза.

2.1.3.5 Вимоги до організаційного забезпечення

Для забезпечення належного рівня безпеки та контролю доступу до технічного приміщення, де розташоване обладнання комп'ютерної системи лікарні, розробити вхід до приміщення лише співробітникам ІТ-відділу за допомогою індивідуальних карт-ключів. Для запобігання нештатним

ситуаціям, резервні картки-ключі зберігаються у безпечному місці. Кожен вхід та вихід з приміщення фіксується у спеціальному журналі доступу.

Права доступу співробітників регулярно перевіряються та оновлюються, щоб гарантувати, що лише авторизовані особи мають доступ до технічного приміщення. Весь персонал проходить регулярні інструктажі та навчання з правил безпеки та доступ.

2.1.3.6 Вимоги до методичного забезпечення

Для ефективного управління та експлуатації комп'ютерної системи лікарні необхідно мати повний комплект методичної документації. Це включає детальну структурну схему комплексу технічних засобів, яка відображає всі компоненти системи та їх взаємозв'язки. Також важливо мати топологічну схему корпоративної мережі, що візуально представляє її структуру та підключення між пристроями.

Для зручності адміністрування мережі необхідна таблиця адресації пристроїв, де вказані всі IP-адреси та відповідні їм пристрої. Таблиця специфікації обладнання містить детальну інформацію про характеристики та специфікації кожного компонента системи, що дозволяє швидко знайти необхідні дані для обслуговування та заміни обладнання.

Таблиця специфікації структурованої кабельної мережі та схема розміщення кабельних мереж детально описують кабельну інфраструктуру лікарні, включаючи типи кабелів, конектори та їх розташування. Це важливо для ефективного управління мережею та швидкого усунення можливих проблем.

Інструкції з монтажу та налаштування надають покрокові інструкції щодо встановлення, налаштування та обслуговування обладнання та програмного забезпечення. Регламенти та процедури обслуговування описують порядок проведення регулярних перевірок, моніторингу та оновлення системи.

Плани аварійного відновлення визначають дії, які необхідно вжити у разі виникнення аварійних ситуацій, щоб швидко відновити працездатність системи та мінімізувати втрати даних.

2.2 Розробка апаратної частини системи

Розробка апаратної частини комп'ютерної системи Дніпропетровської обласної лікарні ім. І.І. Мечникова розпочалася з детального аналізу потреб медичного закладу та вивчення особливостей його роботи.

На основі отриманих даних було розроблено загальну архітектуру мережі, яка враховує специфіку кожного відділення та забезпечує надійний зв'язок між ними. Структурна схема комплексу технічних засобів була створена з урахуванням необхідності забезпечення високої продуктивності, масштабованості та безпеки системи.

Для з'єднання маршрутизаторів в комп'ютерній системі лікарні використовуються спеціальні кабелі Serial DTE або крос-кабелі, тоді як для з'єднання маршрутизаторів та комутаторів, а також комп'ютерів з комутаторами, застосовуються прямі кабелі. Щоб забезпечити зв'язок між комутаторами, використовуються крос-кабелі.

Враховуючи розроблену організаційну структуру лікарні, технічні вимоги до системи та особливості розташування її підрозділів, мною була сформована структурна схема комплексу технічних засобів комп’ютерної системи яка зображена рисунку 2.1.

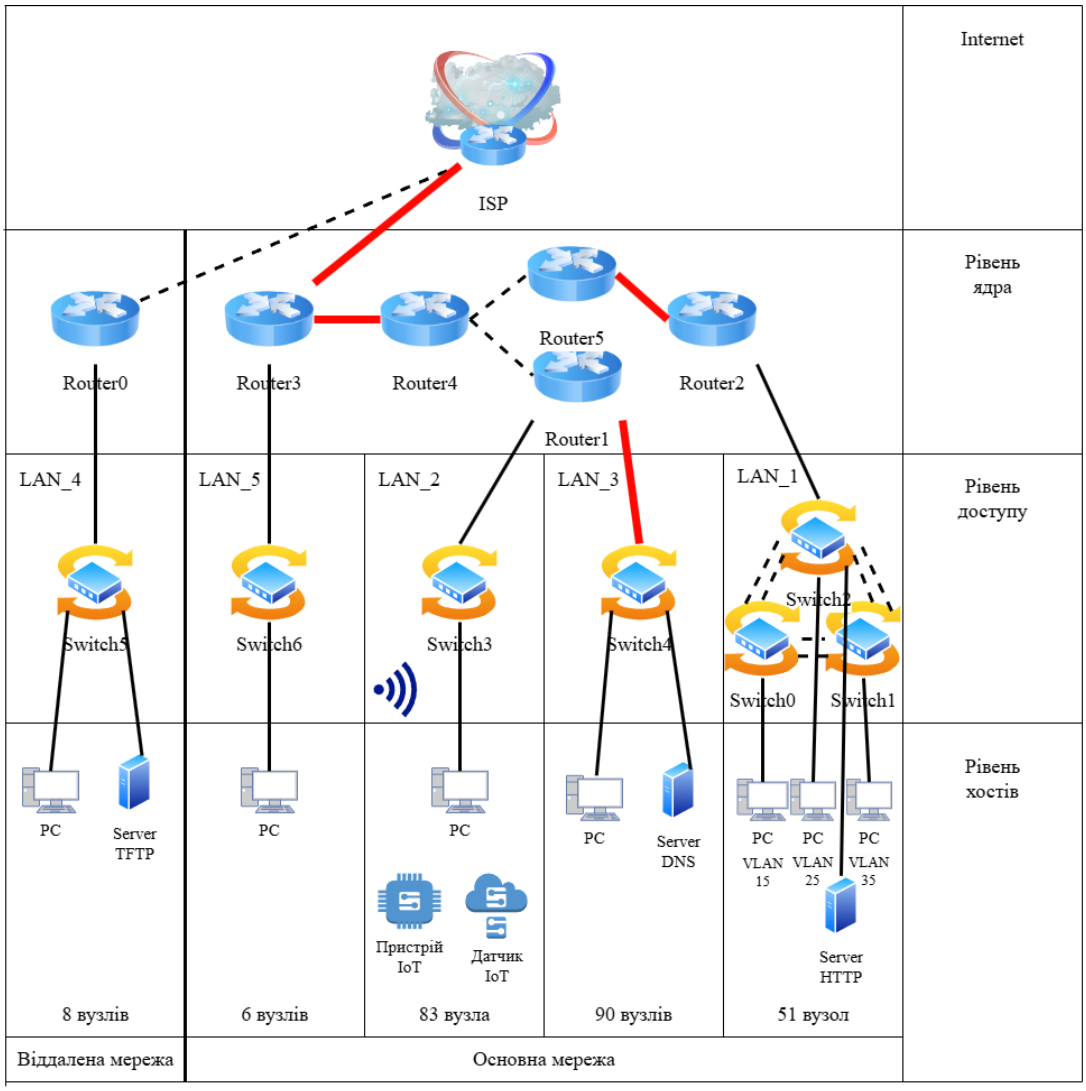

Рисунок 2.1 - Структурна схема комплексу технічних засобів комп’ютерної системи

На основі проведеного аналізу об'єкта проектування, я розробив детальну специфікацію апаратних засобів для комп'ютерної системи лікарні, включаючи необхідні сенсори та пристрої для збору і передачі даних. Її процес включав ретельний вибір фізичного середовища передачі даних, кабелів, портів та з'єднувачів, а також вибір мережевих пристроїв та компонентів, що відповідають технічним вимогам системи.

В таблиці 2.1 наведено специфікація обладнання, а саме кабелі, компоненти, мережеві пристрої, розетки, з'єднувачі. Також наведено їх кількість та модель.

Таблиця 2.1 - Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці вимірy	Кількість	Примітки
1	Комутатор Cisco Catalyst 2960	Switch 2960-24TT	од.	15	З'єднання вузлів комп'ютерної мережі
2	Маршрутизатор Cisco 2811	Router 2811	од.	6	Поєднання мереж та маршрутизація
3	Маршрутизатор Cisco 1941	Router 1941	од.	1	Поєднання мереж та маршрутизація
4	Шлюз IoT	Home Gateway	од.	1	Підключення домашньої мережі
5	DNS сервер	Server-PT	од.	1	Перетворення доменних імен на IP-адреси
6	HTTP сервер	Server-PT	од.	1	Розміщення веб-сторінок
7	TFTP сервер	Server-PT	од.	1	Передача файлів між пристроями в мережі
8	Комп’ютер	PC	од.	239	Опрацювання даних

Продовження таблиці 2.1

9	Кабельний канал 40×25 мм	Sokol	Метри	55	Прокладка
10	LAN-кабель	OK-Net	Метри	60	Підключення локальної мережі
11	WAN-кабель	ОдесКабель	Метри	40	Для підключення маршрутизаторів
12	RJ-45 з'єднувач	EServer	од.	32	Для підключення кабелів Ethernet
13	Розетка	Schneider Electric Asfora	од.	260	Підключення електричних приладів
14	Комутаційна коробка	UA13G	од.	6	Захист з’єднання кабелів
15	Кабель живлення	Gembird	од.	239	Передає електричний струм

Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Пропускна здатність вихідного каналу мережі складає 1000 Мбіт/с. Для запобігання перевантаження каналу, швидкість надходження пакетів повинна бути нижчою за швидкість їх відправлення.

З огляду на середню інтенсивність трафіку 219 кадрів/с та середню довжину повідомлення 650 байт, пропускна здатність мережі LAN2, що складається з 83 вузлів, розраховується наступним чином:

$$P_{р.р.} = \mu * L_{пов} * N * 8 = 219 * 650 * 83 * 8 = 94{,}6194 \text{ Мбіт/с},$$

Де μ=219 кадрів/с (середня інтенсивність трафіку),

$L_{пов}$ = 650 байт (середня довжина повідомлення),

N=83 (кількість вузлів в мережі),

8 - для переведення байтів у біти.

Оскільки отримане значення не перевищує пропускну здатність вихідного каналу (1000 Мбіт/с), перевантаження каналу не очікується. Комутатор рівня доступу передає трафік на маршрутизатор зі швидкістю 1000 Мбіт/с. Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих}= 1000\ 000\ 000/(650*8)=192308 \text{ пакетів/с}$$

З огляду на середню інтенсивність трафіку від кожного джерела (219 пакетів/с), максимальна кількість приєднань, яку може обслуговувати комутатор, становить:

$$N= \mu_{вих}/ \mu= 192308/219= 878 \text{ джерел}$$

Це задовольняє мережу з 83 ПК, тому вимоги до кількості приєднань виконуються. Інтенсивність вихідного трафіку:

$$\lambda=N*\mu=83*219=18177 \text{ пакетів/с}$$

Коефіцієнт затримки та коефіцієнт зайнятості комутатора розраховуються відповідно:

$$\rho=\lambda/\mu_{вих}=18177/192308= 0.0946$$

$$\rho_{зайн}=\rho/(1-\rho)=0.0946/(1-0.0946)=0.1045$$

Середня затримка кадру становлять:

$$T=1/(\mu_{вих}-\lambda)=1/(192308-18177)=5.74 \text{ мкс}$$

Середня довжина черги:

$$L_{чер}= = \rho^2/(1-\rho)=0.0946^2/0.9054=0.00987$$

Середній час перебування пакета у черзі:

$$T_{оч}=L_{чер}/\lambda=0.00987/18177=0.54 \text{ мкс}$$

Оскільки середній час перебування пакета у черзі (0.54 мкс) менше 6 мс, вимоги до затримки також виконуються.

