

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 Кривлені Нікити Юрійовича
 (ПІБ)

академічної групи 123-20-2
 (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 Першотравенської центральної міської лікарні”
 (назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Ткаченко С.М.			
спеціальної частини	ас. Бешта Л.В.			
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)" " _____ 2024 року**ЗАВДАННЯ****на кваліфікаційну роботу****ступеня бакалавр**студента Кривлені Н.Ю. академічної групи 123-20-2
(прізвище та ініціали) (шифр)спеціальності 123 «Комп'ютерна інженерія»за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)на тему «Комп'ютерна система Першотравенської центральної міської лікарні»затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується 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 _____
(підпис керівника)доц. Ткаченко С.М.
(прізвище, ініціали)Дата видачі 25.01.2024Дата подання до екзаменаційної комісії 01.07.2024

Прийнято до виконання _____

Кривленя Н.Ю.

РЕФЕРАТ

Пояснювальна записка: 104 с., 58 рис., 11 табл., 3 дод., 14 джерел.

КОМП'ЮТЕРНА СИСТЕМА, ОХОРОНА ЗДОРОВ'Я, ІОТ, БЕЗПЕКА,
CISCO, HELSI, ІНФОРМАЦІЙНІ СИСТЕМИ

Об'єкт – Першотравенська центральна міська лікарня.

Мета роботи – Проектування комп'ютерної мережі КЗ «Першотравенська центральна міська лікарня» для підтримки роботи медичних сервісів загального вжитку, а також забезпечення обміну медичними, економічними та даними системи безпеки між відділами.

Розглянута мережа трьох амбулаторій комунального закладу «Першотравенська центральна міська лікарня». Реалізоване розподілення на п'ять підмережі та впровадження систем безпеки з допомогою ІоТ-речей.

Комп'ютерна мережа та ІоТ прилади забезпечуватимуть виконання наступних функцій:

- забезпечення доступу до медичних інформаційних систем;
- забезпечення відеоспостереження за підприємством;
- забезпечення безпеки у разі несанкціонованого доступу у приміщення;
- забезпечення безпеки у разі виникнення пожежі.

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

Робота системи перевірена за допомогою моделі схеми корпоративної мережі із застосуванням програми Cisco Packet Tracer.

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

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів.....	8
Вступ.....	9
1 Стан питання і постановка завдання.....	10
1.1 Стисла характеристика галузі та умов застосування комп'ютерної мережі.....	10
1.2 Характеристика і структура КЗ «Першотравенська центральна міська лікарня».....	11
1.3 Стислі відомості про технологію керування для КЗ «Першотравенська центральна міська лікарня».....	14
1.4 Принципи та технічні методи керування КЗ «Першотравенська центральна міська лікарня».....	19
1.5 Аналіз процесу керування і визначення якісних задач	20
1.6 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови КЗ «Першотравенська центральна міська лікарня», відомих рішень у галузі, що розглядається	21
1.7 Мета роботи, що виконується	22
1.8 Визначення можливих напрямків рішення поставлених завдань ...	23
2 Розробка апаратної частини комп'ютерної системи підприємства	24
2.1 Технічні вимоги до комп'ютерної системи.....	24
2.1.1 Вимоги до системи в цілому.....	24
2.1.1.1 Вимоги до структури і функціонування системи.....	24
2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації системи.....	24
2.1.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи.....	25

2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами	25
2.1.1.1.4 Вимоги до діагностування системи	26
2.1.1.1.5 Перспективи розвитку та модернізації системи	26
2.1.1.2 Вимоги до показників призначення	27
2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи.....	27
2.1.1.3.1 Умови і регламент (режим) експлуатації, що повинні забезпечувати використання технічних засобів системи з заданими технічними показниками.....	27
2.1.1.3.2 Вимоги до параметрів мереж енергопостачання	27
2.1.1.3.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи	28
2.1.1.3.4 Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів	28
2.1.1.3.5 Вимоги до регламенту обслуговування.....	28
2.1.1.4 Вимоги до патентної чистоти.....	28
2.1.1.5 Додаткові вимоги	29
2.1.1.5.1 Вимоги до системи, пов'язані з особливими умовами її експлуатації.....	29
2.1.1.5.2 Вимоги до активного обладнання.....	29
2.1.1.5.3 Вимоги до кабель-каналів та електричним розеткам... 29	
2.1.1.5.4 Вимоги до комунікаційного обладнання і його розташування	30
2.1.1.5.5 Вимоги до однорідності.....	30
2.1.1.5.6 Вимоги до резервування.....	30
2.1.1.5.7 Спеціальні вимоги за розсудом розроблювача чи замовника Системи	30
2.1.2 Вимоги до функцій (задач), виконуваним системою.....	30

2.1.3	Вимоги до видів забезпечення.....	34
2.1.3.1	Вимоги до інформаційного забезпечення системи	34
2.1.3.2	Вимоги до лінгвістичного забезпечення системи	34
2.1.3.3	Вимоги до організаційного забезпечення.....	34
2.1.3.4	Вимоги до методичного забезпечення	35
2.2	Розробка апаратної частини комп'ютерної системи	36
2.2.1	Взаємодія користувачів з мережевими ресурсами і сервісами.	36
2.2.2	Обстеження об'єкту розробки з метою аналізу всіх способів внутрішнього і зовнішнього доступу до інфраструктури мережі	39
2.2.3	Аналіз об'єкту проектування та розробка специфікації апаратних засобів комп'ютерної системи	41
2.2.4	Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі	44
3	Розробка корпоративної мережі.....	47
3.1	Розрахунок адресації комп'ютерної мережі лікарні.....	47
3.2	Налаштування моделі комп'ютерної мережі лікарні	55
3.3	Налаштування пристроїв у мережі.....	59
3.3.1	Базове налаштування конфігурації пристроїв у мережі	59
3.3.2	Налаштування маршрутизаторів у мережі.....	64
3.3.3	Налаштування роботи Інтернет	68
3.3.4	Захист інформації в комп'ютерній мережі від несанкціонованого доступу	74
4	Розробка компонента системи	79
4.1	Вибір компонента системи.....	79
4.2	Функціонал IoT у мережі лікарні	79
4.3	Реалізація компоненту системи.....	84
4.4	Перевірка працездатності IoT	89
	Висновки.....	96
	Перелік посилань	97

Додаток А.....	99
Додаток Б.....	100
Додаток В.....	101

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ,
СКОРОЧЕНЬ І ТЕРМІНІВ**

ОЗ – охорона здоров'я.

КМ – комп'ютерна мережа.

ІС – інформаційна система.

КЗ – комунальний заклад.

ЕМК – Електронні медичні картки

VLAN – Virtual Local Area Network.

IP – Internet Protocol.

TFTP – Trivial File Transfer Protocol.

DNS – Domain Name System.

HTTP – HyperText Transfer Protocol.

VPN – Virtual Private Network.

IoT – Internet of Things.

LAN – Local Area Network.

AAA – Authentication Authorization and Accounting.

CM – Carbon Monoxide.

MD – Motion Detector.

WB – Window Blinds.

ВСТУП

У сучасному світі інформаційних технологій комп'ютерні мережі є невід'ємною складовою ефективного функціонування організацій, зокрема медичних закладів. Удосконалення технологій та інформаційних систем сприяє поліпшенню якості медичних послуг та ефективному управлінню даними пацієнтів. Це робить комп'ютерні мережі (КМ) важливою частиною медичного процесу.

Об'єктом дослідження є комунальний заклад «Першотравенська центральна міська лікарня». Аналіз стану об'єкта свідчить про необхідність оптимізації КМ для забезпечення якісного надання медичних послуг. Оптимізація включає розробку оптимальної архітектури, вибір необхідного обладнання та налаштування відповідних протоколів і сервісів для стабільного функціонування мережі.

Актуальність роботи базується на потребі вдосконалення КМ лікарні для оптимізації роботи медичного персоналу та забезпечення безпеки за допомогою IoT-пристроїв.

Метою роботи є створення КМ для підтримки медичних сервісів у КЗ «Першотравенська центральна міська лікарня», вдосконалення процесів обробки інформації у закладі та забезпечення стабільної роботи медичних систем.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп'ютерної мережі

Галузь ОЗ (охорони здоров'я) - це комплексна система, яка забезпечує надання послуг і допомоги людям для підтримки, відновлення і покращення їх фізичного і психічного здоров'я. Ця галузь включає різноманітні професії, такі як лікарі, медсестри, фармацевти та інші медичні працівники. Вона також включає різні заклади, такі як лікарні, поліклініки, амбулаторії, аптеки. Крім того, в галузі ОЗ використовуються різні технології і надаються послуги, спрямовані на підтримку і поліпшення стану здоров'я населення.

Зростаючі телекомунікаційні можливості комп'ютерних мереж, Web сайтів та Web-додатків відкривають нові перспективи для поліпшення взаємодії лікарів з пацієнтами. Впровадження таких технологій може зменшити, або зовсім прибрати черги, зменшити витрати часу як пацієнтів, так і лікарів.

Багато медичних інформаційних систем, таких як Helsi та Health24, розроблені з метою поліпшення доступу до медичних послуг та оптимізації управління медичною інформацією. Ці системи надають можливість швидко знаходити лікарів у будь-якому куточку України, реєструватися на відео-прийом або в офлайн медичні заклади, обирати сімейного лікаря для укладення декларації згідно з медичною реформою. Крім того, вони дозволяють зберігати всю медичну інформацію пацієнта, такі як призначення лікаря, історію візитів, рецепти, медичні документи, направлення, вакцинації [1][2].

Інші медичні ІС, такі як E-Life, або Ciet, надають можливість автоматизувати роботу медичних, бухгалтерських, економічних та управлінських бізнес-процесів системи ОЗ, планувати та управляти записами на прийом, забезпечувати криптографічний захист інформації та електронного цифрового підпису, а також надавати статистичну звітність [3][4].

Підключення до медичних ІС, таких як Helse, є критичним для забезпечення ефективного управління медичною інформацією та покращення якості надання медичних послуг. Для забезпечення цього зв'язку потрібна належно побудована КМ, яка забезпечить стійке та безпечне підключення до цих систем. Саме тому задача побудови КМ у «КЗ «Першотравенська центральна міська лікарня» Дніпропетровської обласної ради» є актуальною.

1.2 Характеристика і структура КЗ «Першотравенська центральна міська лікарня»

«Комунальний заклад «Першотравенська центральна міська лікарня» Дніпропетровської обласної ради» є багатoproфільною лікарнею вторинного рівня.

У 1960 році, з самого початку формування міста, була відкрита лікарня з 28 ліжками, а в 1965 році розпочала роботу нова лікарня з 175 ліжками. У 1972 році було введено в експлуатацію нове приміщення лікарні, що включало поліклініку та 4-поверховий корпус.

Поступово були відкриті нові відділення, і міська лікарня стала багатoproфільним медичним закладом. Завдяки впровадженню передових технологій, методів діагностики та лікування, був організований лікувально-діагностичний процес. В лікарні працюють анестезіологи, рентгенолаборанти, педіатри, акушери-гінекологи, неонатологи, хірурги, травматологи, невропатологи, клінічні лаборанти, які надають цілодобову медичну допомогу. Клініко-діагностична лабораторія оснащена сучасним обладнанням [5].

Сьогодні лікарня продовжує розвиватися та вдосконалювати свої медичні послуги, зосереджуючись на забезпеченні найвищих стандартів медичного обслуговування. Зокрема, лікарня активно використовує сучасні інформаційні технології для організації електронних медичних карт та звітності.

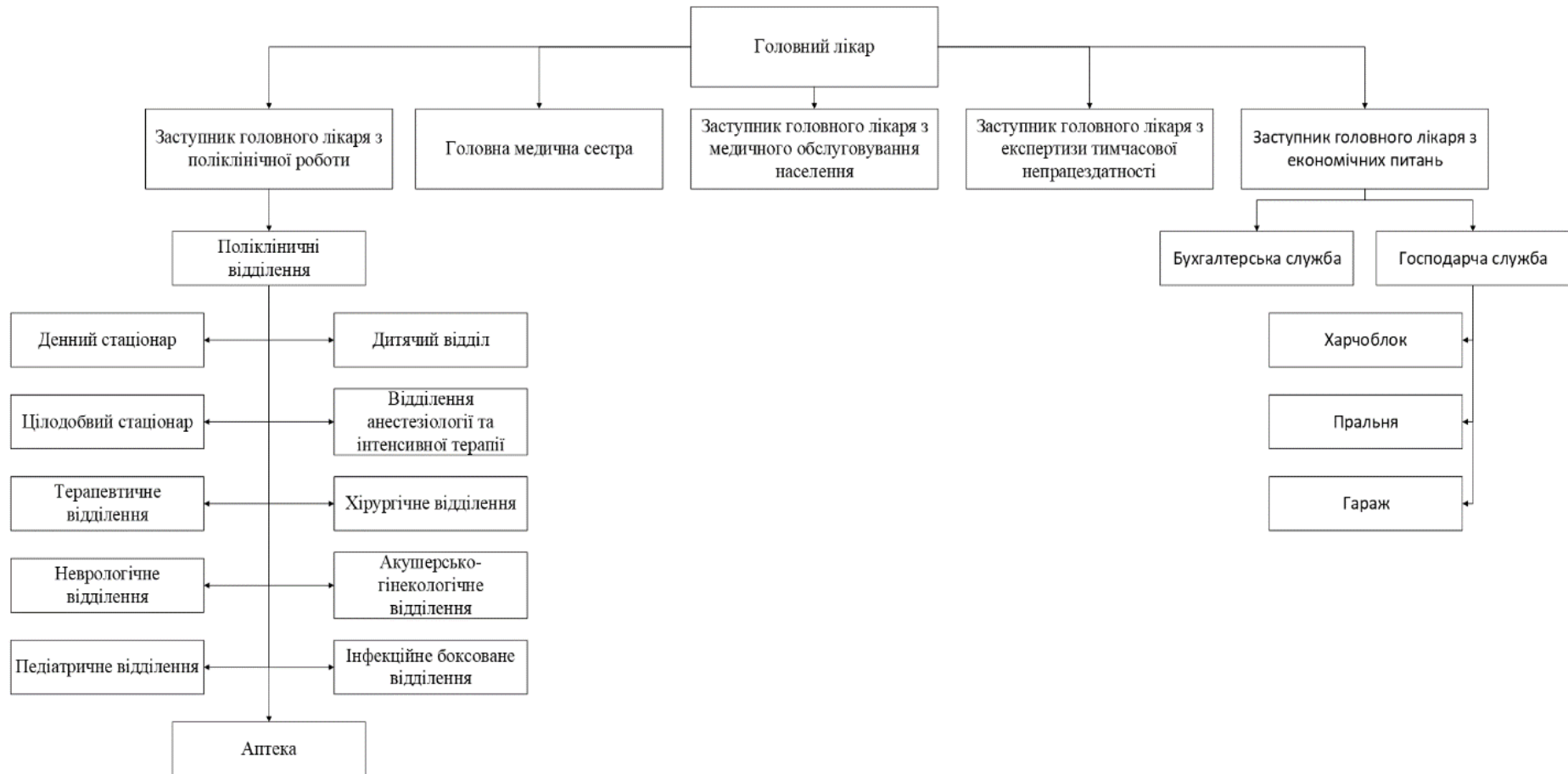


Рисунок 1.1 - Організаційна структура підприємства [6]

Об'єкт впровадження КМ знаходиться за юридичною адресою: вул. Шахтарської Слави, б.1, м. Першотравенськ, Дніпропетровської обл. Також має Амбулаторію №3, яка знаходиться за адресою: вул. Ювілейна, 13, м. Першотравенськ (рисунок 1.2).



Рисунок 1.2 – Схема гео-позиції КЗ «Першотравенська центральна міська лікарня»

1.3 Стислі відомості про технологію керування для КЗ «Першотравенська центральна міська лікарня»

Топологія КЗ «Першотравенська центральна міська лікарня» складається з трьох будівель: головна будівля, яка складається з амбулаторії №1 та стаціонару (який у цьому проекті розглянутий не буде), амбулаторія №2, в яку входить багато додаткових відділів, з них дитяча поліклініка та бухгалтерське відділення будуть розглянуті у проекті, та амбулаторія №3, яка знаходиться на відстані 700м – 1км від головної будівлі та розташована у багатоповерховому житловому будинку, на першому поверсі.

Топологічна схема розглянутих відділів була побудована спираючись на інформацію, що містилася безпосередньо в амбулаторії №1 і №2 (Додаток А). На рисунках 1.3 – 1.5 (сторінка 15 - 17) представлена топологічна схема першого та другого поверху амбулаторії №1 та топологічна схема бухгалтерського відділу (амбулаторії №2). Топологічна схема дитячої поліклініки представлена на рисунку 1.6 (сторінка 18).



Рисунок 1.3 – Топологічна схема першого поверху амбулаторії №1

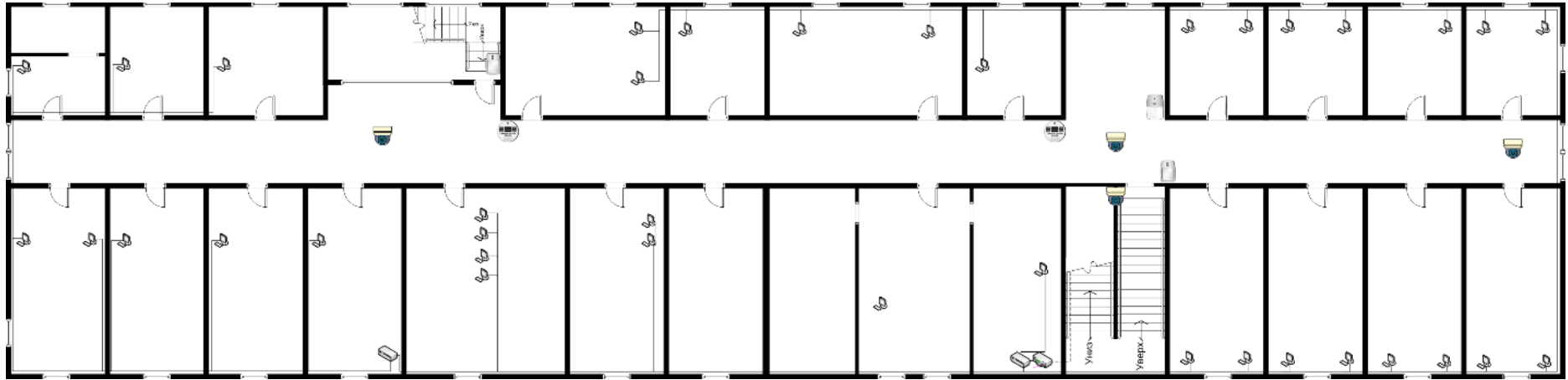


Рисунок 1.4 – Топологічна схема другого поверху амбулаторії №1

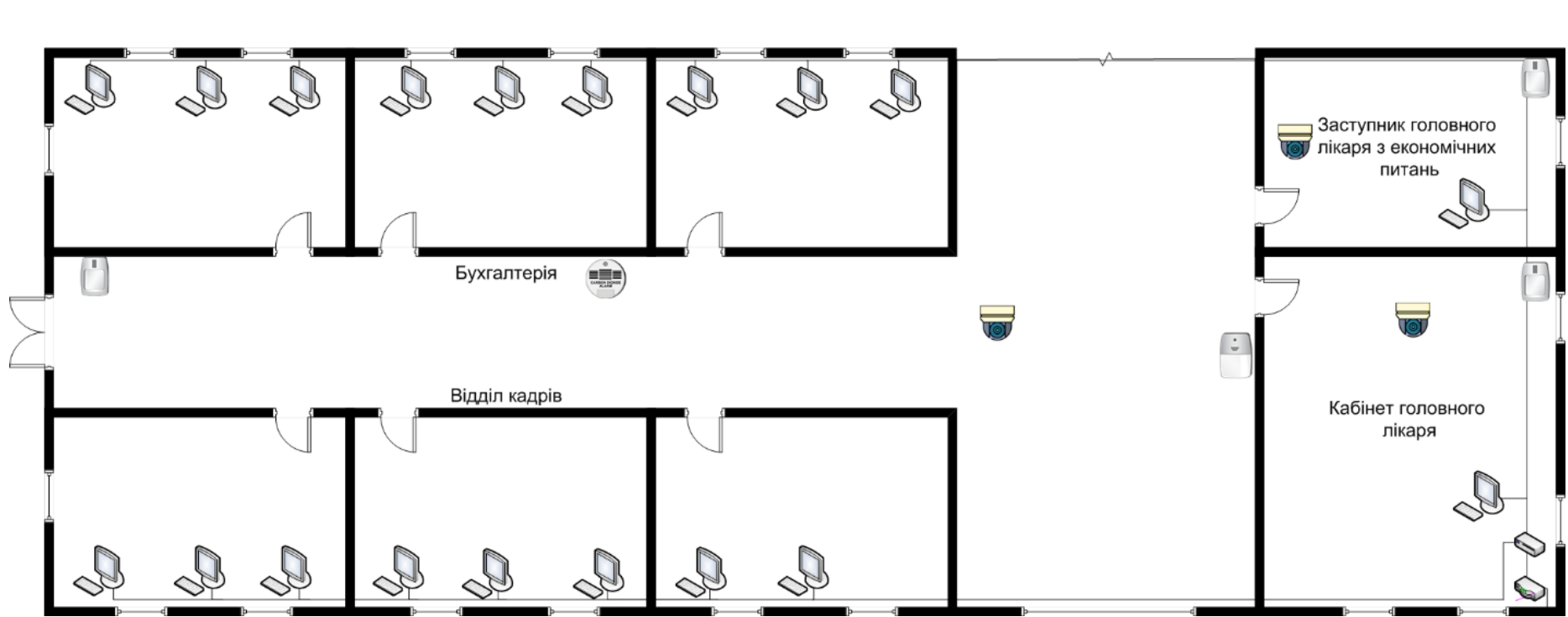


Рисунок 1.5 – Топологічна схема бухгалтерського відділення,
амбулаторія №2



Рисунок 1.6 – Топологічна схема дитячої поліклініки, амбулаторія №2

На першому поверсі амбулаторії №1 розташована реєстратура, гардеробна, підсобне приміщення, аптека та кабінети лікарів. Розмір першого поверху 50 м на 20 м. Другий поверх представлений тільки кабінетами лікарів, розмір - 60 м на 20 м. Бухгалтерський відділ в амбулаторії №2 представлений кабінетом головного лікаря та заступника головного лікаря з економічних питань, бухгалтерією та відділом кадрів, розмір – 30 м на 15 м У дитячій поліклініці в амбулаторії №2 розташована рецепція, кабінет старшої медичної сестри та кабінети лікарів. Розміри дитячої поліклініки – 42 м на 15 м.

1.4 Принципи та технічні методи керування КЗ «Першотравенська центральна міська лікарня»

Проектування ефективної та надійної мережі в закладі ОЗ вимагає застосування ряду принципів та технічних методів, щоб забезпечити безперебійний доступ до медичних даних та відповідати всім необхідним стандартам безпеки.

1. Принципи мережевого проектування:

- Сегментація мережі: Бухгалтерський відділ буде поділений на сегменти: «Для бухгалтерії», «Для відділу кадрів» та «Для гостей». Для сегментації використаємо VLAN (віртуальні локальні мережі). VLAN дозволяє логічно розділити пристрої на основі таких факторів, як відділ, місцезнаходження, функція або вимоги до безпеки. Кожен VLAN працює як окрема віртуальна мережа, що покращує безпеку і зменшує обсяг потенційних проблем мережі [8]. Наприклад, один VLAN може відокремити бухгалтерію, тоді як інший VLAN дозволяє базовий доступ до Wi-Fi для гостей.

- Резервування: Сервер TFTP виконуватиме функцію резервного копіювання конфігурацій мережевих пристроїв для подальшого їх відновлювання у разі збою.

2. Технічні методи:

- VPN та шифрування: Віртуальна приватна мережа буде налаштована через site-to-site VPN з використанням IPsec для трафіку, що проходить між основною мережею, тобто амбулаторії №1 та №2, та віддаленою мережею, тобто амбулаторії №3, через Internet.

1.5 Аналіз процесу керування і визначення якісних задач

Медичний персонал активно використовує комп'ютерні системи для підвищення ефективності своєї роботи та якості надання медичних послуг. Потрібно розуміти для яких задач будуть використовуватися мережі у закладі ОЗ.

Сімейний лікар:

- планування прийомів;
- виписування направлень до спеціаліста.

Лікар:

- перевірка записів на прийом;
- записи у електронний журнал;
- перевірка наявності ліків в мережі аптек;
- виписування рецептів.

Старша медична сестра:

- планування розкладу роботи медсестер;
- керування кадровим складом;
- замовлення препаратів.

Денний стаціонар:

- управління записами пацієнтів;
- планування процедур;
- моніторингу стану пацієнтів.

Дитяча поліклініка:

- ведення медичних карток дітей;

- освітні програми та ігри, які допомагають у лікуванні та реабілітації.

Аптека:

- ведення обліку ліків;
- управління запасами;
- обробка рецептів.

Бухгалтерський відділ:

- ведення «головної книги»;
- облік зобов'язань;
- створення звітів;
- розрахунок зарплати.

Відділ кадрів:

- автоматизація процесів управління персоналом.