3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

3.1 Розрахунок адресації комп'ютерної мережі

Для забезпечення ефективної роботи мережі лікарні, що складається з 238 користувачів, було проведено розділення мережі 10.24.40.0/21 на п'ять підмереж, використовуючи метод VLSM (маскування підмережі змінної довжини). Цей метод дозволяє оптимально розподілити IP-адреси, враховуючи потреби кожного підрозділу, як показано в таблиці 3.1.

Таблиця 3.1 – Блок адрес мережі та кількість вузлів в кожній підмережі

Блок адрес	LAN1	LAN2	LAN3	LAN4	LAN5
10.24.40.0/21	51	83	90	8	6

Для розподілу мережі 10.24.40.0/21 на п'ять підмереж, необхідно визначити відповідну маску для кожної з них. Оскільки ми працюємо з протоколом IPv4, кількість адрес у підмережі може бути представлена як ступінь двійки (1, 2, 4, 8, 16, 32, 64, 128 або 256). При цьому слід врахувати, що дві адреси (мережева та широкомовна) не можуть бути використані для призначення пристроям.

З метою забезпечення масштабованості мережі та враховуючи кількість вузлів у кожній підмережі, було прийнято рішення про наступний розподіл:

- LAN1 (51 вузол): 64 адреси (маска /26);
- LAN2 (83 вузли): 128 адрес (маска /25);
- LAN3 (90 вузлів): 128 адрес (маска /25);
- LAN4 (8 вузлів): 16 адрес (маска /28);
- LAN5 (6 вузлів): 16 адрес (маска /28).

Для виділення кожної підмережі, адресу мережі було переведено у двійковий формат, і частина, що відповідає вибраній масці, була відокремлена.

На основі визначених потреб кожної підмережі, було виділено наступні блоки адрес:

LAN1: для 51 вузла виділено блок з 64 адрес (10.24.40.0/26), що охоплює діапазон від 10.24.40.1 до 10.24.40.62. Широкомовна адреса підмережі - 10.24.40.63.

LAN2: для 83 вузлів виділено блок з 128 адрес (10.24.40.64/25), що охоплює діапазон від 10.24.40.65 до 10.24.40.126. Широкомовна адреса підмережі - 10.24.40.127.

LAN3: для 90 вузлів також виділено блок з 128 адрес (10.24.40.128/25), що охоплює діапазон від 10.24.40.129 до 10.24.40.190. Широкомовна адреса підмережі - 10.24.40.191.

LAN4: для 8 вузлів виділено блок з 16 адрес (10.24.40.192/28), що охоплює діапазон від 10.24.40.193 до 10.24.40.206. Широкомовна адреса підмережі - 10.24.40.207.

LAN5: для 6 вузлів також виділено блок з 16 адрес (10.24.40.208/28), що охоплює діапазон від 10.24.40.209 до 10.24.40.222. Широкомовна адреса підмережі - 10.24.40.223.

Схема адресації мережі наведена в таблиці 3.2

Таблиця 3.2 – Схема адресації мережі

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN1	51	10.24.40.0	/26	10.24.40.1	10.24.40.62
LAN2	83	10.24.40.64	/25	10.24.40.65	10.24.40.126
LAN3	90	10.24.40.128	/25	10.24.40.129	10.24.40.190
LAN4	8	10.24.40.192	/28	10.24.40.193	10.24.40.206
LAN5	6	10.24.40.208	/28	10.24.40.209	10.24.40.222

Для організації зв'язку між маршрутизаторами було виділено блок адрес 10.1.5.0/24. Застосовуючи метод VLSM, цей блок було розділено на п'ять підмереж, кожна з яких містить два вузли. Детальний розподіл адрес представлено у таблиці 3.3.

Таблиця 3.3 – Схема адресації каналів між маршрутизаторами

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
WAN1	2	10.1.5.0	/30	10.1.5.1	10.1.5.2
WAN2	2	10.1.5.4	/30	10.1.5.5	10.1.5.6
WAN3	2	10.1.5.8	/30	10.1.5.9	10.1.5.10
WAN4	2	10.1.5.12	/30	10.1.5.13	10.1.5.14
WAN5	2	10.1.5.16	/30	10.1.5.17	10.1.5.18

Такий підхід до розподілу адрес забезпечує оптимальне використання IP-адресного простору та дозволяє ефективно масштабувати мережу у майбутньому.

3.2 Розрахунок схеми адресації пристроїв

У таблиці 3.4 детально представлено розраховану схему адресації для всіх маршрутизаторів мережі.

Таблиця 3.4 - Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Інтерфейс підключеного пристрою
Karpenko_Router0	g0/0	64.100.13.0	/30	fa0/0
	g0/1	10.24.40.193	/28	eth6

Продовження таблиці 3.4

Karpenko_Router1	fa0/0	10.24.40.129	/25	fa0/2
	fa0/2/0	10.1.5.1	/30	fa0/0
	se0/3/0	10.24.40.65	/25	eth6
	fa0/1	10.1.5.2	/30	fa0/1
Karpenko_Router2	fa0/0	10.24.40.1	/26	fa0/5
	se0/2/0	10.1.5.5	/30	se0/2/0
Karpenko_Router3	se0/2/0	10.1.5.9	/30	se0/2/0
	se0/2/1	209.165.202.0	/30	se0/2/1
	fa0/0	10.24.40.209	/28	eth6
Karpenko_Router4	se0/2/0	10.1.5.9	/30	se0/2/0
	fa0/0	10.1.5.1	/30	fa0/2/0
	fa0/1	10.1.5.17	/30	fa0/0
Karpenko_Router5	fa0/0	10.1.5.17	/30	fa0/1
	fa0/1	10.1.5.2	/30	fa0/1
	se0/2/0	10.1.5.5	/30	se0/2/0
Karpenko_RouterIPS	fa0/0	209.165.201.5	/28	fa0
	fa0/1	64.100.13.0	/30	g0/0
	se0/2/1	209.165.202.0	/30	se0/2/1

В таблиці 3.5 містяться IP-адреси серверів, які пораховані за формулою (перша адреса підмережі + 9 + № варіанта), 10.24.40.1+9+5=10.24.40.15.

Таблиця 3.5 - Адресація інтерфейсів серверів

Назва серверу	Назва інтерфейсу	IP-адреса	Маска	Шлюз
Karpenko_ServerDNS	Fa0	10.24.40.79	255.255.255.128	10.24.40.65
Karpenko_ServerTFTP	Fa0	10.24.40.206	255.255.255.240	10.24.40.193

Продовження таблиці 3.5

Karpenko_ServerHTTP	Fa0	10.24.40.15	255.255.255.192	10.24.40.1

3.3 Розробка топологічної схеми корпоративної мережі

На рисунку 3.1 представлено топологічну схему корпоративної мережі лікарні, яка складається з основної та віддаленої мережі, а також підключення до мережі інтернет-провайдера. З'єднання між компонентами мережі здійснюється за допомогою кабелів Serial Ethernet та Gigabit Ethernet, що забезпечує високу швидкість передачі даних та надійність зв'язку.

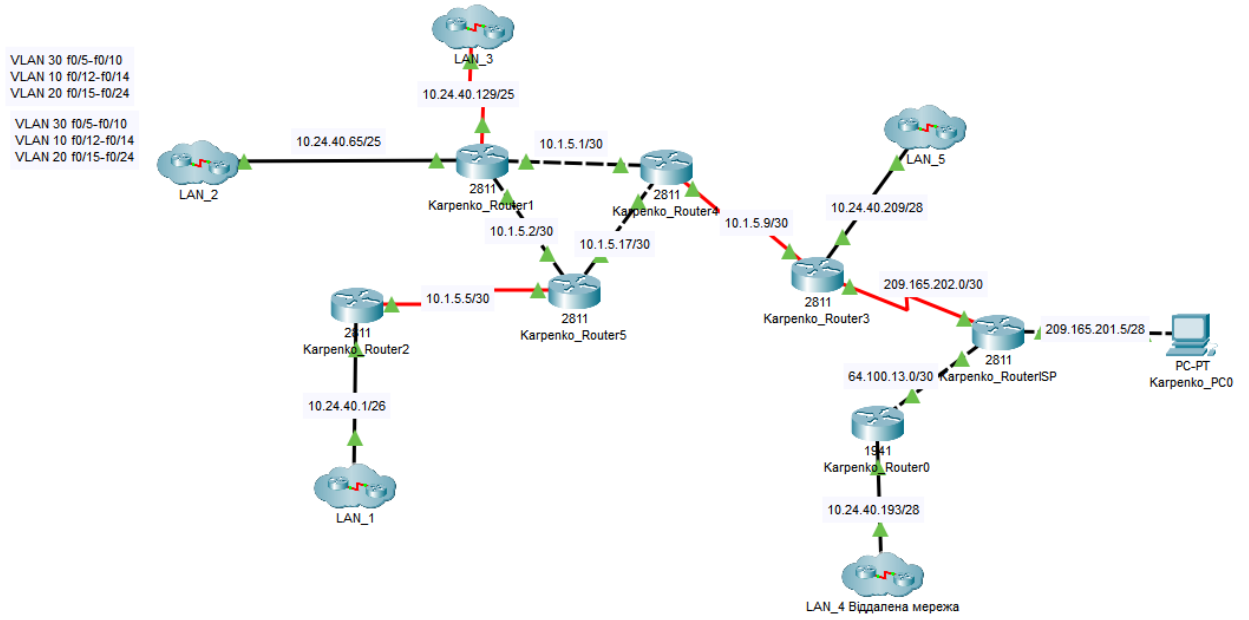

Рисунок 3.1 – Топологічна схема корпоративної мережі

3.4 Налаштування пристроїв комп’ютерної мережі

3.4.1 Налаштування маршрутизаторів

Базове налаштування конфігурації пристроїв на прикладі Karpenko_Router4:

Enable // Перехід у привілейований режим

configure terminal // Перехід у глобальний режим

no ip domain-lookup // Вимкнення DNS-пошуку для неповних команд

hostname Karpenko_Router4 // Встановлення імені хоста маршрутизатора

ip domain-name Karpenko.123-20-1.com // Встановлення доменного імені

crypto key generate rsa // генерації ключів RSA для SSH

1024 // Визначення довжини ключа

username admin secret cisco // Створення користувача "admin" з паролем "cisco"

enable secret class // Встановлення пароля "class" для привілейованого режиму

line console 0 // Перехід до налаштування консолі

password cisco // Встановлення пароля для консольного доступу

login // Вимога вводу пароля для доступу

line vty 0 4 // Перехід до налаштування ліній VTY

login local // Використання локальної аутентифікації

transport input ssh // Дозвіл лише SSH-з'єднань

service password-encryption // Увімкнення шифрування паролів у конфігураційному файлі

interface Serial0/2/0 // Перехід до налаштування інтерфейсу

ip address 10.1.5.9 255.255.255.252 // Призначення IP-адреси та маски підмережі

no shut

Повторення для інтерфейсів fa0/0-1

do copy run start // Збереження поточної конфігурації у файл запуску

3.4.2 Налаштування технології EtherChannel

У локальній мережі LAN_1 застосовується технологія EtherChannel, яка об'єднує кілька фізичних інтерфейсів комутатора в один логічний канал. Це дозволяє значно збільшити пропускну здатність та забезпечити високу надійність каналів зв'язку в мережі.