1.6 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови КЗ «Першотравенська центральна міська лікарня», відомих рішень у галузі, що розглядається

Галузь ОЗ активно розвивається завдяки технологічним інноваціям у сфері обробки та передачі інформації. Відомі такі рішення у галузі:

1. Електронні медичні карти - ЕМК дозволяють лікарям та медичним працівникам ефективно зберігати, передавати та обмінюватися медичними даними пацієнтів. ЕМК включають інформацію про діагнози, результати аналізів, призначені лікування та інші важливі дані. ІС Helsi, яка буде використовуватися у цій комп'ютерній системі має можливість створювання та ведення електронних карток.

2. Мобільні медичні додатки - різні мобільні додатки допомагають пацієнтам керувати своїм здоров'ям, відстежуючи фізичну активність, харчування, ліки тощо. Додатки можуть також надавати доступ до медичних карт та консультацій. Helsi також має свій мобільний додаток.

3. Інтернет речей (IoT) в ОЗ - пристрої, які підключені до інтернету, можуть відстежувати життєві показники пацієнтів, такі як серцевий ритм, тиск, рівень глюкози в крові та ін. Ці дані можуть бути передані лікарям для моніторингу стану пацієнтів у реальному часі. Також IoT поширено використовується у системах безпеки. У цій системі IoT буде використовуватися для забезпечення відеоспостереження та пожежної безпеки.

4. Хмарні технології - хмарні технології дозволяють ефективно зберігати та обмінюватися медичними даними. У системі буде використовуватися пошта та Heli.

1.7 Мета роботи, що виконується

Мета роботи: Проектування комп'ютерної мережі КЗ «Першотравенська центральна міська лікарня» для підтримки роботи медичних сервісів загального вжитку, а також забезпечення обміну медичними, економічними та даними системи безпеки між відділами.

Для досягнення поставленої мети потрібно виконати наступні задачі:

1. Провести аналіз діяльності КЗ ОЗ «Першотравенська центральна міська лікарня» як господарчого об'єкта;
2. Скласти технічні вимоги на проектування КМ закладу;
3. Сформуванати структурну схему комплексу технічних засобів комп'ютерної системи.
4. Розробити специфікацію апаратних засобів підсистеми контролю, у тому числі засобів збору та передачі даних;
5. Виконати вибір відповідного фізичного середовища, кабелів, портів і з'єднувачів для підключення мережевих пристроїв до інших пристроїв мережі і вузлів, вибір мережевих пристроїв і компонентів, необхідних для задоволення технічних вимог мережі;
6. Виконати розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі;

7. Розрахувати налаштування для заданої топології мережі, а саме, вибір інтерфейси каналів зв'язку та протоколи обміну;
8. Розробити логічну топологічну схему мережі;
9. Розрахувати налаштування маршрутизації комп'ютерної мережі:
10. Розробити методи та налаштування обладнання для захисту інформації в системі;
11. Розробити компонент системи, а саме Інтернет речей у мережі.

1.8 Визначення можливих напрямків рішення поставлених завдань

1. Вибір провайдера: Усі приміщення знаходяться на не дуже великій відстані один від одного, тому дуже висока швидкість тут буде зайвою. У місті Першотравенськ доступно небагато провайдерів: Візіт, Київстар, Укртелеком та Vodafone. Візіт та Укртелеком мають дуже погані відгуки [7], тому обираємо Київстар, так як він має найвищий рейтинг з вказаних вище провайдерів. КМ КЗ «Першотравенська центральна міська лікарня» має віддалену амбулаторію №3, підключення якої може бути складним. Амбулаторія №3 не має підрозділів, яким потрібне високошвидкісне з'єднання з головними відділами. До її складу входять реєстратура, 3 кабінети сімейних лікарів, ординаторська та маніпуляційний кабінет.

2. Лікарня за умовою працює з Helse, яка являється однією з найбільших медичних ІС в Україні. Через цю систему було укладено понад 17 мільйонів декларацій між лікарями та пацієнтами. Системою користуються понад 1300 закладів ОЗ та 42 000 лікарів по всій Україні. Helse надає пацієнтам можливість швидко та зручно записатися на прийом до лікаря, проходити діагностику, аналізи, вакцинацію та замовляти медикаменти.

3. За вимогами організації вибір мережевого обладнання здійснюється серед обладнання компанії Cisco.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної 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

Комп'ютерна система КЗ «Першотравенська центральна міська лікарня» призначена для організації ефективного управління медичними процесами, забезпечення доступу до інформаційних ресурсів, а саме Helse. Забезпечення безпеки у закладі за допомогою IoT-речей.

Комп'ютерна мережа «КЗ «Першотравенська центральна міська лікарня» Дніпропетровської обласної ради» буде складатись з п'яти підмереж. Чотири підмережі розподілені між двома амбулаторіями (№1 та №2), та одна підмережа виділена на амбулаторію №3, згідно із загальною архітектурою мережі підприємства, наданою нам замовником (Додаток Б).

Розподілення підмереж:

LAN_1 (Віддалена) – Амбулаторія №3;

LAN_2 – Бухгалтерський відділ, амбулаторія №2;

LAN_3 – Перший поверх, амбулаторія №1;

LAN_4 – Другий поверх, амбулаторія №1;

LAN_5 – Дитяча поліклініка, амбулаторія №2.

У амбулаторій №1 на першому поверсі повинні бути розташовані HTTP та DNS сервери, сервер TFTP - у дитячій поліклініці амбулаторії №2.

Також у дитячій поліклініці амбулаторії №2 буде розташований сервер IoT, який буде збирати данні з датчиків та стани актуаторів. Для забезпечення безпеки

у лікарні – будуть створені сценарії керування IoT-пристроями, а саме: камерами відеоспостереження, детектори чадного газу, детекторів руху та сирен.

Розміщення IoT-пристроїв:

Перший поверх, амбулаторія №1 – 3 детектори чадного газу, 3 камери відеоспостереження, 2 детектори руху, 1 сирена;

Другий поверх, амбулаторія №1 – 2 детектори чадного газу, 4 камери відеоспостереження, 2 детектори руху, 1 сирена;

Бухгалтерський відділ, амбулаторія №2 – 1 детектор чадного газу, 3 камери відеоспостереження, 3 детектори руху, 1 сирена, IoT замок на двері;

Дитяча поліклініка, амбулаторія №2 – 3 детектори чадного газу, 4 камери відеоспостереження, 2 детектори руху, 1 сирена.

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

Система закладів ОЗ мають бути обладнані цілодобовим доступом до телефонної мережі, мережі Інтернет та інших систем зв'язку згідно з медичним завданням.

В приміщеннях закладу має бути забезпечена наявність дротового Інтернету [9].

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

Система повинна мати взаємозв'язок із суміжними системами за допомогою мережевих інтерфейсів, таких як Ethernet. Wi-Fi та ZigBee будуть використовуватися для підключення IoT-речей до шлюзу IoT.

2.1.1.1.4 Вимоги до діагностування системи

У системі має бути передбачена можливість технічної діагностики пристроїв у системі. Для діагностики неполадок у системі можуть бути використані збережені налаштування пристроїв, перевірка фізичних кабелів.

2.1.1.1.5 Перспективи розвитку та модернізації системи

У системі має бути передбачена перспектива розвитку, наприклад поява нових вузлів у КМ через перебудови, або додавання нових відділів в лікарні. Через це потрібно врахувати можливість розширення мережі.

Модернізація системи передбачається розширенням підмережі першого поверху амбулаторії №1 до 145 вузлів, підмережі другого поверху до 64 вузлів, підмережі бухгалтерського відділу амбулаторії №2 до 90 вузлів, підмережі амбулаторії №3 до 41 вузла. Підмережа дитячої поліклініки амбулаторії №2, за завданням замовника запланована на 13 вузлів, але її рекомендовано розширити до 20 вузлів.

Для забезпечення всіх вузлів у підмережі, буде встановлено відповідну кількість комутаторів. З огляду на видане замовником завдання і кількість портів у комутаторів (24 порти FastEthernet і 2 порти GigabitEthernet), у підмережі першого поверху амбулаторії №1 LAN_3 буде встановлено 7 комутаторів, у підмережі другого поверху LAN_4 - 3 комутатори, в підмережі бухгалтерського відділу амбулаторії №2 LAN_2 - 5 комутаторів, в підмережі дитячої поліклініки амбулаторії №2 LAN_5 - 1 комутатор, в підмережі амбулаторії №3 LAN_1 - 3 комутатори.

До кожного з комутаторів, крім тих, що під'єднані до маршрутизаторів, буде під'єднано щонайменше 2 комп'ютери. У кожній з підмереж буде встановлено від 10 комп'ютерів.

2.1.1.2 Вимоги до показників призначення

Система має забезпечувати оптимальні умови для роботи обладнання. Вона повинна забезпечувати захист даних, що зберігаються на сервері, від втрат при збоях.

Крім того, комп'ютерна система має дозволяти користувачам підприємства підключатися до Інтернету, а саме до медичного ІС Helsi, для виконання їхніх робочих обов'язків.

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

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

1. Температура: 18 – 24 °C [10].
2. Відносна вологість від 25% до 60%.
3. Атмосферний тиск від 700мм рт. ст. до 800мм рт. ст.
4. Періодично повинно здійснюватись ретельне прибирання та дезінфекція.
5. В наявності повинні бути засоби протипожежної безпеки.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Кожне робоче місце має мати свою електричну мережу з розетками, що працюють на напрузі 230 В і частоті 50 Гц, обладнаними заземлювальним контактом типу TN-C та TN-C-S (у дитячій поліклініці амбулаторії №2). Також у наявності має бути резервне живлення, для випадку перебоїв у мережі, захист від струму короткого замикання та ізоляція.

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

Необхідно мати двох системних адміністраторів з бакалаврським ступенем вищої освіти за спеціальністю «Комп'ютерна інженерія», які мають досвід роботи з обладнанням від компанії Cisco та мають сертифікат CCNA (Cisco Certified Network Associate). Час роботи: 45 годин на тиждень, вихідні у суботу та неділю. Також можуть бути викликані на роботу в будь-який час у випадку надзвичайних ситуацій або проблем з системою. [11]

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

У наявності повинні бути запасні комутатори, маршрутизатори, кабелі для забезпечення можливості негайної заміни в разі виникнення аварійних ситуацій або виходу з ладу обладнання.

Розташування складу запасних виробів повинно бути в такому місці, щоб персонал мав до нього легкий доступ у разі необхідності.

2.1.1.3.5 Вимоги до регламенту обслуговування

Технічне обслуговування повинно проводитися відповідно до графіка, який передбачає перевірку і догляд за всіма технічними засобами, що використовуються, не рідше ніж раз у місяць або, за необхідності, частіше.

У технічне обслуговування входить перевірка з'єднання, працездатності та чистка комп'ютерів, серверів, комутаторів та маршрутизаторів.

2.1.1.4 Вимоги до патентної чистоти

Обладнання та програмне забезпечення повинно мати патентну чистоту на території України та охоронятись міжнародним законодавством

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до системи, пов'язані з особливими умовами її експлуатації

У зв'язку з наявністю воєнного стану, заклад повинен мати готовність до можливих перебоїв у електропостачанні, для чого необхідно бути обладнаним джерелом безперебійного живлення для серверів, яке буде діяти від години до двох, для запобігання втрати даних.

2.1.1.5.2 Вимоги до активного обладнання

Система має бути забезпечена:

1. Стаціонарними комп'ютерами з базовими портами та портом Fast Ethernet;
2. Маршрутизаторами з трьома портами Gigabit Ethernet та можливістю додавати модулі з портами Serial;
3. Комутаторами з двома портами Gigabit Ethernet та 24 портами Fast Ethernet;
4. Серверами з портами Fast Ethernet.
5. IoT шлюзами з чотирма портами Fast Ethernet, портом Internet та бездротовим з'єднанням через технологію Wi-Fi, ZigBee.

2.1.1.5.3 Вимоги до кабель-каналів та електричним розеткам

Для проведення кабелів будуть використовуватися настінні пластикові кабель-канали. Ширина і висота в перерізі становить від 10 до 60 мм.

Якщо це не порушує правила безпеки, то розетки, за європейським стандартом, встановлюються на відстані приблизно 30 см від підлоги. Ступінь захисту – IP22. Тип – F.

2.1.1.5.4 Вимоги до комунікаційного обладнання і його розташування

Комунікаційне обладнання у системі повинно розташовуватись у спеціальних приміщеннях або спеціалізованих настінних шафах, які будуть захищати його від фізичних пошкоджень та несанкціонованого доступу. Щоб уникнути перегрівання пристроїв, у приміщенні повинна бути вентиляція.

2.1.1.5.5 Вимоги до однорідності

Типи кабелів: мідні перехрестні та наскрізні. Стандарт не нижче категорії 5. Довжина не повинна перевищувати 100 метрів [12].

2.1.1.5.6 Вимоги до резервування

У разі виходу з ладу одного з маршрутизаторів – трафік буде переходити через інший, поки цей маршрутизатор не буде знову у працюючому стані. Три комутатори, які з'єднані трикутником у підмережі амбулаторії №3, можна використовувати для налагодження резервування мережі у випадку відмови одного з вузлів.

Резервні копії налаштувань маршрутизаторів будуть збережені на сервері TFTP.

2.1.1.5.7 Спеціальні вимоги за розсудом розроблювача чи замовника Системи

Схема топології мережі від замовника вказана у Додатку Б

2.1.2 Вимоги до функцій (задач), виконуваних системою

Комп'ютерна мережа складається з 5-ти підмереж: LAN_1 – LAN_5;

Кількість вузлів у кожній підмережі: 41, 90, 145, 64, 13 відповідно;

Блок адрес для виділення підмереж: 10.25.56.0/22;

Інтенсивність трафіку: $\mu = 203$ кадрів/с;

Блок адрес для каналів між маршрутизаторами: 10.1.7.0/24;

Зовнішня адреса HTTP-сервера: 209.165.200.4;

Вимоги до налаштування системи:

- Усім пристроям має бути назначена назва наприклад, Kryvlenia_Router_1;
- На всіх пристроях має бути назначений пароль cisco до консолі і vty;
- На всіх пристроях має бути назначений пароль class до привілейованого режиму;
- Усі паролі, що зберігаються у відкритому вигляді, пропонується під час налаштування моделі комп'ютерної системи зашифрувати;
- Має бути розроблений банер MOTD;
- Назначити на усіх лініях vty використання протоколу ssh;
- Призначити на всіх пристроях користувача, наприклад 123202_Kryvlenia, з паролем admincisco;
- В якості імені домена використати ім'я пристрою. Для шифрування даних створювати ключ RSA завдовжки 1024 біт;
- На DCE-інтерфейсах маршрутизаторів призначити встановлення значення тактової частоти – 128000;
- З метою збільшення пропускної здатності і надійності каналів в мережі LAN_1 на комутаторах виконати об'єднання фізичних ліній.
- Оголосити безпосередньо підключені мережі і відключити поширення оновлень маршрутизації на інтерфейси в локальні мережі;
- Для VLAN у LAN_2 налаштувати сумарний маршрут і оголосити його іншим маршрутизаторам;
- У мережі буде реалізований протокол OSPF. У цьому разі потрібно змінити еталонну пропускну спроможність для обчислення вартості за умовчанням для дозволу інтерфейсів Gigabit на значення = 1000;
- Задати пропускну спроможність на serial-інтерфейсах = 128 Кб/с, вартість метрики = 7500;

- Налаштувати маршрут за умовчанням на маршрутизаторі з прямим підключенням до інтернет-провайдера (ISP) і розповсюдити його через оновлення маршрутизації;

- Додати статичні маршрути так, щоб будь-які два комп'ютера мережі могли взаємодіяти один з одним.

Налаштувати всі маршрутизатори на підтримку служби AAA необхідно таким чином:

- Для перевірки підключень до VTY ліній на маршрутизаторі використовувати локальну базу даних користувачів;

- Для доступу до консолі використовувати аутентифікацію на основі протоколу RADIUS;

- RADIUS-сервер налаштувати наступним чином: ключове слово – radius123; в якості облікового запису користувачів використовувати ім'я пристрою з паролем admin123.

Функції мережі амбулаторії №3, віддаленої мережі, LAN_1:

- У сімейних лікарів має бути доступ до IC Helse, завдяки якому вони зможуть отримувати записи на прийоми.

Функції мережі бухгалтерського відділу амбулаторії №2, LAN_2:

- Головний лікар повинен отримувати звіти з заступників головного лікаря;

- У головного лікаря має бути доступ до IC Helse для управління розкладом лікарів та налаштування прав доступу для працівників;

- Бухгалтерія повинна отримувати звіти з фінансової діяльності для введення фінансового обліку та відправки звітів до заступника головного лікаря з економічних питань;

- Відділ кадрів повинен здійснювати підбор і розстановку кадрів за діловими якостями;

- У відділу кадрів має бути доступ до Helse для конструктору бланків та форм прийняття нових працівників;

- Заступник головного лікаря з економічних питань повинен отримувати звіти з відділку кадрів та бухгалтерії;

- IoT-пристрої повинні відправляти статус роботи до IoT-серверу та отримувати з нього правила дії.

Функції мережі першого поверху амбулаторії №1, LAN_3:

- DNS-сервер повинен розпізнавати доменне ім'я та розподіляти запити, перенаправляти на <http://209.165.200.4> при вводі <http://123.dnipro.ua>;

- HTTP-сервер повинен відкривати веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу студента.

- Лікарі повинні мати доступ до Helse для перевірки записів на прийом, ведення історії хвороби пацієнтів та ЕМК (електронних медичних карток);

- Аптека повинна мати доступ до Helse для обліку медичних препаратів та ведення оплат;

- IoT-пристрої повинні відправляти статус роботи до IoT-серверу та отримувати з нього правила дії.

Функції мережі другого поверху амбулаторії №1, LAN_4:

- Лікарі повинні мати доступ до Helse для перевірки записів на прийом, ведення історії хвороби пацієнтів та ЕМК (електронних медичних карток);

- IoT-пристрої повинні відправляти статус роботи до IoT-серверу та отримувати з нього правила дії.

Функції мережі дитячої поліклініки амбулаторії №5, LAN_5:

- IoT-сервер повинен зберігати стани IoT-пристроїв, та мати змогу налаштування правил функціонування IoT-пристроїв;

- TFTP-сервер повинен отримувати файли конфігурації мережевих пристроїв;

- Старша медична сестра повинна мати доступ до Helse для планування розкладу роботи медсестер, обліку медичних препаратів та замовлення нових;

- У сімейних лікарів має бути доступ до ІС Helse, завдяки якому вони зможуть отримувати записи на прийоми.

– IoT-пристрої повинні відправляти статус роботи до IoT-серверу та отримувати з нього правила дії.

Функції IoT сегменту мережі:

- Забезпечення відеоспостереження за допомогою камер;
- У разі несанкціонованого доступу у підприємство, камери починають запис;
- При перевищенні показників чадного газу – вмикається сирена;
- При несанкціонованому доступі до бухгалтерського відділу, камери починають запис, двері зачиняються та вмикається сирена.

2.1.3 Вимоги до видів забезпечення

2.1.3.1 Вимоги до інформаційного забезпечення системи

Інформація в системі зберігатиметься на серверах та IC Helsei.

Сервер IoT зберігатиме інформацію о підключених до системи IoT-речах, їх статус та данні з них.

TFTP сервер зберігатиме файли конфігурації для їх відновлення на пристроях у разі збою.

2.1.3.2 Вимоги до лінгвістичного забезпечення системи

На всіх кінцевих пристроях повинна бути українська та англійська мова. При програмуванні MCU буде використовуватися мова програмування Python.

2.1.3.3 Вимоги до організаційного забезпечення

Основне завдання контролю за ефективністю роботи комп'ютерної системи покладається на системного адміністратора підприємства. Система поділятиметься на окремі відділи користувачів, які матимуть різний рівень доступу у мережі. Для поділення користувачів у різні групи – будуть використовуватися віртуальні локальні мережі (VLAN).

Кожна група користувачів матиме свою документацію та інструкцію яка матиме таку інформацію: як працювати з встановленими програмами, перелік сайтів з логіном та паролем для входу в систему, принцип роботи мережевого обладнання та куди потрібно звертатися у разі проблем з доступом до мережі.

Для захисту від помилок дій персоналу системи – будуть проводитись технічне обслуговування, під час яких будуть зроблені резервні копії на вузлах мережі

2.1.3.4 Вимоги до методичного забезпечення

У системі повинні бути такі документації та інструкції:

- Керівництво оператора - цей документ надає інструкції для фахівців, які використовують систему. Він описує процедури роботи, налаштування та усунення неполадок.

- Інструкція користувача - ця документація призначена для медичного персоналу, який використовує систему. Вона пояснює, як користуватися різними функціями.

- План приміщення

- Технічна документація - надає детальну інформацію про технічні аспекти системи. Сюди входять описи архітектури, баз даних, інтеграцій, безпеки та інші технічні деталі.

- Документація з підтримки - включає відповіді на часті запитання, рекомендації щодо усунення проблем та контактні дані служби підтримки.

- Документація процедур та стандартів - описує стандарти та процедури, які використовуються в закладі охорони здоров'я. Це може включати правила обробки даних, безпеки, ведення медичної документації та інше.

- Документація з безпеки - забезпечує інформацію про заходи безпеки, захист від несанкціонованого доступу.

2.2 Розробка апаратної частини комп'ютерної системи

2.2.1 Взаємодія користувачів з мережевими ресурсами і сервісами

Лікарі, які працюють у КЗ «Першотравенська центральна міська лікарня», матимуть доступ до стаціонарних комп'ютерів у яких повинен бути доступ до інтернету та медичного ІС Helsi.

Системні адміністратори матимуть доступ до серверів, на яких будуть налаштовані сервіси: HTTP, DNS, TFTP та ІоТ (кожен з серверів буде налаштований на один з сервісів).

Більш детальний огляд взаємодії користувачів розглянутий у таблиці 2.1.

Таблиця 2.1 – Взаємодія користувачів у мережі

№	Взаємодія	Вхід/вихід з мережі	Вид інформації	Джерело	Отримувач
LAN_1, мережа амбулаторії №3					
1.	Вхід до ІС Helsi	Вихід	Запит	ПК сімейного лікаря	Сервера Helsi
2.	Отримування записів на прийом	Вхід	Прийом	Сервера Helsi	ПК сімейного лікаря
3.	Запис направлень до спеціалістів	Вихід	Запис	ПК сімейного лікаря	Сервера Helsi
4.	Введення звіту про роботу	Вихід	Запис	ПК сімейного лікаря	Сервера Helsi
LAN_2, мережа бухгалтерського відділу амбулаторії №2					
5.	Вхід до ІС Helsi	Вихід	Запит	ПК у бухгалтерії	Сервера Helsi
6.	Отримування звітів про роботу працівників та витрати	Вхід	Прийом	Сервера Helsi	ПК у бухгалтерії
7.	Відправка звіту о витратах лікарні	Вихід	Електронний лист	Бухгалтерія	ПК заступника головного лікаря з економічних питань
8.	Вхід до ІС Helsi	Вихід	Запит	ПК у відділі кадрів	Сервера Helsi
9.	Використання конструктору бланків та форм прийняття нових працівників	Вихід	Запис	Відділ кадрів	Сервера Helsi
10.	Отримання заяв на роботу	Вхід	Електронний лист	ПК клієнтів	ПК відділу кадрів

Продовження таблиці 2.1

№	Взаємодія	Вхід/вихід з мережі	Вид інформації	Джерело	Отримувач
11.	Відправка звіту о нових працівників	Вихід	Електронний лист	Відділ кадрів	ПК заступника головного лікаря з економічних питань
12.	Отримування звіту о витратах в лікарні	Вхід	Електронний лист	Бухгалтерія	ПК заступника головного лікаря з економічних питань
13.	Отримування звіту о нових працівників	Вхід	Електронний лист	Відділ кадрів	ПК заступника головного лікаря з економічних питань
14.	Відправка звітів	Вихід	Електронний лист	ПК заступника головного лікаря з економічних питань	ПК головного лікаря
15.	Вхід до IC Helsi	Вихід	Запит	ПК головного лікаря	Сервера Helsi
16.	Налаштування прав працівників	Вихід	Запис	ПК головного лікаря	Сервера Helsi
17.	Управління розкладом лікарів	Вихід	Запит	ПК головного лікаря	Сервера Helsi
18.	Отримання звіту з головної медичної сестри	Вхід	Електронний лист	ПК головної медичної сестри	ПК головного лікаря
19.	Отримання звітів з заступників	Вхід	Електронний лист	Заступники головного лікаря	ПК головного лікаря
20.	Інформація з датчиків	Вихід	Данні	ІоТ датчики	Сервер ІоТ
21.	Дія ІоТ речей	Вхід	Данні	Сервер ІоТ	ІоТ речі
22.	Запис камер	Вихід	Данні	ІоТ камери	Сервер ІоТ
LAN_3, мережа першого поверху амбулаторії №1					
23.	Отримування запитів на доменне ім'я http://123.dnipro.ua	Вхід	Запит	Користувачі	DNS сервер
24.	Перенаправлення на HTTP сервер	Вихід	Запит	DNS сервер	HTTP сервер