Розглянемо приклад налаштування EtherChannel на комутаторі Karpenko_Switch0:

interface range fa0/1-2 // Вибираємо діапазон інтерфейсів FastEthernet

channel-group 1 mode active // Додаємо інтерфейси до port-channel 1

interface port-channel 1 // Переходимо до налаштування port-channel 1

switchport mode trunk // Налаштовуємо port-channel 1 як транковий порт

switchport trunk allowed vlan all // Дозволяємо проходження всіх VLAN через port-channel 1

interface range fa0/3-4 // Вибираємо діапазон інтерфейсів FastEthernet

channel-group 2 mode active // Додаємо інтерфейси до port-channel 2

interface port-channel 2 // Переходимо до налаштування port-channel 2

switchport mode trunk // Налаштовуємо його як транковий порт

switchport trunk allowed vlan all // Дозволяємо проходження всіх VLAN через port-channel 2

3.4.3 Налаштування базових маршрутів мережі

Для автоматизації процесу призначення IP-адрес комп'ютерам у мережі лікарні буде застосовано протокол DHCP (Dynamic Host Configuration Protocol). Це дозволить значно спростити адміністрування мережі та зменшити час, необхідний для налаштування нових пристроїв.

Розглянемо приклад налаштування DHCP на маршрутизаторі Karpenko_Router2:

ip dhcp excluded-address 10.24.40.1 10.24.40.3 // Виключаємо адреси з пулу DHCP

ip dhcp excluded-address 10.24.40.15

ip dhcp pool LAN_1 // Створюємо пул DHCP

network 10.24.40.0 255.255.255.192 // Вказуємо мережу для DHCP

default-router 10.24.40.1 // Встановлюємо шлюз за замовчуванням

dns-server 10.24.40.79 // Вказуємо DNS-сервер

В цій мережі використовується динамічна маршрутизація, яка дозволяє автоматично оновлювати маршрути при змінах в топології мережі, забезпечуючи більшу гнучкість та зручність адміністрування.

OSPF визначає найкоротших шляхів передачі даних, що сприяє оптимізації роботи мережі та підвищенню її швидкодії. Розглянемо приклад налаштування протоколу OSPF на маршрутизаторі Karpenko_Router5:

router ospf 1 // Активація протоколу OSPF

network 10.1.5.0 0.0.0.3 area 0 // Визначення мереж в зоні OSPF

network 10.1.5.4 0.0.0.3 area 0

network 10.1.5.8 0.0.0.3 area 0

network 10.1.5.12 0.0.0.3 area 0

network 10.1.5.16 0.0.0.3 area 0

network 10.1.5.18 0.0.0.3 area 0

passive-interface default // Вимкнення OSPF на всіх інтерфейсах за замовчуванням

no passive-interface Fa0/0 // Вмикання OSPF на інтерфейсах

no passive-interface Fa0/1

no passive-interface Se0/2/0

Налаштування маршруту за замовчуванням на маршрутизаторі Karpenko_Router3 до маршрутизатора провайдера ISP:

ip route 0.0.0.0 0.0.0.0 209.165.202.2 // Налаштування маршруту за замовчуванням

router ospf 1 // Активація протоколу OSPF

redistribute static subnets // Функція розповсюдження статичних маршрутів

ip route 209.165.201.0 255.255.255.240 209.165.202.2 // Додається статичний маршрут

3.4.4 Налаштування роботи інтернету

Для забезпечення доступу комп'ютерної системи лікарні до мережі Інтернет використовується технологія NAT.

Пул адрес NAT: 209.165.202.5 – 209.165.202.30.

Для цього на прикордонному маршрутизаторі Karpenko_Router3 налаштовується пул NAT-адрес:

ip access-list extended NAT5 // Створення списку контролю доступу

deny ip 10.24.40.0 0.0.0.63 10.24.40.192 0.0.0.15 // Заборона трафіку між підмережема

deny ip 10.24.40.0 0.0.0.127 10.24.40.192 0.0.0.15

deny ip 10.24.40.128 0.0.0.127 10.24.40.192 0.0.0.15

deny ip 10.24.40.208 0.0.0.15 10.24.40.192 0.0.0.15

deny ip 10.1.5.0 0.0.0.3 10.24.40.192 0.0.0.15

permit ip 10.24.40.0 0.0.0.63 any // Дозвол трафіку з підмережами

permit ip 10.24.40.0 0.0.0.127 any

permit ip 10.24.40.128 0.0.0.127 any

permit ip 10.24.40.208 0.0.0.15 any

permit ip 10.1.5.0 0.0.0.3 any

ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 // Створення пулу NAT з ім'ям Internet

ip nat inside source list NAT5 pool Internet // Зв'язування списку з пулом

ip nat inside source static 10.24.40.15 209.165.200.4 // Надання HTTP-серверу публічної IP-адреси

ip nat inside source static 10.24.40.79 209.165.200.3 // Надання DNS-серверу публічної IP-адреси

interface Serial0/2/1 // Конфігурація інтерфейсу

ip nat outside // Визначення інтерфейсу як зовнішнього

interface Serial0/2/0

ip nat inside // Визначення інтерфейсу як внутрішнього

interface FastEthernet0/0

ip nat inside

3.5 Налаштування безпеки мережі

3.5.1 Налаштування RADIUS-серверу

Для налаштування Radius-серверу, використовується модель AAA. Вона забезпечує ідентифікацію користувачів, авторизацію їх доступу та облік використаних ресурсів.

Потрібно налаштувати всі маршрутизатори в мережі, на прикладі Karpenko_Router5:

aaa new-model // Включення нової моделі AAA

radius-server host 10.24.40.151 auth-port 1645 key radius123 // Налаштування RADIUS-сервера

aaa authentication login console group radius local // Налаштування аутентифікації для консолі

line console 0 // Вхід у режим конфігурації

login authentication console // Застосування методу аутентифікації console

aaa authentication login default local // Налаштування локальної бази даних як методу аутентифікації

username Karpenko_Router5 password admin123 // Створення користувача "Karpenko_Router5" з паролем "admin123"

line vty 0 15 // Вхід у режим конфігурації для ліній VTY

login authentication default // Застосування методу аутентифікації default

3.5.2 Налаштування віртуальних локальних мереж VLAN

Технологія VLAN дозволяє ефективно розділити одну фізичну мережу на кілька віртуальних підмереж, що значно спрощує управління мережею та підвищує її безпеку. У нашому випадку, підмережа LAN_2 була розділена на три VLAN. Номери та назви цих VLAN мереж детально описані в таблиці 3.6.

Таблиця 3.6 - Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
1	default	Не використовується

Продовження таблиці 3.6

15	Accounting	Для бухгалтерії
25	Resources Department	Для відділу кадрів
35	Guest	Для гостей
99	Management	Для управління пристроями
100	Native	Власна мережа

Схема адресації підмереж VLAN детально представлена в таблиці 3.8.

Таблиця 3.7 – Адресація мереж VLAN

Номер VLAN	Розмір	Адреса	Маска	Діапазон адрес	Широкомовна адреса
15	16	10.24.40.71	255.255.255.240	10.24.40.72	10.24.40.86
25	16	10.24.40.87	255.255.255.240	10.24.40.88	10.24.40.102
35	16	10.24.40.103	255.255.255.240	10.24.40.104	10.24.40.118
99	8	10.24.40.119	255.255.255.248	10.24.40.120	10.24.40.127
100	16	10.24.40.111	255.255.255.240	10.24.40.112	10.24.40.127

Розподіл портів для віртуальної мережі VLAN описано в таблиці 3.8.

Таблиця 3.8 – Порти для окремих мереж VLAN

Назва VLAN	VLAN	Розподіл портів
Accounting	15	F0/12-14
Resources Department	25	F0/15-24
Guest	35	F0/5-10

Приклад налаштування VLAN на комутаторі Karpenko_Switch3:

```
vlan 15 // Створення VLAN
name Accounting // Присвоєння імені
vlan 25
name Resources_Department
```

vlan 35

name Guest

vlan 99

name Management

vlan 100

name Native

interface range fa0/1–2 // Конфігурація інтерфейсів

switchport mode trunk // Надання порту режим транка

switchport trunk native vlan 99 // Вказання VLAN 99 як рідного

switchport trunk allowed vlan 25,35,45,99,100 // Дозвіл передачі VLAN

switchport trunk native vlan 100 // Вказання VLAN 100 як рідного

interface range fa0/5-10// Конфігурація інтерфейсів

switchport mode access // Надання порту режиму доступу

switchport access vlan 35 // Призначення цих інтерфейсів до VLAN 35

interface range fa0/12-14

switchport mode access

switchport access vlan 15

interface range fa0/15-24

switchport mode access

switchport access vlan 25

interface vlan 99 // Конфігурація інтерфейса

ip address 10.24.40.120 255.255.255.248 // Призначення IP-адреси

no shutdown // Ввімкнення інтерфейсу

Налаштування підінтерфейсів маршрутизатора Karpenko_Router1, які виконуватимуть роль шлюзів для визначених VLAN:

int fa0/0.15 // Конфігурація інтерфейсу

encapsulation dot1Q 15 // Встановлення тегування VLAN

ip address 10.24.40.72 255.255.255.240 // Призначення IP-адреси

int fa0/0.25

encapsulation dot1Q 25

ip address 10.24.40.88 255.255.255.240

int fa0/0.35

encapsulation dot1Q 35

ip address 10.24.40.104 255.255.255.240

int fa0/0.99

encapsulation dot1Q 99

ip address 10.24.40.120 255.255.255.240

ip dhcp excluded-address 10.24.40.66 10.24.40.79 // Виключення діапазону адрес з пулу DHCP

ip dhcp excluded-address 10.24.40.72

ip dhcp excluded-address 10.24.40.88

ip dhcp pool LAN5-VLAN15 // Створення нового DHCP-пулу

network 10.24.40.71 255.255.255.240 // Призначення IP-адреси

default-router 10.24.40.72 // Вказання IP-адреси маршрутизатора

dns-server 10.24.40.79 // Вказання IP-адреси DNS-сервера

ip dhcp pool LAN5-VLAN25

network 10.24.40.87 255.255.255.240

default-router 10.24.40.88

dns-server 10.24.40.79

ip dhcp pool LAN5-VLAN35

network 10.24.40.103 255.255.255.240

default-router 10.24.40.104

dns-server 10.24.40.79

3.5.3 Налаштування VPN

VPN - це технологія, яка створює захищене та зашифроване з'єднання через менш захищену мережу, таку як Інтернет. VPN дозволяє користувачам безпечно передавати дані між своїми пристроями і віддаленими серверами або мережами, забезпечуючи конфіденційність та цілісність інформації.

Налаштування VPN, буде виконуватись на маршрутизаторі Karpenko_Router0:

license boot module c2900 technology-package securityk9 // Активація ліцензії

crypto isakmp policy 10 // Налаштування політики ISAKMP

encr aes // Використання AES для шифрування

authentication pre-share // Використання попередньо узгодженого ключа для аутентифікації

group 2 // Використання групи 2 для обміну ключами

crypto isakmp key cisco address 209.165.202.2 // Встановлює попередньо узгоджений ключ cisco

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac // Визначає набір трансформацій для IPSec

crypto map MAP 10 ipsec-isakmp // Налаштування карти з іменем MAP

description VPN connection to R5 // Описання VPN-з'єднання

set peer 209.165.202.2 // Встановлення IP-адресу віддаленого піра

set transform-set VPN-SET // Встановлення трансформаційного набору для IPSec

match address VPN // Вказання пакетів для обробки

int g0/0 // Конфігурація інтерфейсу

crypto map MAP // Прив'язування карти

ip access-list extended NAT // Розширений список контролю доступу

permit ip 10.24.40.192 0.0.0.15 10.24.40.0 0.0.0.63 // Дозволення трафіку

permit ip 10.24.40.192 0.0.0.15 10.24.40.64 0.0.0.127

permit ip 10.24.40.192 0.0.0.15 10.24.40.128 0.0.0.127

permit ip 10.24.40.192 0.0.0.15 10.24.40.208 0.0.0.15

permit ip 10.24.40.192 0.0.0.15 10.1.5.0 0.0.0.3

3.6 Перевірка роботи комп’ютерної системи

Для перевірки правильності базового налаштування маршрутизатора Karpenko_Router1 використовуємо команду do show running-config. Ця команда дозволяє переглянути поточну конфігурацію маршрутизатора, включаючи встановлені параметри.