Продовження таблиці 2.1

№	Взаємодія	Вхід/вихід з мережі	Вид інформації	Джерело	Отримувач
25.	Отримування запитів на адресу http://209.165.200.4	Вхід	Запит	Користувачі	НТТР сервер
26.	Відправка інформації з серверу	Вихід	Прийом	НТТР сервер	Користувачі
27.	Вхід до ІС Helsi	Вихід	Запит	ПК лікаря	Сервера Helsi
28.	Отримування записів на прийом	Вхід	Прийом	Сервера Helsi	ПК лікаря
29.	Отримування історії хвороби пацієнта	Вхід	Прийом	Сервера Helsi	ПК лікаря
30.	Ведення історії хвороби пацієнта	Вихід	Запис	ПК лікаря	Сервера Helsi
31.	Отримування ЕМК пацієнта	Вхід	Прийом	Сервера Helsi	ПК лікаря
32.	Запис у ЕМК пацієнта	Вихід	Запис	ПК лікаря	Сервера Helsi
33.	Введення звіту про роботу	Вихід	Запис	ПК лікаря	Сервера Helsi
34.	Вхід до ІС Helsi	Вихід	Запит	ПК в аптці	Сервера Helsi
35.	Облік медичних препаратів та ведення оплати	Вихід	Запис	ПК в аптеці	Сервера Helsi
36.	Інформація з датчиків	Вихід	Данні	ІоТ датчики	Сервер ІоТ
37.	Дія ІоТ речей	Вхід	Данні	Сервер ІоТ	ІоТ речі
38.	Запис камер	Вихід	Данні	ІоТ камери	Сервер ІоТ
LAN_4, мережа другого поверху амбулаторії №1					
39.	Вхід до ІС Helsi	Вихід	Запит	ПК лікаря	Сервера Helsi
40.	Отримування записів на прийом	Вхід	Прийом	Сервера Helsi	ПК лікаря
41.	Отримування історії хвороби пацієнта	Вхід	Прийом	Сервера Helsi	ПК лікаря
42.	Ведення історії хвороби пацієнта	Вихід	Запис	ПК лікаря	Сервера Helsi
43.	Отримування ЕМК пацієнта	Вхід	Прийом	Сервера Helsi	ПК лікаря
44.	Запис у ЕМК пацієнта	Вихід	Запис	ПК лікаря	Сервера Helsi
45.	Введення звіту про роботу	Вихід	Запис	ПК лікаря	Сервера Helsi
46.	Інформація з датчиків	Вихід	Данні	ІоТ датчики	Сервер ІоТ
47.	Дія ІоТ речей	Вхід	Данні	Сервер ІоТ	ІоТ речі
48.	Запис камер	Вихід	Данні	ІоТ камери	Сервер ІоТ
LAN_5, мережа дитячої поліклініки амбулаторії №2					
49.	Вхід до ІС Helsi	Вихід	Запит	ПК сімейного лікаря	Сервера Helsi
50.	Отримування записів на прийом	Вхід	Прийом	Сервера Helsi	ПК сімейного лікаря

Продовження таблиці 2.1

№	Взаємодія	Вхід/вихід з мережі	Вид інформації	Джерело	Отримувач
51.	Запис направлень до спеціалістів	Вихід	Запис	ПК сімейного лікаря	Сервера Helsi
52.	Введення звіту про роботу	Вихід	Запис	ПК сімейного лікаря	Сервера Helsi
53.	Вхід до IC Helsi	Вихід	Запит	ПК старшої медичної сестри	Сервера Helsi
54.	Отримування звітів о праці медичних сестер	Вхід	Прийом	Сервера Helsi	ПК старшої медичної сестри
55.	Отримування звітів з аптери	Вхід	Прийом	Сервера Helsi	ПК старшої медичної сестри
56.	Відправка звітів головному лікарю	Вихід	Електронний лист	ПК старшої медичної сестри	ПК головного лікаря
57.	Інформація з датчиків	Вихід	Данні	IoT датчики	Сервер IoT
58.	Отримання інформації з датчиків	Вхід	Данні	IoT датчики	Сервер IoT
59.	Передача правил дій для IoT речей	Вихід	Данні	Сервер IoT	IoT речі
60.	Дія IoT речей	Вхід	Данні	Сервер IoT	IoT речі
61.	Запис камер	Вихід	Данні	IoT камери	Сервер IoT
62.	Отримання та зберігання запису з камер	Вхід	Данні	IoT камери	Сервер IoT

2.2.2 Обстеження об'єкту розробки з метою аналізу всіх способів внутрішнього і зовнішнього доступу до інфраструктури мережі

Використовуючи розроблені вимоги до функції та задану замовником топологію мережі (Додаток Б) формуємо структурну схему комплексу технічних засобів комп'ютерної системи КЗ «Першотравенська центральна міська лікарня» (рисунок 2.1, сторінка 40).

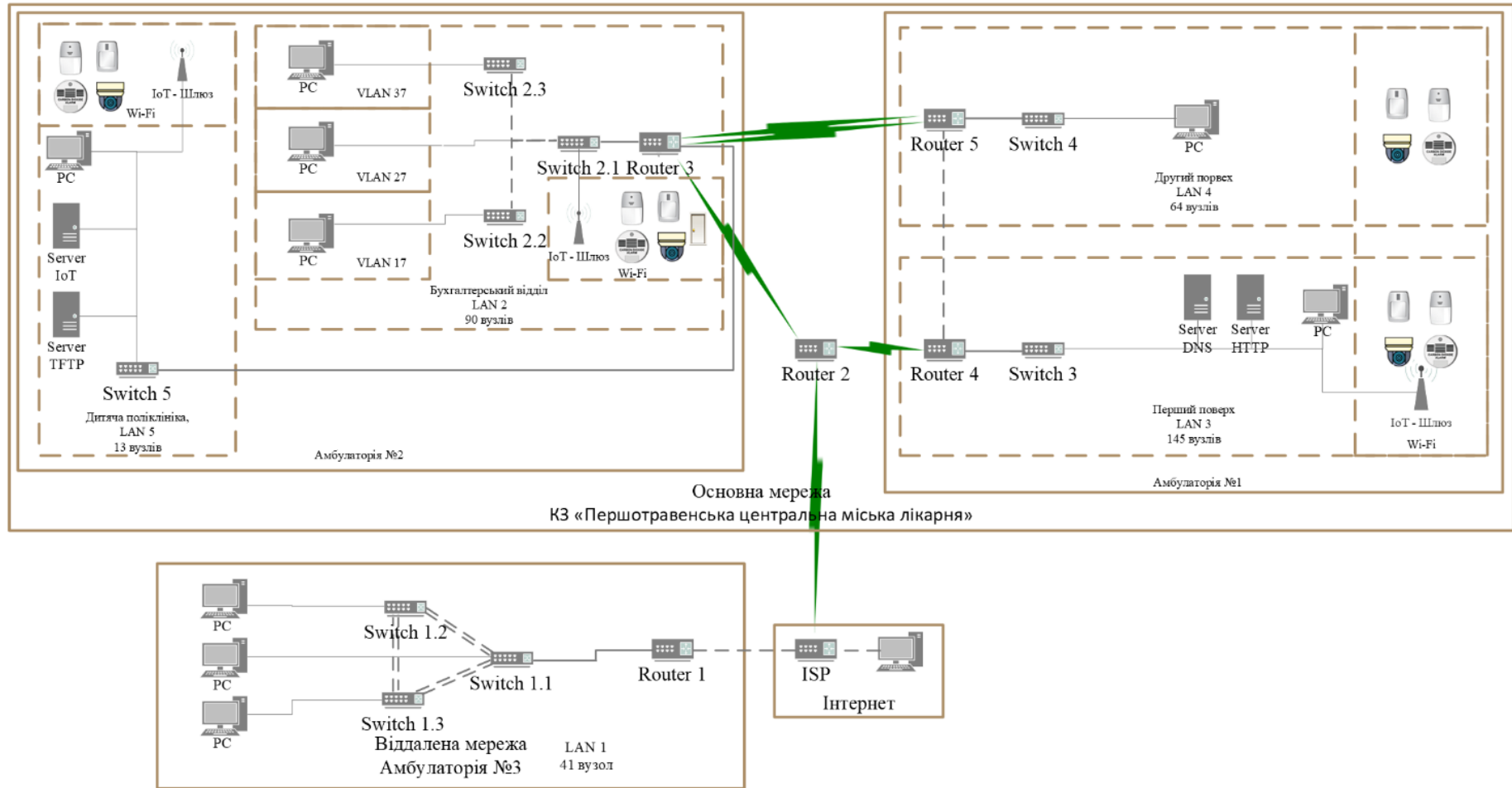


Рисунок 2.1 - Структурна схема комплексу технічних засобів комп'ютерної системи КЗ «Першотравенська центральна міська лікарня»

2.2.3 Аналіз об'єкту проектування та розробка специфікації апаратних засобів комп'ютерної системи

Комп'ютерній система КЗ «Першотравенська центральна міська лікарня» розраховується на 353 вузла. З них: комутатори – 15 од., IoT-речі – 37 од., шлюзи IoT – 3 од., сервери – 4 од. Маршрутизатори між собою з'єднані Serial DTE або крос-кабелями. Комутатори між собою з'єднані крос-кабелем. Прилади різного виду з'єднані прямим кабелем. IoT-речі з'єднані з шлюзом IoT через Wi-Fi, ZigBee.

Технічні характеристики та кількість пристроїв наводиться у таблиці 2.2.

Таблиця 2.2 - Специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
1.	Маршрутизатор Cisco 2911, 3 вбудовані порти 10/100/1000 Ethernet (RJ-45), Слот(и) розширення: 1 слот сервісного модуля 1 слот внутрішнього сервісного модуля 2 слоти для вбудованого цифрового сигнального процесора (DSP) 4 розширені слоти для високошвидкісних інтерфейсних карт WAN, Оперативна пам'ять 512 МБ (встановлена) / 2 ГБ (макс.), Флеш-пам'ять 256 МБ (встановлена) / 8 ГБ (макс.), Необхідна напруга: АС 120/230 В (50/60 Гц)	CISCO2911/K9	од.	6	Використовується у всіх підмережах. Докладніше у [13]

Продовження таблиці 2.2

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
2.	Інтерфейсний модуль для маршрутизаторів Cisco HWIC-2T, 2-портова послідовна плата WAN-інтерфейсу	HWIC-2T	од.	7	Доповнює маршрутизатори 2-ма Serial портами. На Router 3 та Router 2 стоїть 2 модуля
3.	Комутатор Cisco 2960-24TT-L, Інтерфейси висхідних ліній: 2 x 10/100/1000 TX висхідних ліній, Порти: 24 x Ethernet 10/100 порти, Пропускна здатність: 6,5 Мбіт/с, Пропускна здатність задньої панелі: 16 Гбіт/с, Оперативна пам'ять: 16 МБ	WS-C2960-24TT-L	од.	19	Докладніше у [14]
4.	Комп'ютер ARTLINE Business B27 v65, Intel Core i3-12100 (3.3 - 4.3 ГГц), RAM: 8 ГБ, SSD: 480 ГБ, Intel UHD Graphics 730, DVD+,-RW, LAN, без ОС (буде встановлена Windows 11 Pro)	ARTLINE Business B27 v65	од.	293	
5.	Шлюз IoT Aqara M2 EU Провідні інтерфейси: LAN Бездротовий стандарт: Bluetooth, Wi-Fi, ZigBee	Aqara M2	од.	3	

Продовження таблиці 2.2

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
6.	Сервер UCS C220 M4 SFF Процесор: 2 шт x Intel Xeon E5-2650L v2, 1.70-2.10 GHz, 10-Core, 25MB, 70W, 1600, Оперативна пам'ять: 8 GB DDR3 (2 x 4 GB), RAID-контролер: Cisco UCS RAID SAS 2008M-8i, Мережевий контролер: 2x порта 1 Gb Ethernet, Віддалений доступ: Cisco Integrated Management Controller (CIMC), Блок живлення: 2 x 650 W SSD: 2 x 480 GB Жорсткий диск: 2 x 2 TB	Cisco UCS C220 M4 SFF	од.	4	HTTP, DNS, TFTP та IoT сервери
7.	IP-камера Imou IPC-TA22CP-D, Інтерфейси: Wi-Fi, Роздільна здатність камери: 1.3 Мп, Роздільна здатність відео: 1280x960, Розмір матриці: 1/2.8", Частота запису: 25 кадрів/с	Imou IPC-TA22CP-D	од.	14	
8.	Датчик диму та чадного газу Wi-Fi Tuuya	Wi-Fi Tuuya Smart Tuuya	од.	9	
9.	Датчик руху Nous E2, Протокол: Zigbee3.0 Тип бездротової передачі: WiFi IEEE 802.15.4	Nous E2	од.	9	
10.	Сирена WiFi TUYA (NAS-AB02W) Звук: максимум 100 дБ на відстані 1 метра	TUYA (NAS-AB02W)	од.	4	
11.	Розумний замок Aquara Smart Lock U100 Протокол: Zigbee 3.0, Bluetooth 5.0	Aquara Smart Lock U100	од.	1	

На рисунках 1.3 – 1.6 вказана топологічна схема будівель у яких буде налаштовуватися комп'ютерна система. Розміри будівель вказані у пункті 1.3 на сторінці 14, до цього добавимо розміри амбулаторій №3 – 10м на 10м. Враховуючи ці данні та можливе розширення системи створимо специфікацію структурованої кабельної мережі (таблиця 2.3).

Таблиця 2.3 – Специфікація структурованої кабельної мережі

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
1.	Кабельний канал, настінний, Матеріал: ПВХ, 16мм на 25мм, довжина 2 м	Expert	од.	300	
2.	Лан кабель, патч-корд, Категорія кабелю: Cat 5e, Інтерфейси: RJ-45 Тип кабелю: UTP	Cablexpert	м	600	
3.	Комп'ютерна розетка Schneider Electric Asfora RJ45 5 категорія	Schneider Electric Asfora	од.	30	
4.	Розетка подвійна із заземленням 230В, 50 Гц, IP22	ElectroHouse Enzo	од.	200	
5.	Кабель живлення ПВС 3х1	Одескабель	м	100	
6.	Комутаційна коробка		од.	10	

2.2.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі

Згідно з вимогами: Середня довжина вихідного повідомлення в найбільшій мережі складає 650 байт, найбільша мережа складається з 145 вузлів, середня інтенсивність трафіку дорівнює 203 кадрів/с. Вимоги до затримки передачі пакету в найбільшій мережі – ≤ 6 мс.

Розрахуємо пропускну здатність мережі на рівні доступу:

$$P_{p.p} = \mu * N * l * 8 = 203 * 145 * 650 * 8 = 153,062 \text{ Мбіт/с}, \quad (2.1)$$

де μ – середня інтенсивність трафіку, кадрів/с;

N – кількість вузлів у найбільшій мережі;

l – середня інтенсивність трафіку, байт.

Далі розрахуємо значення інтенсивності виходу. Зазначимо, що швидкість, з якою в мережі пересилається трафік до маршрутизаторів дорівнює 1000 Мбіт/с.

Розрахунок значення інтенсивності виходу:

$$\mu_{\text{вих}} = \frac{C}{l * 8} = \frac{1\,000\,000\,000}{(650 * 8)} = 192\,308 \text{ пакетів/с}, \quad (2.2)$$

де C – пропускну здатність лінії передачі даних, біт/с;

l – середня довжина повідомлення, байт.

Розрахуємо максимальну кількість вузлів, що може бути під'єднано до комутаторів у найбільшій мережі:

$$N = \frac{\mu_{\text{вих}}}{\mu} = \frac{192\,308}{203} = 947 \text{ вузлів} \quad (2.3)$$

Ця кількість вузлів більше ніж у найбільшій локальній мережі, тому вона нас задовольняє.

Розрахунок інтенсивності вихідного трафіку:

$$\lambda = \mu * N = 203 * 145 = 29\,435 \text{ пакетів/с} \quad (2.4)$$

Далі розраховуємо коефіцієнт затримки на рівні розподілу:

$$\rho = \frac{\lambda}{\mu_{\text{вих}}} = \frac{29\,435}{192\,308} = 0.153 \quad (2.5)$$

Розрахунок коефіцієнту зайнятості маршрутизатора:

$$r = \frac{\rho}{1 - \rho} = \frac{0.153}{1 - 0.153} = 0.181 \quad (2.6)$$

Розрахунок середньої затримки кадру:

$$T = \frac{1}{\mu_{\text{вих}} - \lambda} = \frac{1}{192\,308 - 29\,435} = 6.14 \text{ мкс} \quad (2.7)$$

Розрахунок середньої довжини черги:

$$L_{\text{чер}} = \frac{\rho^2}{1 - \rho} = \frac{0.024}{1 - 0.153} = 0.028 \text{ пакетів} \quad (2.8)$$

Розрахунок середнього часу перебування пакета в черзі:

$$T_{\text{оч}} = \frac{L_{\text{чер}}}{\lambda} = \frac{0.028}{29\,435} = 0.95 \text{ мкс} \quad (2.9)$$

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок адресації комп'ютерної мережі лікарні

Як було зазначено у вимогах, мережа Першотравенської Центральної Міської лікарні складається з 5-ти підмереж, які зазначені у таблиці 3.1

Таблиця 3.1 – Назви підмереж та кількість вузлів

№ Підмережі	Назва	Кількість вузлів
LAN_1	Амбулаторія №3	41
LAN_2	Бухгалтерський відділ, амбулаторія №2	90
LAN_3	Перший поверх, амбулаторія №1	145
LAN_4	Другий поверх, амбулаторія №1	64
LAN_5	Дитяча поліклініка, амбулаторія №2	13

Блок адрес для виділення підмереж – 10.25.56.0 з маскою /22 (255.255.252.0). Розробка адресації у мережі буде проводитися методом VLSM (Variable Length Subnet Mask). VLSM дозволяє використовувати IP-адреси ефективніше, з мінімальною витратою адрес.

Для розрахунку методом VLSM розставимо усі підмережі у порядку зменшення:

Перший поверх, амбулаторія №1 – 145 вузлів;

Бухгалтерський відділ, амбулаторія №2 – 90 вузлів;

Другий поверх, амбулаторія №1 – 64 вузлів;

Амбулаторія №3 – 41 вузол;

Дитяча поліклініка, амбулаторія №2 – 13 вузлів.

Для визначення маски для підмережі першого поверху потрібно взяти потрібну кількість бітів. Наприклад, підмережа першого поверху не зможе вміститися, якщо взяти 7 бітів, так як $2^7 = 128$, що менше ніж 145 (кількість вузлів у мережі першого поверху). Тому беремо 8 бітів:

LAN_3. Кількість вузлів: 145 – 8 біт

10.25.00111000.|00000000 /24 – 10.25.56.0/24 – номер мережі

10.25.00111000.|11111111 /24 – 10.25.56.255 /24 – широкомовна адреса

Далі беремо наступну по кількості вузлів підмережу. Тут вже підійде 7 бітів:

LAN_2. Кількість вузлів: 90 – 7 біт

10.25.00111001.0|00000000 /25 – 10.25.57.0/25 – номер мережі

10.25.00111001.0|11111111 /25 – 10.25.57.127 /25 – широкомовна адреса

Далі іде підмережа на 64 вузлів. Сюди 6 бітів ($2^6 = 64$) не підійде, так як 2 адреси не використовуються на вузлах, тому потрібно взяти на 1 біт більше:

LAN_4. Кількість вузлів: – 64 – 7 біт

10.25.00111001.1|00000000 /25 – 10.25.57.128 /25 – номер мережі

10.25.00111001.1|11111111 /25 – 10.25.57.255 /25 – широкомовна адреса

Розрахунок для підмережі амбулаторії №3:

LAN_1. Кількість вузлів: 41 – 6 біт

10.25.00111010.00|000000 /26 – 10.25.58.0/26 – номер мережі

10.25.00111010.00|111111 /26 – 10.25.58.63/26 – широкомовна адреса

Розрахунок для дитячої поліклініки в амбулаторії №2:

LAN_5. Кількість вузлів: 13 – 4 біт

10.25.00111010.0100|0000 /28 – 10.25.58.64/28 – номер мережі

10.25.00111010.0100|1111 /28 – 10.25.58.79/28 – широкомовна адреса

Але у цьому разі у мережу можливо буде додати тільки ще 1 вузол, тому для можливості розширення мережі – візьмемо на 1 біт більше:

10.25.00111010.010|00000 /27 – 10.25.58.64/27 – номер мережі;

10.25.00111010.010|11111 /27 – 10.25.58.95/27 – широкомовна адреса.

Результат розрахунків винесемо у таблиці 3.2, сторінка 49.

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
LAN_1	41	10.25.58.0	/26	10.25.58.1	10.25.58.62
LAN_2	90	10.25.57.0	/25	10.25.57.1	10.25.57.126
LAN_3	145	10.25.56.0	/24	10.25.56.1	10.25.56.254
LAN_4	64	10.25.57.128	/25	10.25.57.129	10.25.57.254
LAN_5	13 (20)	10.25.58.64	/27	10.25.58.65	10.25.58.94

Для з'єднання між маршрутизаторами використовується блок адрес: 10.1.7.0 з маскою /24. Згідно з архітектурою мережі, наданою замовником (Додаток Б), для підключення основної мережі до маршрутизатора інтернет провайдера (ISP) використовується блок адрес: 209.165.202.0/30, а для підключення до віддаленої мережі використовується блок адрес: 64.100.13.0/30. За методом VLSM, для розрахунку адрес з'єднань між маршрутизаторами достатньо взяти 2 біти (маска /30). Враховуючи ці дані, створимо таблицю 3.3.

Таблиця 3.3 – Схема адресації 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
WAN_1	2	10.1.7.0	/30	10.1.7.1	10.1.7.2
WAN_2	2	10.1.7.4	/30	10.1.7.5	10.1.7.6

Продовження таблиці 3.3

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
WAN_3	2	10.1.7.8	/30	10.1.7.9	10.1.7.10
WAN_4	2	10.1.7.12	/30	10.1.7.13	10.1.7.14
WAN_5	2	10.1.7.16	/30	10.1.7.17	10.1.7.18
ISP_1	2	209.165.202.0	/30	209.165.202.1	209.165.202.2
ISP_2	2	64.100.13.0	/30	64.100.13.1	64.100.13.2

Перші з можливих у підмережі адреси призначаються на інтерфейси маршрутизаторам. У мережі бухгалтерського відділу також будуть налаштовані VLAN, тому ця мережа буде поділена на 4 частини, кожна з яких матиме маску /27. Тому на маршрутизаторі, який підключений до бухгалтерського відділу будуть налаштовані підінтерфейси. Усі IP-адреси та інтерфейси на яких вони виставлені вказані у таблиці 3.4.

Таблиця 3.4 – Схема адресації на маршрутизаторах

Пристрій	Інтерфейс	IP-адреса	Маска
Kryvlenia_Router_1	Gig0/1	64.100.13.2	255.255.255.252
	Gig0/0	10.25.58.1	255.255.255.192
Kryvlenia_Router_2	Se0/0/0	209.165.202.2	255.255.255.252
	Se0/0/1	10.1.7.14	255.255.255.252
	Se0/1/0	10.1.7.17	255.255.255.252

Продовження таблиці 3.4

Пристрій	Інтерфейс	IP-адреса	Маска
Kryvlenia_Router_3	Se0/0/0	10.1.7.18	255.255.255.252
	Se0/1/0	10.1.7.1	255.255.255.252
	Se0/1/1	10.1.7.5	255.255.255.252
	Gig0/0.17	10.25.57.1	255.255.255.224
	Gig0/0.27	10.25.57.33	255.255.255.224
	Gig0/0.37	10.25.57.65	255.255.255.224
	Gig0/0.99	10.25.57.97	255.255.255.224
	Gig0/1	10.25.58.65	255.255.255.224
Kryvlenia_Router_4	Se0/0/0	10.1.7.13	255.255.255.252
	Gig0/0	10.1.7.10	255.255.255.252
	Gig0/1	10.25.56.1	255.255.255.0
Kryvlenia_Router_5	Se0/0/0	10.1.7.2	255.255.255.252
	Se0/0/1	10.1.7.6	255.255.255.252
	Gig0/0	10.1.7.9	255.255.255.252
	Gig0/1	10.25.57.129	255.255.255.128
Kryvlenia_ISP	Se0/0/1	209.165.202.1	255.255.255.252
	Gig0/0	209.165.201.1	255.255.255.240
	Gig0/1	64.100.13.1	255.255.255.252

Другі адреси призначаються комутаторам у підмережах. Серверам привласнюється адреса, яка дорівнює першій адресі у підмережі+9+7. Усі інші вузли отримують адресу за протоколом DHCP. Повна таблиця схема адресації пристроїв у мережі наведена у таблиці 3.5.