Аналізуючи вивід команди, перевіряємо правильність налаштування таких параметрів, як назва пристрою, використання протоколу SSH для віддаленого доступу, пароль до привілейованого режиму, ім'я користувача та пароль, а також ім'я домену. Ці параметри відображаються на рисунках 3.2-3.7.

```
!
hostname Karpenko_Router1
!
```

Рисунок 3.2 - Найменування пристрою

```
line con 0
 password 7 0822455D0A16
 login authentication console
!
```

Рисунок 3.3 – Пароль для доступу до консолі

```
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
```

Рисунок 3.4 - Пароль до привілейованого режиму

```
!
username Karpenko_Router1 password 7 082048430017544541
username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
```

Рисунок 3.5 – Логін та пароль

```
!
no ip domain-lookup
ip domain-name Karpenko.123-20-1.com
!
```

Рисунок 3.6 – Домен

Перевіримо функціонування технології EtherChannel у локальній мережі LAN_1 на прикладі комутатора Karpenko_Switch2 (рис. 3.7). Також зробимо перевірку протоколу OSPF (рис. 3.8).

```
Karpenko_Switch2(config)#do show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------

1      Po1(SU)           LACP   Fa0/1(P) Fa0/2(P)
2      Po2(SU)           LACP   Fa0/3(P) Fa0/4(P)
```

Рисунок 3.7 – Перевірка EtherChannel

```
Karpenko_Router1(config-router)#do show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.24.40.129
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.5.0 0.0.0.3 area 0
    10.1.5.4 0.0.0.3 area 0
    10.1.5.8 0.0.0.3 area 0
    10.1.5.12 0.0.0.3 area 0
    10.1.5.16 0.0.0.3 area 0
  Passive Interface(s):
    Vlan1
    Serial0/3/1
    FastEthernet0/0.15
    FastEthernet0/0.25
    FastEthernet0/0.35
    FastEthernet0/0.99
```

Рисунок 3.8 – Перевірка протоколу OSPF

Перевірив зв’язок між різними підмережами LAN_1 - LAN_2, результат зображено на рисунку 3.9.

Fire	Last Status	Source	Destination	Type	Color
	Successful	Karpenko_PC1	Karpenko_PC19	ICMP	

Рисунок 3.9 – Маршрутизація між підмережами

Перевіримо налаштування пропускної спроможності на послідовних інтерфейсах маршрутизатора Karpenko_Router2. Для цього використаємо команду do show interfaces serial0/2/0, результат якої показано на рисунку 3.10.

```
Karpenko_Router2(config)#do show interfaces serial0/2/0
Serial0/2/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Internet address is 10.1.5.5/30
  MTU 1500 bytes, BW 128 Kbit, DLY 75000 usec,
```

Рисунок 3.10 – Перевірка пропускної спроможності

Перевірив маршрути за замовчуванням на пограничному маршрутизаторі Karpenko_Router3 (рисунок 3.11).

```
Karpenko_Router3(config)#do show ip route static
     209.165.201.0/28 is subnetted, 1 subnets
S       209.165.201.0 [1/0] via 209.165.202.2
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.11 – Перевірка маршрутів за замовчуванням

Перевір налаштування RADIUS-серверу виконавши вхід на маршрутизаторі Karpenko_Router5 (рисунок 3.12-13).

```
Username: Karpenko_Router5
Password:
Karpenko_Router5>en
Password:
Karpenko_Router5#conf t
```

Рисунок 3.12 – Перевірка RADIUS-серверу

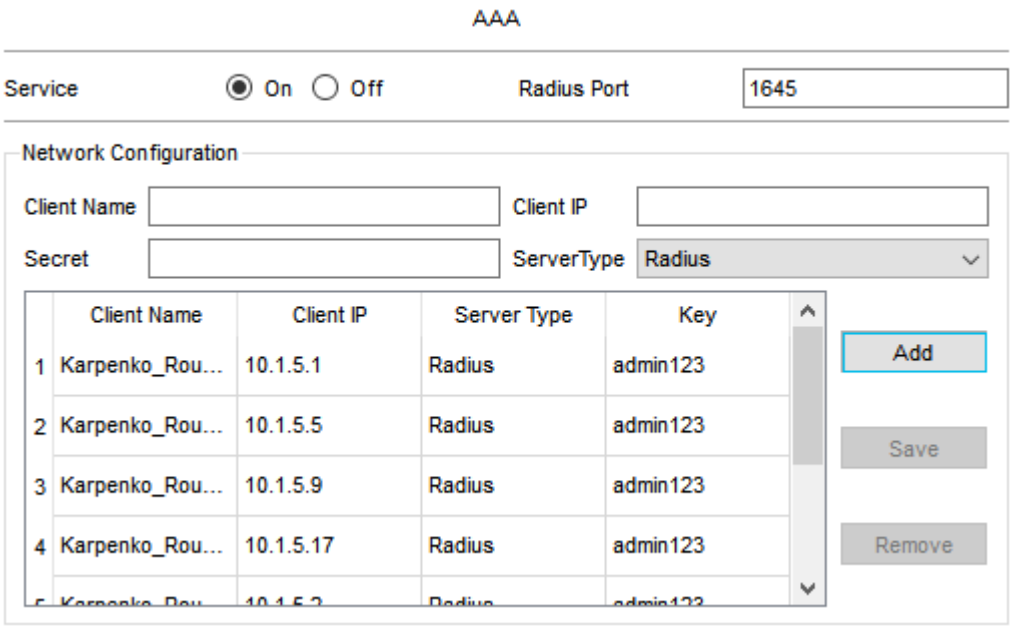

Рисунок 3.13 – Налаштування служби AAA

Перевірив налаштування сервісу dhcp на прикладі Karpenko_PC24, що розташований в LAN_3 (рисунок 3.14).

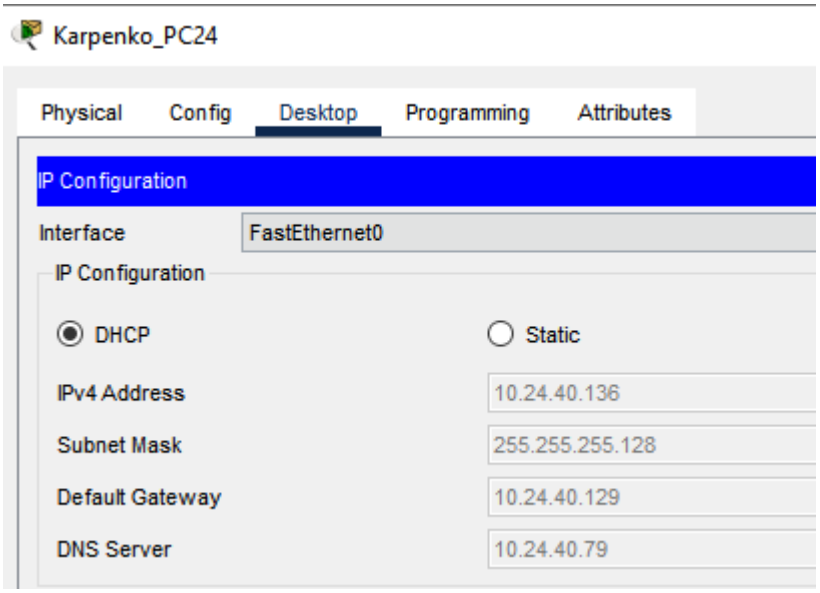

Рисунок 3.14 – Перевірка налаштування dhcp сервісу

Тепер потрібно перевірити адресацію сервері DNS, HTTP та TFTP (рисунок 3.15-17).

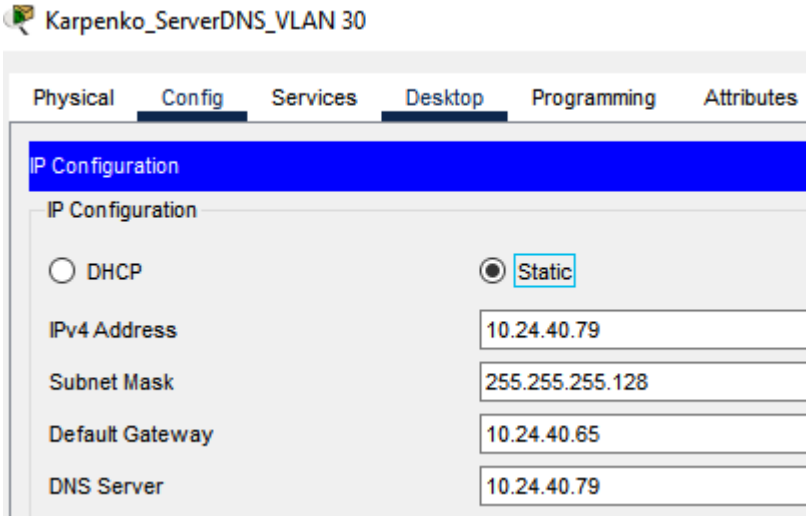

Рисунок 3.15 – Сервер DNS

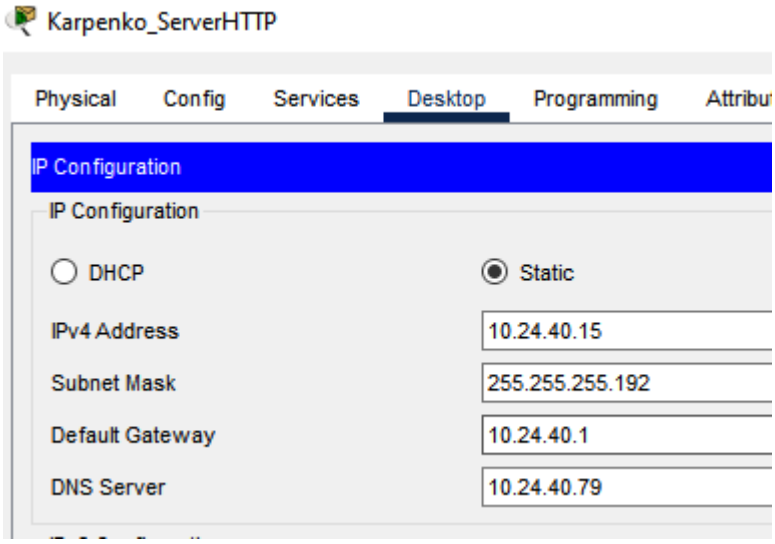

Рисунок 3.16 – Сервер HTTP

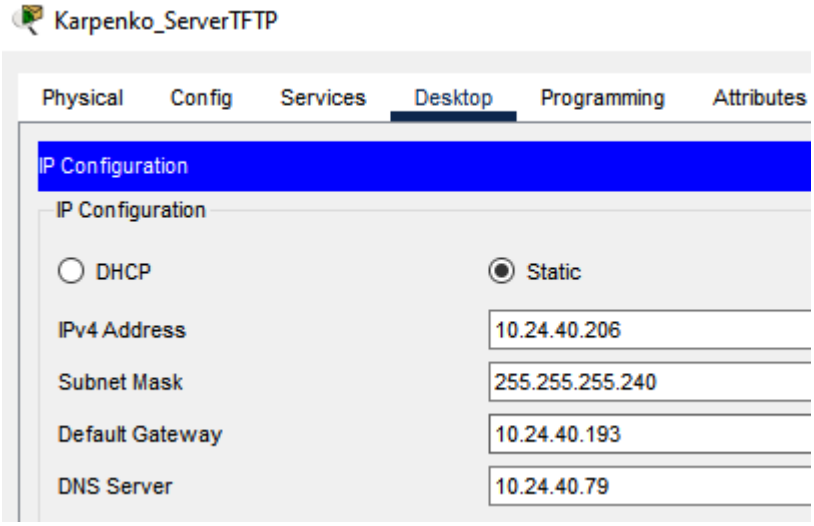

Рисунок 3.17 – Сервер TFTP

Для перевірки коректності призначення IP-адрес маршрутизатору Karpenk_Router1 використаємо команду do show ip interface brief. Результати виконання цієї команди, які відображають призначені IP-адреси та стан інтерфейсів, представлені на рисунку 3.18.