Таблиця 3.5 – Схема адресації пристроїв у мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Kryvlenia_Switch_1.1	-	10.25.58.2	/26	10.25.58.1	VLAN1	-
Kryvlenia_Switch_1.2	-	10.25.58.3	/26	10.25.58.1	VLAN1	-

Продовження таблиці 3.5

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Kryvlenia_Switch_1.3	SVI	10.25.58.4	/26	10.25.58.1	VLAN1	-
Kryvlenia_Switch_2.1	SVI	10.25.57.98	/27	10.25.57.97	VLAN99	-
	Fa0/24 – Fa0/15	-		10.25.57.1	VLAN17	-
	Fa0/14 – Fa0/10	-		10.25.57.33	VLAN27	-
	Fa0/9 – Fa0/5	-		10.25.57.65	VLAN37	-
Kryvlenia_Switch_2.2	SVI	10.25.57.99	/27	10.25.57.97	VLAN99	-
	Fa0/24 – Fa0/15	-		10.25.57.1	VLAN17	-
	Fa0/14 – Fa0/10	-		10.25.57.33	VLAN27	-
	Fa0/9 – Fa0/5	-		10.25.57.65	VLAN37	-
Kryvlenia_Switch_2.3	SVI	10.25.57.100	/27	10.25.57.97	VLAN99	-
	Fa0/24 – Fa0/15	-		10.25.57.1	VLAN17	-
	Fa0/14 – Fa0/10	-		10.25.57.33	VLAN27	-
	Fa0/9 – Fa0/5	-		10.25.57.65	VLAN37	-
Kryvlenia_Switch_2.4	SVI	10.25.57.101	/27	10.25.57.97	VLAN99	-
	Fa0/24 – Fa0/15	-		10.25.57.1	VLAN17	-
	Fa0/14 – Fa0/10	-		10.25.57.33	VLAN27	-
	Fa0/9 – Fa0/5	-		10.25.57.65	VLAN37	-
Kryvlenia_Switch_2.5	SVI	10.25.57.102	/27	10.25.57.97	VLAN99	-
	Fa0/24 – Fa0/15	-		10.25.57.1	VLAN17	-
	Fa0/14 – Fa0/10	-		10.25.57.33	VLAN27	-
	Fa0/9 – Fa0/5	-		10.25.57.65	VLAN37	-
Kryvlenia_Switch_3.1	SVI	10.25.56.2	/24	10.25.56.1	VLAN1	-
Kryvlenia_Switch_3.2	SVI	10.25.56.3	/24	10.25.56.1	VLAN1	-
Kryvlenia_Switch_3.3	SVI	10.25.56.4	/24	10.25.56.1	VLAN1	-
Kryvlenia_Switch_3.4	SVI	10.25.56.5	/24	10.25.56.1	VLAN1	-
Kryvlenia_Switch_3.5	SVI	10.25.56.6	/24	10.25.56.1	VLAN1	-
Kryvlenia_Switch_3.6	SVI	10.25.56.7	/24	10.25.56.1	VLAN1	-
Kryvlenia_Switch_3.7	SVI	10.25.56.8	/24	10.25.56.1	VLAN1	-
Kryvlenia_Switch_4.1	SVI	10.25.57.130	/25	10.25.57.129	VLAN1	-
Kryvlenia_Switch_4.2	SVI	10.25.57.131	/25	10.25.57.129	VLAN1	-

Продовження таблиці 3.5

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Kryvlenia_Switch_4.3	SVI	10.25.57.132	/25	10.25.57.129	VLAN1	-
Kryvlenia_Switch_5	SVI	10.25.58.66	/27	10.25.58.65	VLAN1	-
Server_HTTP	Fa0	10.25.56.17	/24	10.25.56.1	-	Fa0/3
Server_DNS	Fa0	10.25.56.18	/24	10.25.56.1	-	Fa0/4
Server_TFTP	Fa0	10.25.58.81	/27	10.25.58.65	-	Fa0/1
Server_IoT	Fa0	10.25.58.82	/27	10.25.58.65	-	Fa0/2
Kryvlenia_PC_1.1	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/5
Kryvlenia_PC_1.2	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/6
Kryvlenia_PC_1.3	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/7
Kryvlenia_PC_1.4	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/8
Kryvlenia_PC_1.5	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/5
Kryvlenia_PC_1.6	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/6
Kryvlenia_PC_1.7	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/7
Kryvlenia_PC_1.8	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/5
Kryvlenia_PC_1.9	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/6
Kryvlenia_PC_1.10	Fa0	DHCP LAN1	/26	10.25.58.1	-	Fa0/7
Kryvlenia_PC_2.1	Fa0	DHCP poolvlan37	/27	10.25.57.65	VLAN37	Fa0/5
Kryvlenia_PC_2.2	Fa0	DHCP poolvlan27	/27	10.25.57.33	VLAN27	Fa0/10
Kryvlenia_PC_2.3	Fa0	DHCP poolvlan17	/27	10.25.57.1	VLAN17	Fa0/15
Kryvlenia_PC_2.4	Fa0	DHCP poolvlan37	/27	10.25.57.65	VLAN37	Fa0/5
Kryvlenia_PC_2.5	Fa0	DHCP poolvlan27	/27	10.25.57.33	VLAN27	Fa0/10
Kryvlenia_PC_2.6	Fa0	DHCP poolvlan17	/27	10.25.57.1	VLAN17	Fa0/15
Kryvlenia_PC_2.7	Fa0	DHCP poolvlan37	/27	10.25.57.65	VLAN37	Fa0/5
Kryvlenia_PC_2.8	Fa0	DHCP poolvlan27	/27	10.25.57.33	VLAN27	Fa0/10
Kryvlenia_PC_2.9	Fa0	DHCP poolvlan17	/27	10.25.57.1	VLAN17	Fa0/15

Продовження таблиці 3.5

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Kryvlenia_PC_2.10	Fa0	DHCP poolvlan37	/27	10.25.57.65	VLAN37	Fa0/5
Kryvlenia_PC_2.11	Fa0	DHCP poolvlan27	/27	10.25.57.33	VLAN27	Fa0/10
Kryvlenia_PC_2.12	Fa0	DHCP poolvlan17	/27	10.25.57.1	VLAN17	Fa0/15
Kryvlenia_PC_3.1	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/5
Kryvlenia_PC_3.2	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/6
Kryvlenia_PC_3.3	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/3
Kryvlenia_PC_3.4	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/4
Kryvlenia_PC_3.5	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/3
Kryvlenia_PC_3.6	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/4
Kryvlenia_PC_3.7	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/3
Kryvlenia_PC_3.8	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/4
Kryvlenia_PC_3.9	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/3
Kryvlenia_PC_3.10	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/4
Kryvlenia_PC_3.11	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/3
Kryvlenia_PC_3.12	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/4
Kryvlenia_PC_3.13	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/3
Kryvlenia_PC_3.14	Fa0	DHCP LAN3	/24	10.25.56.1	-	Fa0/4
Kryvlenia_PC_4.1	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/2
Kryvlenia_PC_4.2	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/3
Kryvlenia_PC_4.3	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/4
Kryvlenia_PC_4.4	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/5
Kryvlenia_PC_4.5	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/3

Продовження таблиці 3.5

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Kryvlenia_PC_4.6	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/4
Kryvlenia_PC_4.7	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/5
Kryvlenia_PC_4.8	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/2
Kryvlenia_PC_4.9	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/3
Kryvlenia_PC_4.10	Fa0	DHCP LAN4	/25	10.25.57.129	-	Fa0/4
Kryvlenia_PC_5.1	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/3
Kryvlenia_PC_5.2	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/4
Kryvlenia_PC_5.3	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/5
Kryvlenia_PC_5.4	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/6
Kryvlenia_PC_5.5	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/7
Kryvlenia_PC_5.6	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/8
Kryvlenia_PC_5.7	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/9
Kryvlenia_PC_5.8	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/10
Kryvlenia_PC_5.9	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/11
Kryvlenia_PC_5.10	Fa0	DHCP LAN5	/27	10.25.58.65	-	Fa0/12

3.2 Налаштування моделі комп'ютерної мережі лікарні

Враховуючи усі пристрої та адресацію з таблиць 3.4 – 3.5, налаштуємо модель комп'ютерної мережі (рисунок 3.1 – 3.6, сторінка 56 – 59).

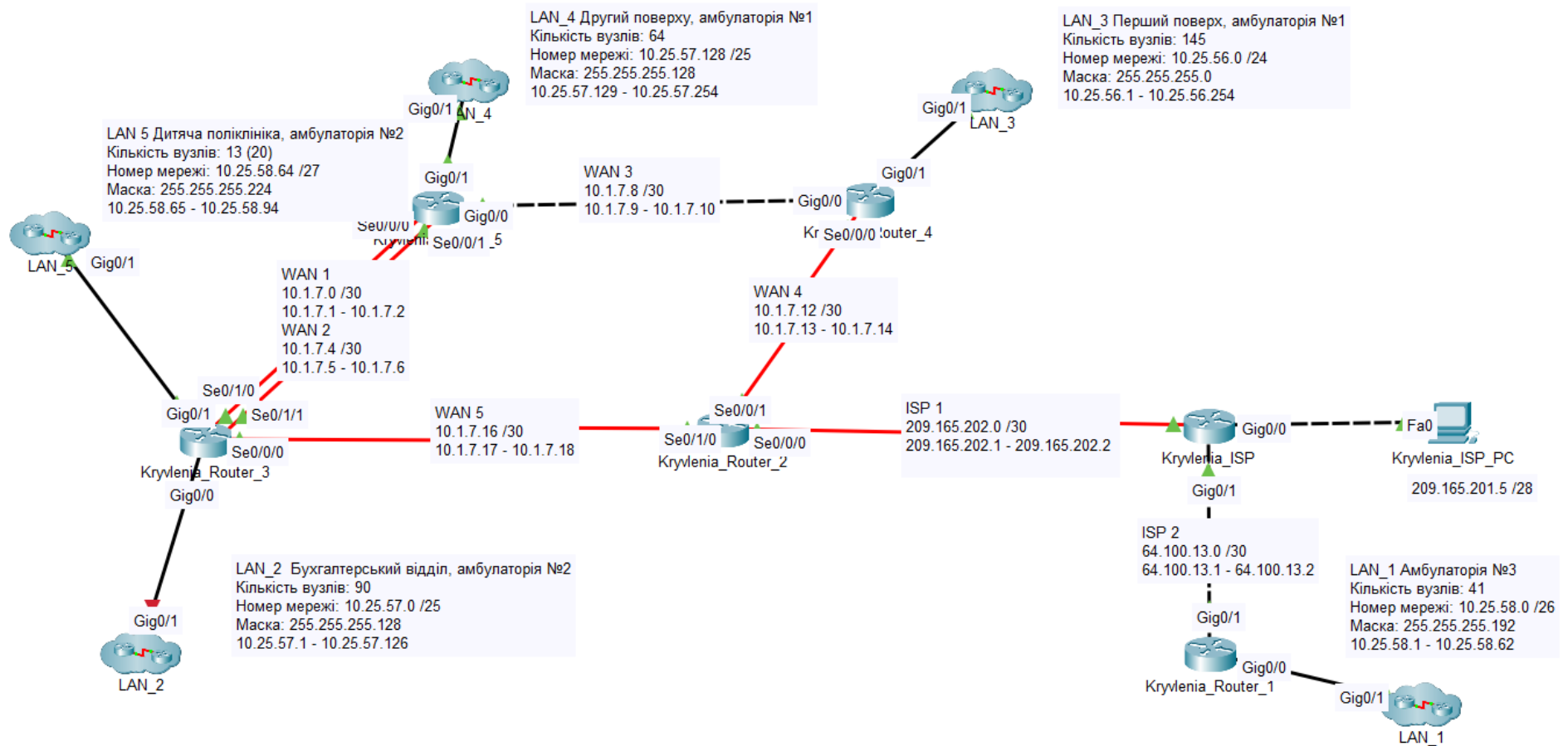


Рисунок 3.1 – Модель комп'ютерної мережі лікарні

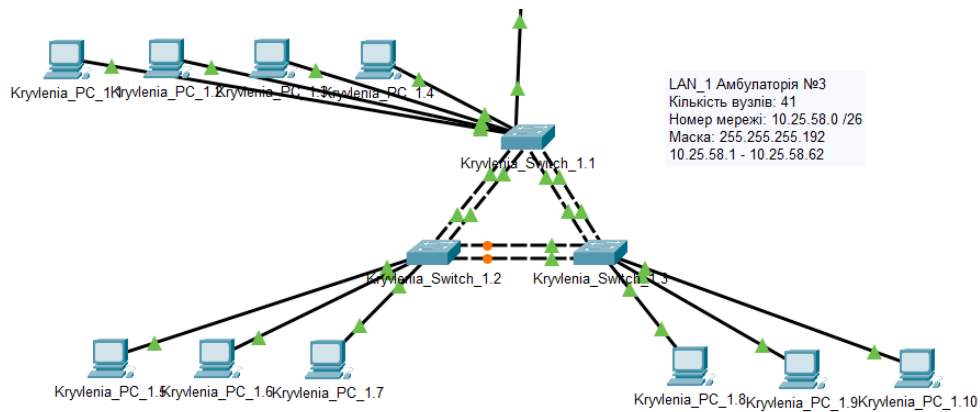


Рисунок 3.2 – Модель комп'ютерної мережі амбулаторії №3

На мережі бухгалтерського відділу має бути поділена на VLAN-и, тому адресація до неї буде налаштована пізніше.