```
Karpenko_Router1(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.24.40.65     YES manual up                    up
FastEthernet0/0.15     10.24.41.1      YES manual up                    up
FastEthernet0/0.25     unassigned      YES unset  up                    up
FastEthernet0/0.35     unassigned      YES unset  up                    up
FastEthernet0/0.99     unassigned      YES unset  up                    up
FastEthernet0/1        10.1.5.2        YES manual up                    up
FastEthernet0/2/0      unassigned      YES unset  up                    up
FastEthernet0/2/1      unassigned      YES unset  up                    down
FastEthernet0/2/2      unassigned      YES unset  up                    down
FastEthernet0/2/3      unassigned      YES unset  up                    down
Serial0/3/0            10.24.40.129    YES manual up                    down
```

Рисунок 3.18 - Адресація інтерфейсів маршрутизатора

Перевіримо правильність призначення IP-адреси віртуальному інтерфейсу VLAN 1 на комутаторі Karpenko_Switch3. Для цього використаємо команду show interface vlan 1. Результати виконання цієї команди, які відображають призначену IP-адресу та стан інтерфейсу VLAN 1, представлені на рисунку 3.19.

```
Karpenko_Switch3#show interface vlan 1
Vlan1 is up, line protocol is down
  Hardware is CPU Interface, address is 00d0.978c.941e (bia 00d0.978c.941e)
  Internet address is 10.24.40.67/25
```

Рисунок 3.19 - IP-адреса комутатора

Перевірив налаштування безпеки порту на комутаторі Karpenko_Switch11, до якого підключено TFTP-сервер (рисунок 3.20).

```
Karpenko_Switch11(config)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
------------------------------------------------------------------------
        Fa0/3        2           0                0         Restrict
------------------------------------------------------------------------
```

Рисунок 3.20 – Перевірка порту TFTP-серверу

Перевірив налаштування віртуальних локальних мереж на комутаторі Karpenko_Switch3. Для цього використаємо команду do show vlan (рисунок 3.21).

```
Karpenko_Switch3(config)#do show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/11, Gig0/1, Gig0/2
15   VLAN0015                         active    Fa0/3, Fa0/12, Fa0/13, Fa0/14
25   Accounting                       active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
35   Resources_Department             active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
45   Guest                            active
99   Management                       active
100  Native                           active
```

Рисунок 3.21 – Налаштування VLAN

Перевірив налаштування trunk портів (рисунок 3.22).

```
Karpenko_Switch3(config)#do show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      99
Fa0/2       on           802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       25,35,45,99-100
Fa0/2       25,35,45,99-100
```

Рисунок 3.22 – Налаштування trunk портів

Перевірив налаштування NAT, виконавши команду и do show ip nat translations (рисунок 3.23).

```
Inside global     Inside local
209.165.200.3     10.24.40.79
209.165.200.4     10.24.40.15
```

Рисунок – 3.23 – Налаштування NAT

Перевірив налаштування HTTP-серверу, перейшовши за посиланням 123.dnipro.ua (рис. 3.24).

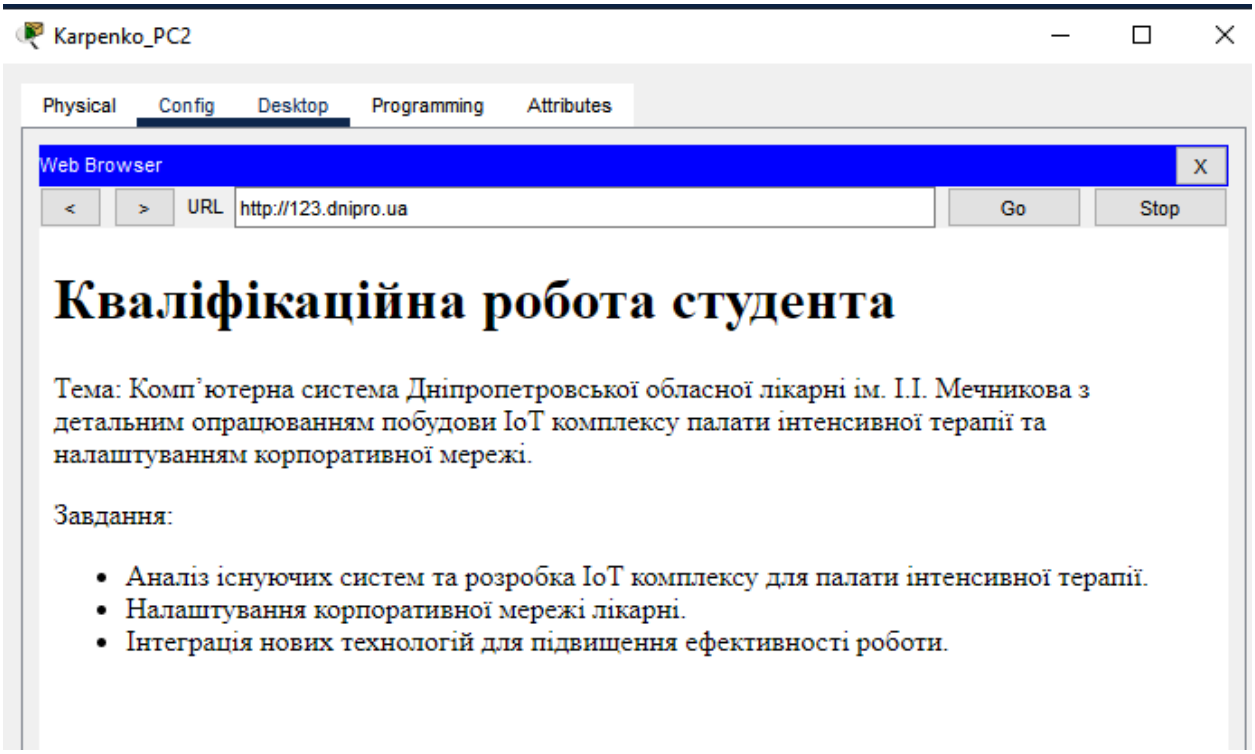

Рисунок 3.24 – Веб-сайт HTTP-серверу

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Положення що до вибору компонентів Системи

Інженерне рішення для розробки компонента Системи Інтернету речей (IoT) являє собою мережу взаємопов'язаних пристроїв, підключених до Інтернету. Ця система використовує датчики для збору даних про навколишнє середовище та пристрої, які реагують на ці дані, автоматизуючи різні процеси, такі як керування освітленням, температурою та безпекою.

У запропонованому рішенні IoT-система включає датчики вогню, руху та зчитувач ID-карток, а також сирену, веб-камеру та двері. Шлюз для розумного будинку HomeGateway служить центральним вузлом, координуючи роботу пристроїв відповідно до заданих умов, наприклад, активація сирени при виявленні вогню або відкриття дверей при успішній ідентифікації картки.

Взаємодія пристроїв забезпечується централізованим шлюзом HomeGateway, який виконує роль "мозку" системи. Він запрограмований на виконання певних дій у відповідь на сигнали від датчиків: активація сирени при виявленні вогню, чадного газу, ввімкнення камери відеоспостереження при руху та відмикання дверей після успішного зчитування ID-картки,

4.2 Налаштування компонентів системи IoT

Встановлюєм HomeGateway в мережі LAN_2. Створюєм захищену Wi-Fi точку доступу з іменем Karpenko та паролем 123-20-1, використовуючи протокол WPA2-PSK з шифруванням AES.

Після цього додаємо IoT-пристрої та підключаєм до HomeGateway за допомогою введених SSID та паролю.

Топологічна схема відділення інтенсивної терапії, включаючи розташування IoT-пристроїв, представлена на рис. 4.

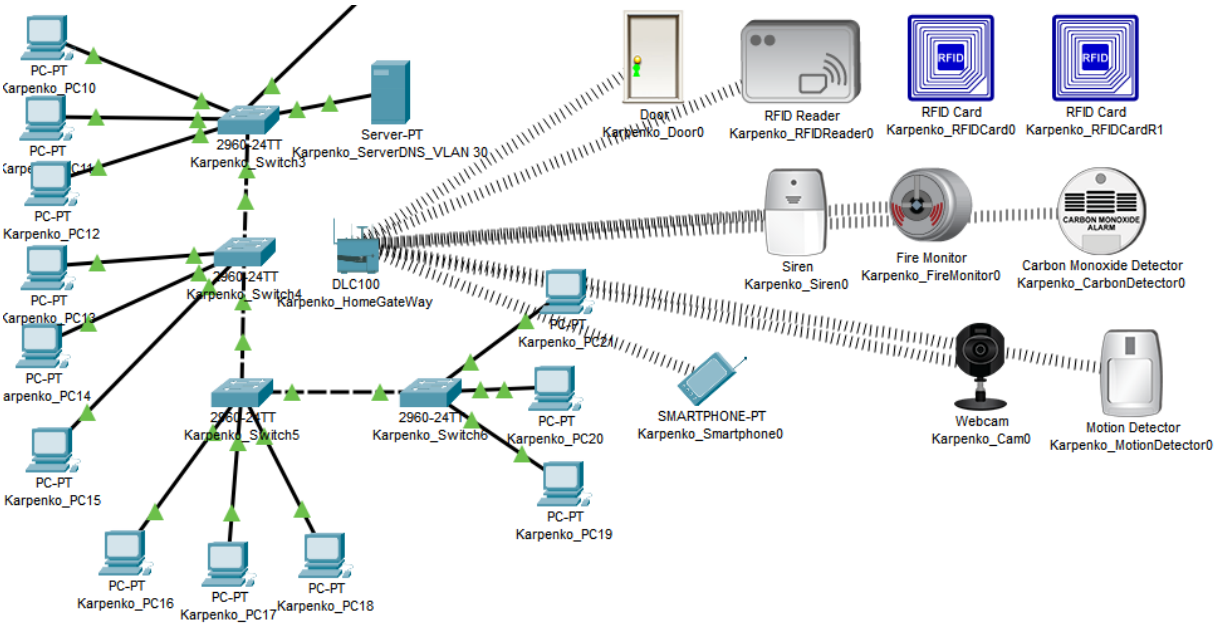

Рисунок 4.1 – Топологічна схема відділення інтенсивної терапії включаючи розташування IoT-пристроїв

Для налаштування умов роботи IoT-системи на смартфоні відкрив IoT Monitor, ввів адресу шлюзу, логін і пароль. Після цього відкриється сторінка з усіма підключеними IoT-пристроями, як показано на рис. 4.2.

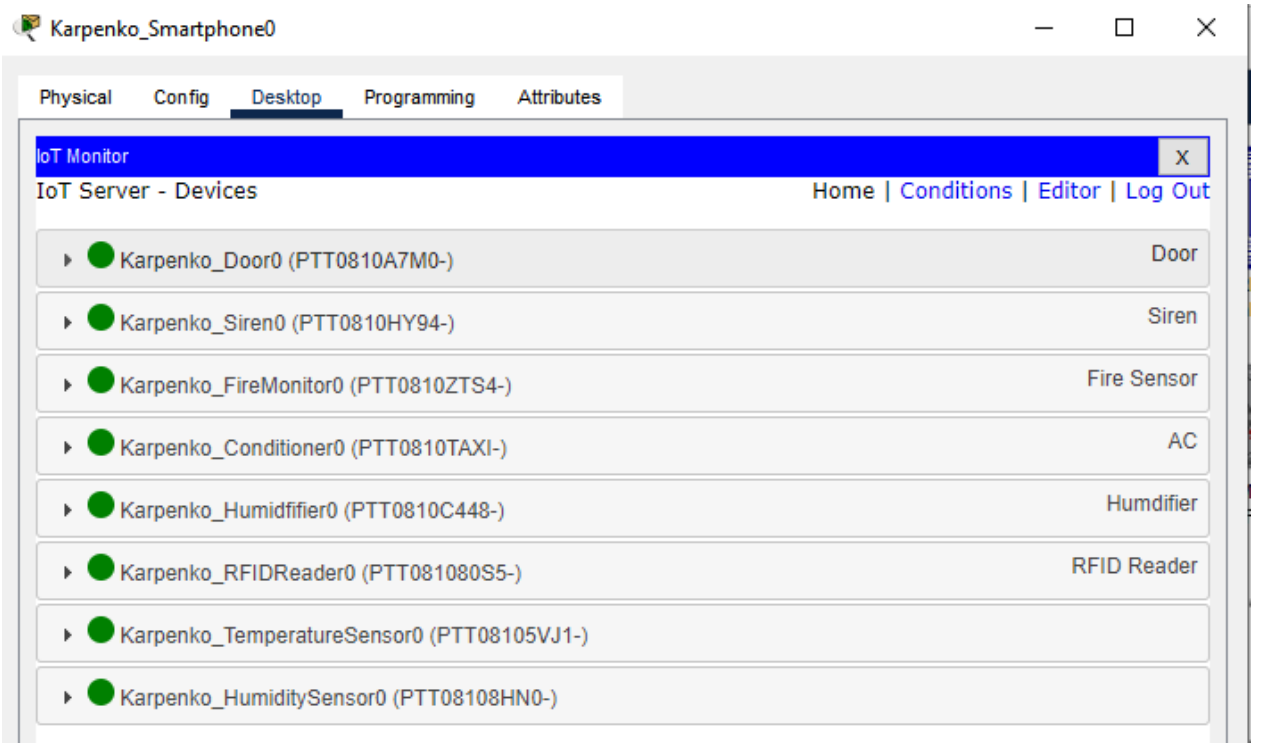

Рисунок 4.2 – Перелік IoT-пристроїв

Перейшов на вкладку Conditions, щоб налаштувати правила для IoT-пристроїв. Налаштував роботу сирени, як показано на рисунку 4.3-3.

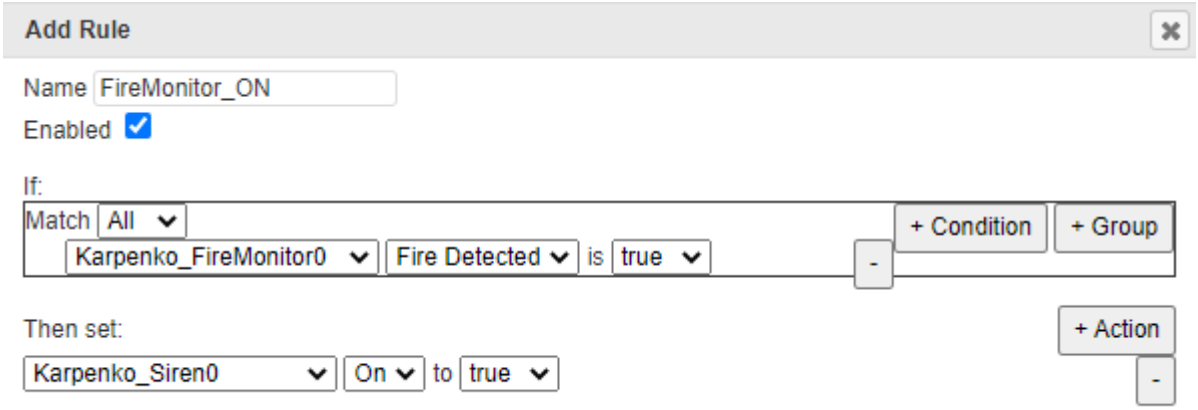

Рисунок 4.3 – Налаштування спрацювання сирени

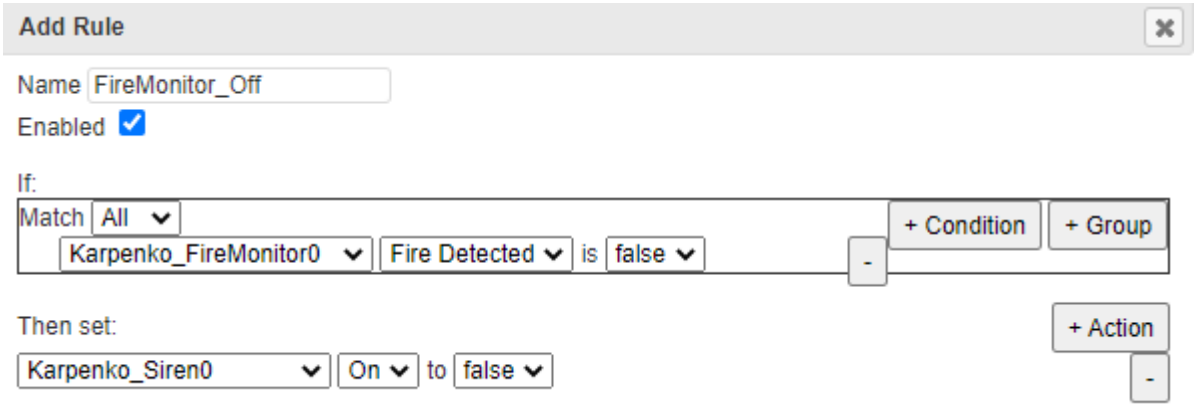

Рисунок 4.4 - Налаштування не спрацювання сирени

Налаштував зчитувач ID-карток, щоб він підтвердив валідність картки, її ідентифікаційний номер повинен бути 123. Якщо ID відрізняється, картка вважається недійсною (рисунок 4.5-6).

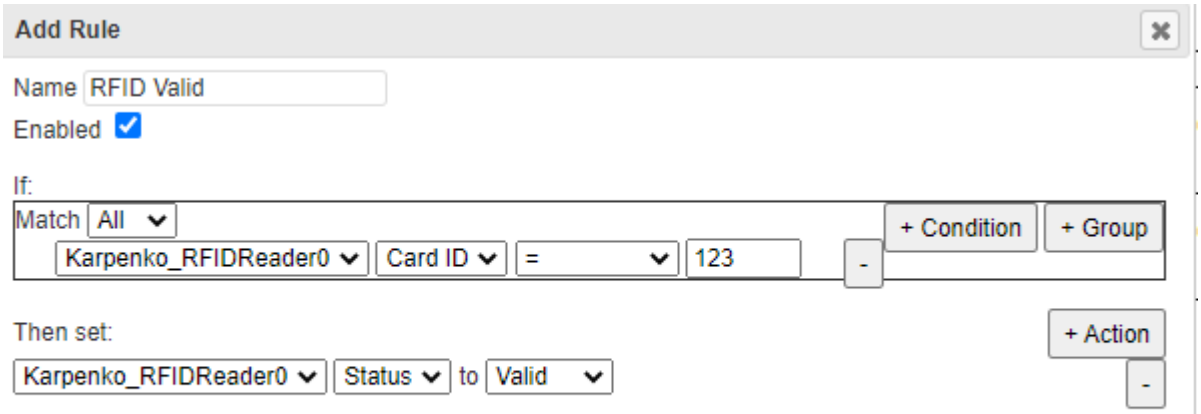

Рисунок 4.5 – Налаштування спрацювання картки

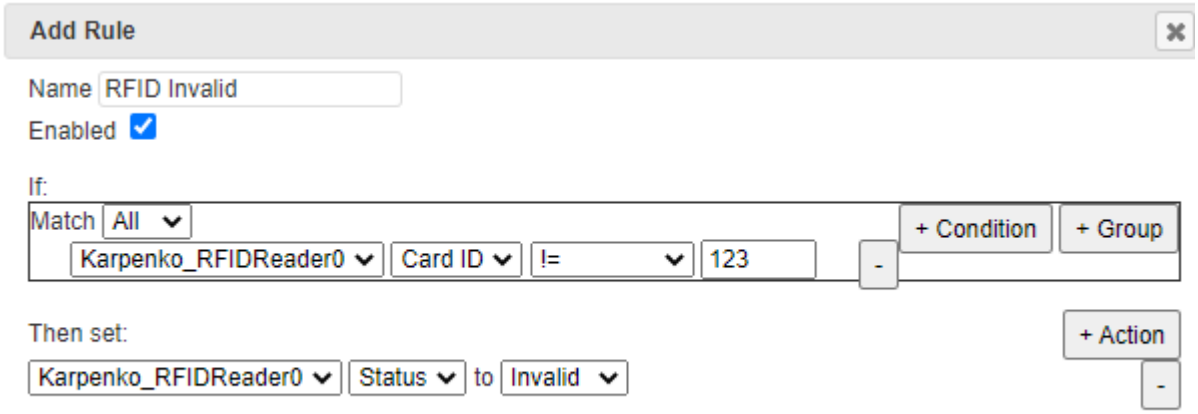

Рисунок 4.6 - Налаштування не спрацювання картки

Після того підтвердження картки, налаштував сценарій відчинення двері який зображений на рисуноках 4.7-8.

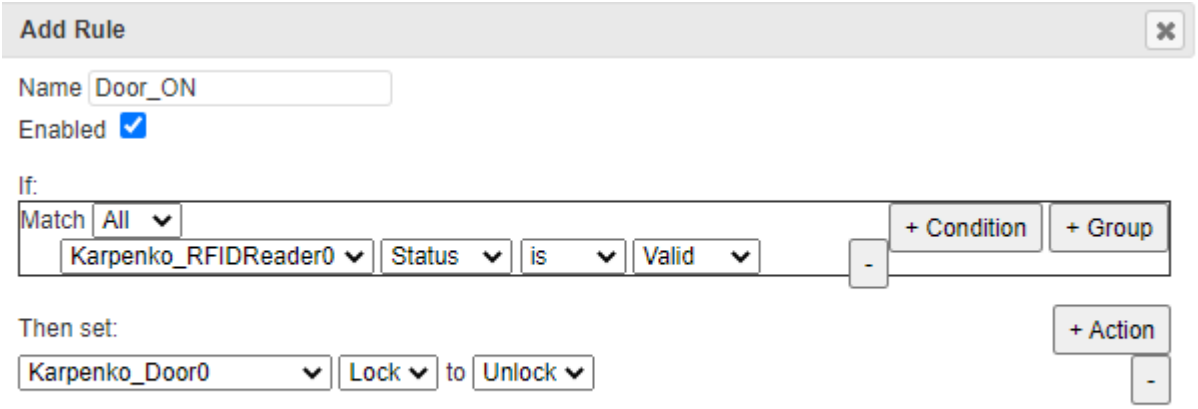

Рисунок 4.7 – Налаштування відкриття дверей

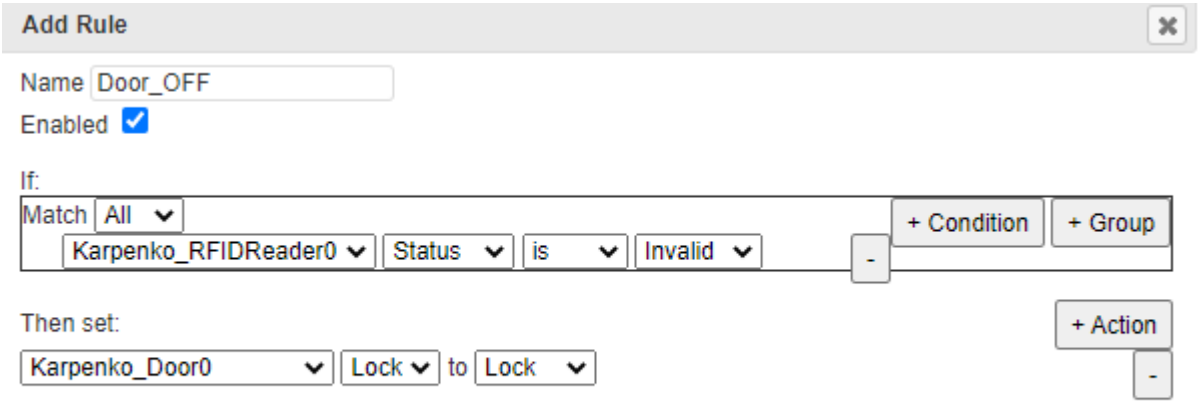

Рисунок 4.8 – Налаштування зачинених дверей

Налаштував ввімкнення сирени при спрацюванні датчику чадного газу (рисунок 4.9-10).

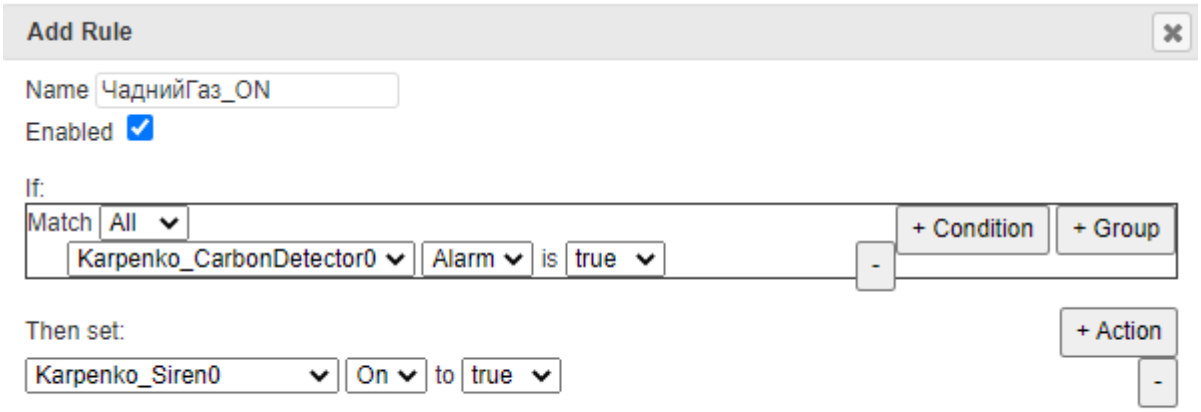

Рисунок 4.9 – Налаштування спрацьовування сирени

Рисунок 4.9 – Налаштування не спрацьовування сирени

Налаштував ввімкнення камери відеоспостереження при спрацюванні датчика руху (рисунок 4.11-12).

Рисунок 4.11 – Налаштування ввімкнення камери відеоспостереження

Рисунок 4.12 – Налаштування вимкнення камери відеоспостереження

4.3 Перевірка роботи IoT пристроїв

Для перевірки справності зчитувача ID-карток були використані картки з ID 123 (для підтвердження успішної роботи) та 321 (для перевірки відхилення недійсної картки). Результат зображено на рисунка 4.13-14.

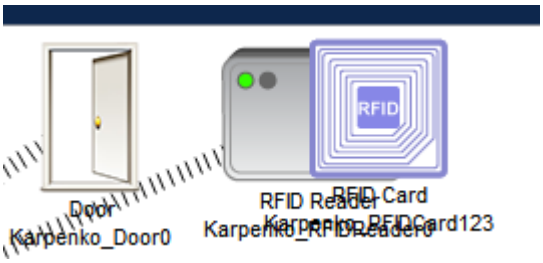

Рисунок 4.13 – Перевірка відчинених дверей

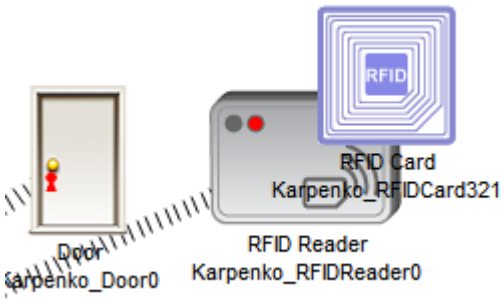

Рисунок 4.13 – Перевірка зачинених дверей

Для перевірки справності датчиків вогню, чадного газу та сирени, на мові було додано елемент, та мовою Javascript прописано скріпт для імітації вогню та чадного газу. Скрипт для імітації пожежі:

```
function setup (){
setDeviceProperty(getName(), 'IR', 900);
```

```
}
```

Скрипт для імітації чадного газу:

```
function setup (){
setDeviceProperty(getName(), "co", 500);
}
```

Результат перевірки зображено на рисунках 4.14 – 4.15.

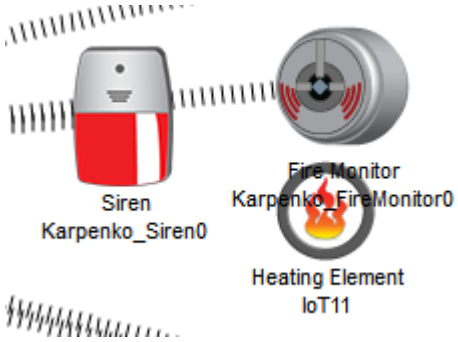

Рисунок 4.14 – Спрацювання датчику вогню та сирени

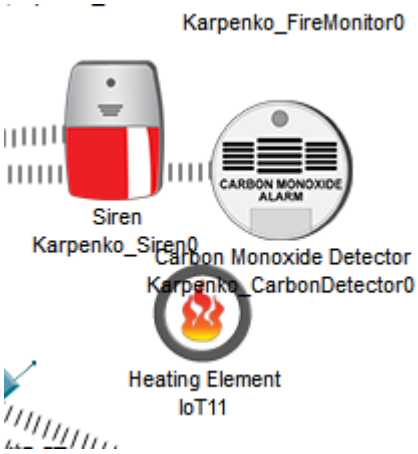

Рисунок 4.15 - Спрацювання датчику чадного газу та сирени

Перевірив налаштування вмикання камери відеоспостереження при фіксуванні руху (рисунок 4.16).

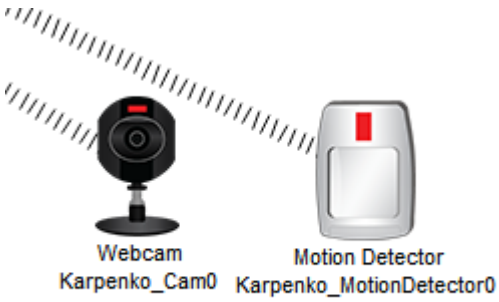

Рисунок 4.16 – Спрацювання датчику руху та камери

ВИСНОВКИ

У рамках даної кваліфікаційної роботи було спроектовано та реалізовано корпоративну мережу для Дніпропетровської обласної лікарні ім. І.І. Мечникова, приділяючи особливу увагу розробці IoT-комплексу для палати інтенсивної терапії.

Після ретельного аналізу потреб лікарні було визначено вимоги до мережевої інфраструктури. На основі цих вимог було підібрано відповідне обладнання та змодельовано комп'ютерну мережу в середовищі Cisco Packet Tracer.

В рамках проекту було розраховано та призначено IP-адреси для кожного пристрою, а також налаштовано ряд технологій для забезпечення надійності, безпеки та ефективності роботи мережі: EtherChannel, DHCP, VLAN, NAT, VPN та AAA. Для організації маршрутизації між підмережами було використано протокол OSPF. Крім того, було проведено базову конфігурацію всіх пристроїв та забезпечено безпеку портів комутатора, що підключений до сервера TFTP.

Для зручності користувачів було налаштовано сервери HTTP та DNS, що дозволяє отримати доступ до веб-сайту з інформацією про кваліфікаційну роботу як за IP-адресою, так і за доменним ім'ям.

Важливим етапом роботи стало створення та налаштування IoT-комплексу для палати інтенсивної терапії. Після завершення всіх налаштувань було проведено комплексне тестування як окремих компонентів системи, так і її роботи в цілому.

Кваліфікаційна робота повністю відповідає поставленим завданням та оформлена згідно з усіма нормативними вимогами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Пороло Є. Удосконалена архітектура мережі для хмарного Інтернету речей / Є. Пороло, В. Курдеча // ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ / Є. Пороло, В. Курдеча. – м. Київ, Україна: ISSN (print) 2663-502X, ISSN (online) 2664-3057, 2020. – С. 219–221.
2. Олексюк В., Балик Н., Балик А. Організація комп’ютерної локальної мережі. / В. Олексюк, Н. Балик, А. Балик. – Тернопіль: Підручники та посібники, 2006. – 41 с.
3. Цвіркун, Л.І. Розробка програмного забезпечення комп’ютерних систем. Програмування: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова, під заг. ред. Л.І. Цвіркуна. – 3-є вид., випр. – Д.: Національний гірничий університет, 2016. – 223 с. – ISBN 978-966-350-595-4.
4. Коваленко А. Інтеграція Інтернету речей в медичні інформаційні системи / А. Коваленко, О. Петренко // Медична інформатика та інженерія. – 2022. – № 2. – С. 45-52.
5. Сидоренко І. Безпека даних в медичних IoT-системах / І. Сидоренко // Український журнал телемедицини та медичної телематики. – 2021. – № 4. – С. 87-95.
6. Валецька Тетяна Михайлівна Комп'ютерні мережі. Апаратні засоби. - К.: Центр навчальної літератури, 2004. - 208 с.
7. Лозікова Г.М. Комп'ютерні мережі. - К.: Центр навчальної літератури, 2004. - 128 с.
8. Дипломування. Методичні вказівки для бакалаврів галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова ; М-во освіти і науки України, Нац. гірн. ун-т. – Дніпро: НГУ, 2016. – 56 с.

Додаток А

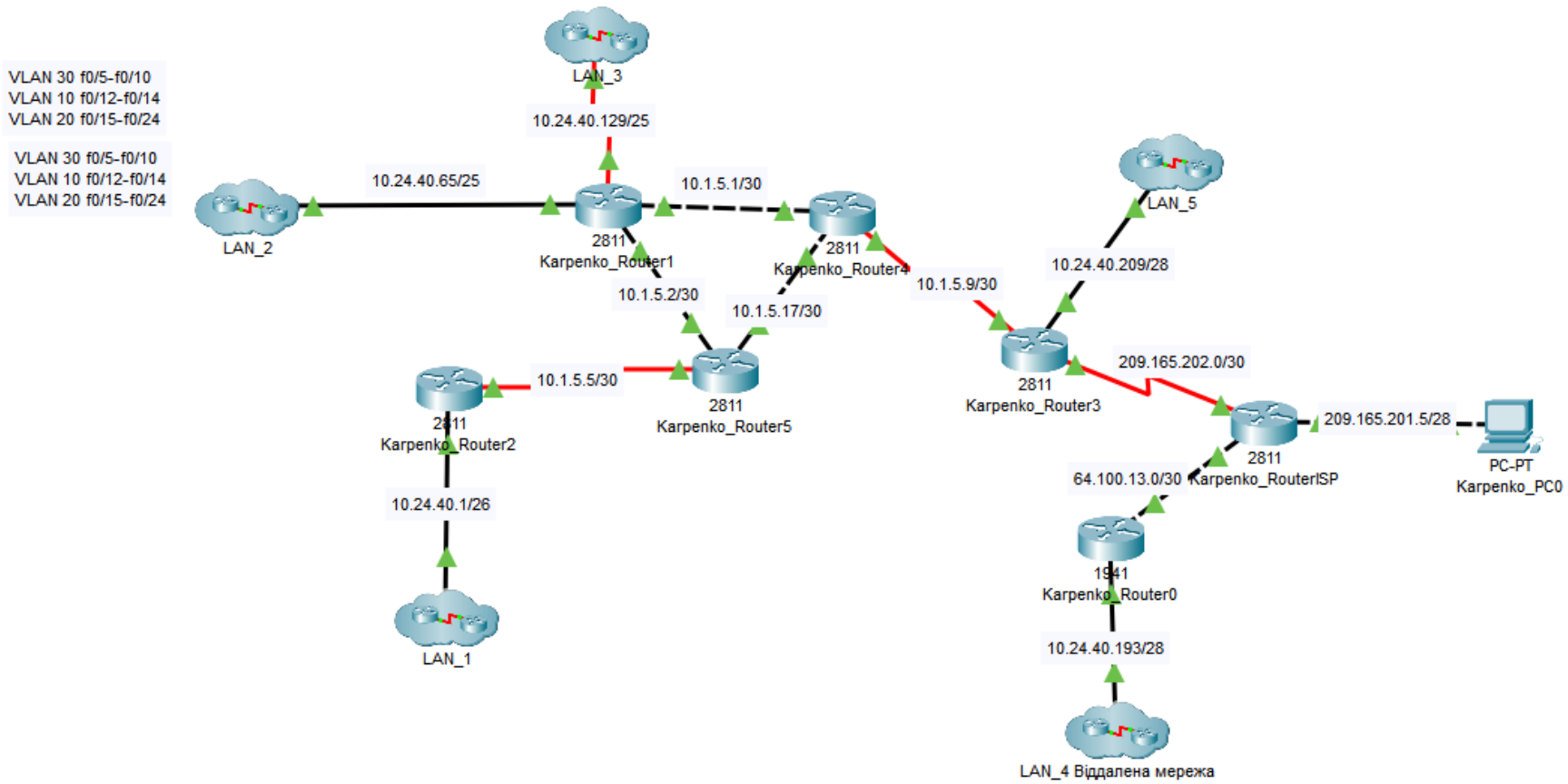

Рисунок ДА.1 – Загальна топологія мережі лікарні

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ “ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.24018-01 12 01

Листів 10

2024

АНОТАЦІЯ

Ця програма включає набір команд для конфігурування маршрутизаторів та комутаторів у корпоративній мережі.

Команди дозволяють налаштувати IP-адресацію, виконати базове налаштування пристроїв, а також налаштувати такі служби та протоколи, як DHCP, NAT, VPN, AAA, OSPF, VLAN, статичну маршрутизацію, EtherChannel та забезпечити безпеку портів.

ЗМІСТ

1. Karpenko_Router0

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Karpenko_Router0
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip dhcp excluded-address 10.24.40.193 10.24.40.206
!
ip dhcp pool LAN_4
network 10.24.40.192 255.255.255.240
default-router 10.24.40.193
dns-server 10.24.40.101
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
ip cef
no ipv6 cef
!
username 123-20-1_Karpenko password 7 082048430017
username Karpenko_Router0 password 7 082048430017544541
username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO1941/K9 sn FTX1524Q796-
license boot module c2900 technology-package securityk9
!
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
rypto isakmp key cisco address 209.165.202.2
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map MAP 10 ipsec-isakmp
description VPN connection to R5
set peer 209.165.202.2
```

```
!
set transform-set VPN-SET
match address VPN
!
int g0/0
crypto map MAP
!
ip domain-name Karpenko.123-20-1.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 64.100.13.1 255.255.255.252
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.24.40.193 255.255.255.240
ip nat outside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
network 10.1.5.0 0.0.0.3 area 0
network 10.1.5.4 0.0.0.3 area 0
network 10.1.5.8 0.0.0.3 area 0
network 10.1.5.12 0.0.0.3 area 0
network 10.1.5.16 0.0.0.3 area 0
!
ip classless
!
ip flow-export version 9
!
ip access-list extended NAT
deny ip 10.24.40.192 0.0.0.15 10.24.40.0 0.0.0.63
```

```
deny ip 10.24.40.192 0.0.0.15 10.24.40.0 0.0.0.127
deny ip 10.24.40.192 0.0.0.15 10.24.40.128 0.0.0.127
deny ip 10.24.40.192 0.0.0.15 10.24.40.208 0.0.0.15
deny ip 10.24.40.192 0.0.0.15 10.1.5.0 0.0.0.3
permit ip 10.24.40.192 0.0.0.15 10.24.40.0 0.0.0.63
permit ip 10.24.40.192 0.0.0.15 10.24.40.0 0.0.0.127
permit ip 10.24.40.192 0.0.0.15 10.24.40.128 0.0.0.127
permit ip 10.24.40.192 0.0.0.15 10.24.40.208 0.0.0.15
permit ip 10.24.40.192 0.0.0.15 10.1.5.0 0.0.0.3
!
no cdp run
!
banner motd ^CKarpenko_Router0^C
!
radius server 10.24.40.151
address ipv4 10.24.40.151 auth-port 1645
key radius123
!
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
```

2. Karpenko_Router3

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Karpenko_Router3
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
```

```
ip dhcp excluded-address 10.24.40.209 10.24.40.215
!
ip dhcp pool LAN-5
network 10.24.40.208 255.255.255.240
default-router 10.24.40.209
dns-server 10.24.40.101
!
aaa new-model
!
aaa authentication login console group radius local
aaa authentication login default local
!
no ip cef
no ipv6 cef
!
username Karpenko_Router3 password 7 082048430017544541
username admin secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO1941/K9 sn FTX1524Q796-
license boot module c2900 technology-package securityk9
!
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
rypto isakmp key cisco address 209.165.202.2
!
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
!
crypto map MAP 10 ipsec-isakmp
description VPN connection to R5
set peer 209.165.202.2
!
set transform-set VPN-SET
match address VPN
!
no ip domain-lookup
ip domain-name Karpenko.123-20-1.com
!
spanning-tree mode pvst
!
interface FastEthernet0/0
ip address 10.24.40.209 255.255.255.240
```

```
ip nat inside
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/2/0
ip address 10.1.5.9 255.255.255.252
delay 7500
ip nat inside
clock rate 128000
!
interface Serial0/2/1
ip address 209.165.202.1 255.255.255.252
delay 7500
ip nat outside
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
redistribute static subnets
passive-interface default
no passive-interface FastEthernet0/0
no passive-interface Serial0/2/0
no passive-interface Serial0/2/1
network 10.1.5.0 0.0.0.3 area 0
network 10.1.5.4 0.0.0.3 area 0
network 10.1.5.8 0.0.0.3 area 0
network 10.1.5.12 0.0.0.3 area 0
network 10.1.5.16 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT5 pool Internet
ip nat inside source static 10.24.40.15 209.165.200.4
ip nat inside source static 10.24.40.79 209.165.200.3
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 209.165.202.2
ip route 209.165.201.0 255.255.255.240 209.165.202.2
!
ip flow-export version 9
!
ip access-list extended NAT5
deny ip 10.24.40.0 0.0.0.63 10.24.40.192 0.0.0.15
deny ip 10.24.40.0 0.0.0.127 10.24.40.192 0.0.0.15
deny ip 10.24.40.128 0.0.0.127 10.24.40.192 0.0.0.15
deny ip 10.24.40.208 0.0.0.15 10.24.40.192 0.0.0.15
deny ip 10.1.5.0 0.0.0.3 10.24.40.192 0.0.0.15
permit ip 10.24.40.0 0.0.0.63 any
permit ip 10.24.40.0 0.0.0.127 any
permit ip 10.24.40.128 0.0.0.127 any
permit ip 10.24.40.208 0.0.0.15 any
permit ip 10.1.5.0 0.0.0.3 any
!
no cdp run
!
radius server 10.24.40.151
address ipv4 10.24.40.151 auth-port 1645
key radius123
!
line con 0
password 7 0822455D0A16
login authentication console
!
line aux 0
!
line vty 0 4
login authentication default
transport input ssh
line vty 5 15
login authentication default
```

3. Karpenko_Switch4

```
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Karpenko_Switch4
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
```

```
!
ip domain-name Karpenko.123-20-1.com
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport trunk allowed vlan 25,35,45,99-100
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 99
switchport trunk allowed vlan 25,35,45,99-100
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 99
switchport trunk allowed vlan 25,35,45,99-100
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport trunk allowed vlan 25,35,45,99-100
switchport mode trunk
!
interface FastEthernet0/5
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 35
```

```
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/11
!
interface FastEthernet0/12
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 25
switchport mode access
!
```

```
interface FastEthernet0/21
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 25
switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 10.24.40.121 255.255.255.248
!
banner motd ^CKarpenko_Router4^C
!
line con 0
password 7 0822455D0A16
login
!
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
```

4. Karpenko_Switch11

```
version 15.0
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Karpenko_Switch11
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip domain-name Karpenko.123-20-1.com
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk native vlan 99
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 99
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/3
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
switchport trunk native vlan 99
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/5
switchport trunk native vlan 99
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 35
switchport mode access
!
```

```
interface FastEthernet0/7
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 35
switchport mode access
!
interface FastEthernet0/11
!
interface FastEthernet0/12
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 15
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 25
```

```
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 25
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 25
switchport mode access
!
interface GigabitEthernet0/1
switchport trunk native vlan 99
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface GigabitEthernet0/2
switchport trunk native vlan 99
switchport trunk allowed vlan 22,32,42,99-100
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 10.24.40.121 255.255.255.248
!
banner motd ^CKarpenko_Router11^C
```

```
!
line con 0
password 7 0822455D0A16
login
!
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
```