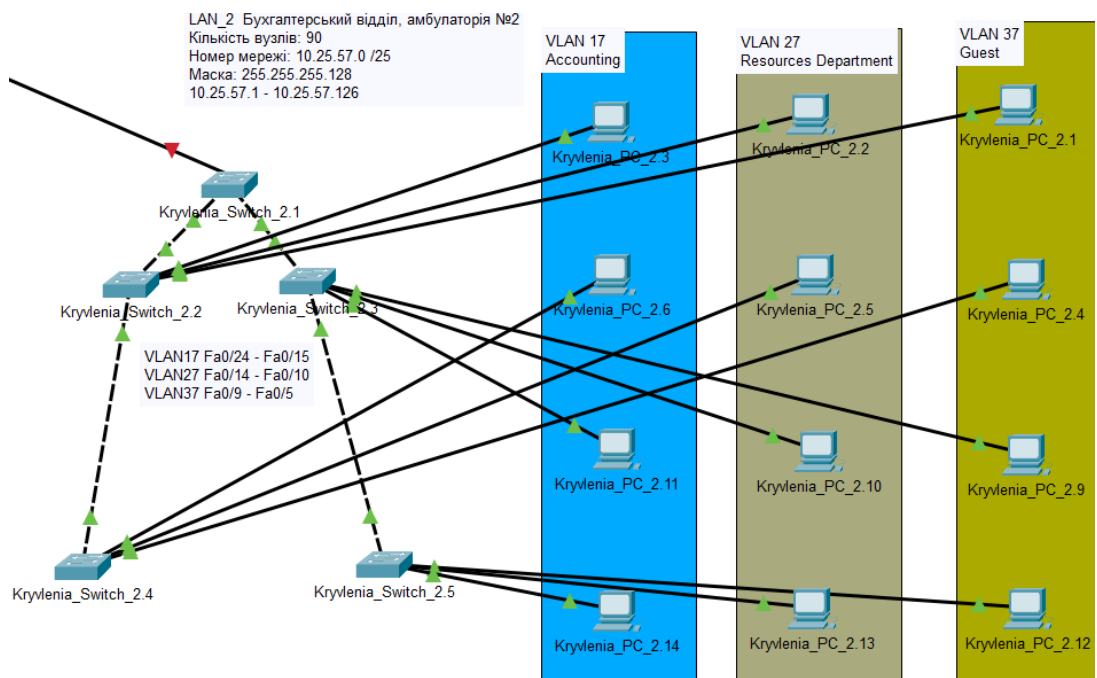


Рисунок 3.3 – Модель комп'ютерної мережі бухгалтерського відділу

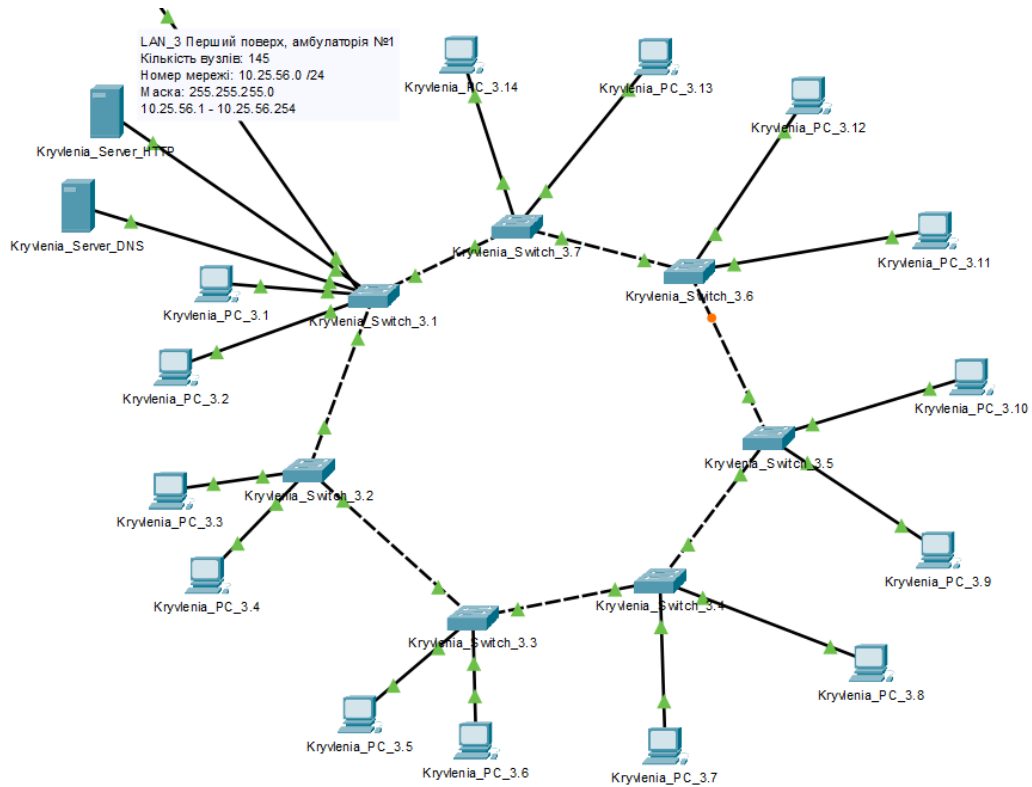


Рисунок 3.4 – Модель комп'ютерної мережі першого поверху амбулаторії №1

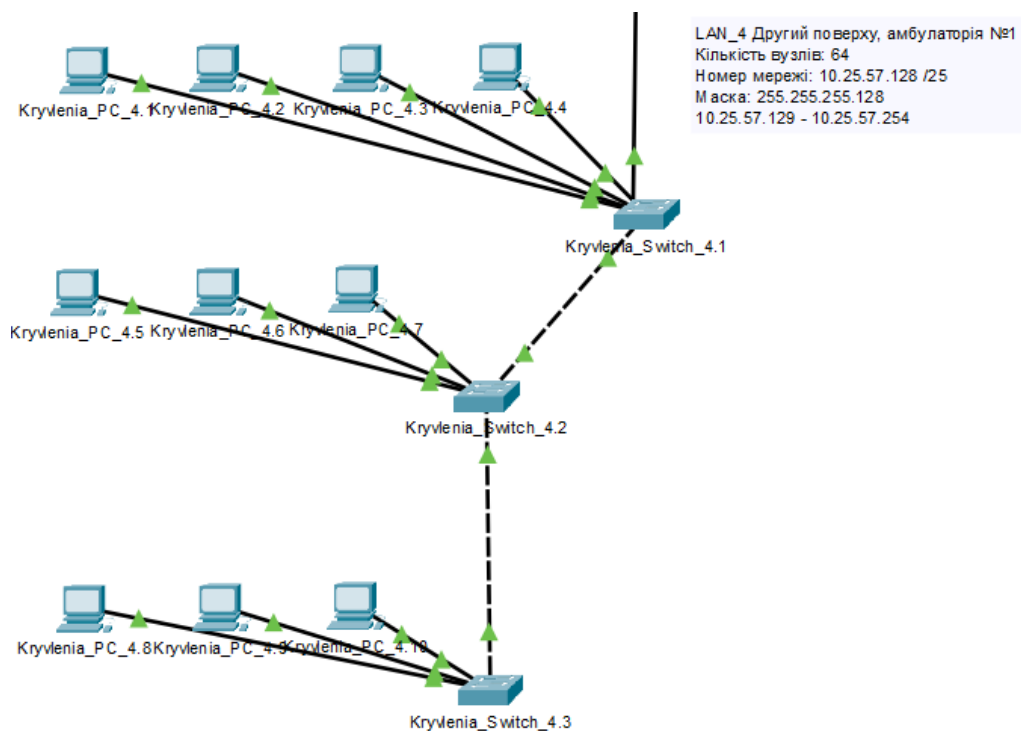


Рисунок 3.5 – Модель комп'ютерної мережі другого поверху амбулаторії №1

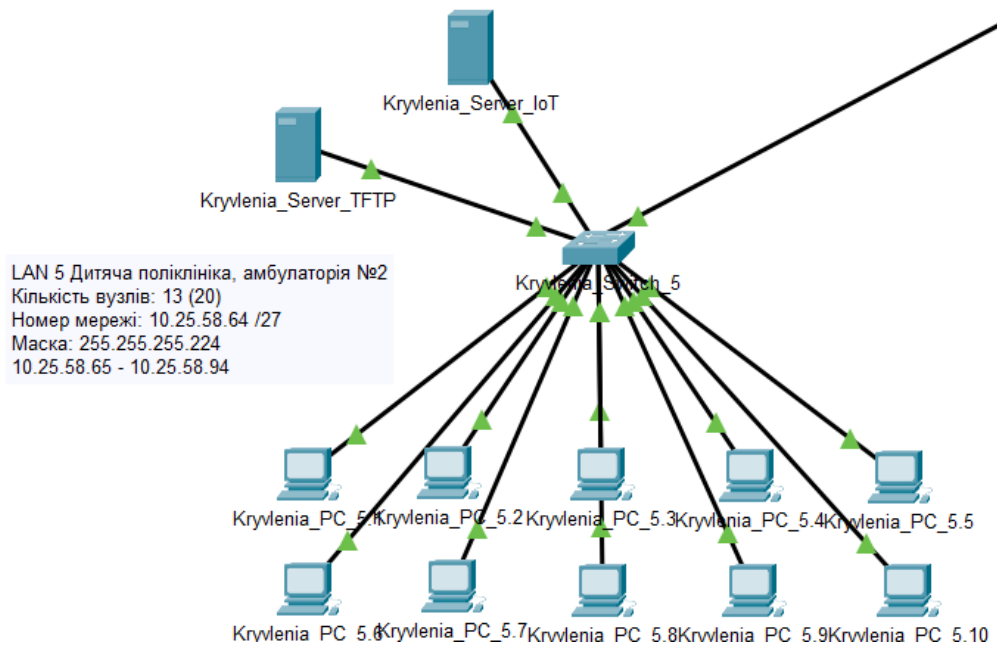


Рисунок 3.6 – Модель комп’ютерної мережі дитячої поліклініки амбулаторії №2

3.3 Налаштування пристроїв у мережі

3.3.1 Базове налаштування конфігурації пристроїв у мережі

Базове налаштування включає в себе: призначення IP-адрес на інтерфейсах маршрутизаторів, призначення назви пристрою, призначення паролів до консолі, vty та привілейованого режиму, шифрування паролів, розробка банеру MOTD, призначення на лініях vty протоколу ssh, призначення користувачів, в якості імені домена використати ім’я пристрою, для шифрування даних створити ключ RSA завдовжки 1024 біт, на DCE-інтерфейсах призначити встановлення значення тактової частоти – 128000.

Розберемо призначення IP-адрес на прикладі Kryvlenia_Router_2:

enable – Переходимо у привілейований режим конфігурації

configure terminal – Переходимо у глобальний режим конфігурації, що дозволяє вносити зміни у конфігурацію маршрутизатора

interface Se0/0/0 – Обираємо інтерфейс Serial0/0/0 для конфігурації

ip address 209.165.202.2 255.255.255.252 – Привласнюємо IP-адресу 209.165.202.2 з маскою підмережі 255.255.255.252 на інтерфейсі Se0/0/0

no shutdown – Вмикаємо інтерфейс

clock rate 128000 – Призначення встановлення значення тактової частоти 128000 на DCE-інтерфейсі

```
interface Se0/0/1
```

```
ip address 10.1.7.14 255.255.255.252
```

```
no shutdown
```

```
interface Se0/1/0
```

```
ip address 10.1.7.17 255.255.255.252
```

```
no shutdown
```

```
clock rate 128000
```

Перевіряємо призначення IP-адрес, використавши команду “*show ip route*” (рисунок 3.7)

```
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.7.12/30 is directly connected, Serial0/0/1
L       10.1.7.14/32 is directly connected, Serial0/0/1
C       10.1.7.16/30 is directly connected, Serial0/1/0
L       10.1.7.17/32 is directly connected, Serial0/1/0
    209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/30 is directly connected, Serial0/0/0
L       209.165.202.2/32 is directly connected, Serial0/0/0
```

Рисунок 3.7 – Результат команди “*show ip route*” на *Kryvlenia_Router_2*

Для ідентифікації кожного пристрою в мережі, призначимо їм назви. Усі наступні налаштування будуть показані на прикладі налаштування *Kryvlenia_Router_3*:

```
hostname Kryvlenia_Router_3
```

Далі розробимо банер MOTD, який буде виводити назву маршрутизатора:

```
banner motd "This is Kryvlenia_Router_3"
```

Для забезпечення базового рівня безпеки, встановимо паролі до консолі, vty-з’єднань та привілейованого режиму:

line console 0 – Обираємо консолі 0 для конфігурації
password cisco – Встановлюємо пароль "cisco" для консолі
login – Створюємо вимогу пароля для входу через консоль
line vty 0 15 – Обираємо діапазон vty з 0 по 15 для конфігурації
password cisco – Встановлюємо пароль "cisco" для vty
login – Створюємо вимогу пароля для входу через vty
enable secret class – Встановлення зашифрованого пароля "class" для доступу до привілейованого режиму

Перевірка налаштувань назви, MOTD та паролів приведені на рисунку 3.8.

```
This is Kryvlenia_Router_3

User Access Verification

Password:

Kryvlenia_Router_3>enable
Password:
Kryvlenia_Router_3#
```

Рисунок 3.8 – Аутентифікація до маршрутизатора Kryvlenia_Router_3

Зашифруємо паролі. Шифрування захищає паролі від перегляду їх у конфігурації пристрою в разі несанкціонованого доступу.

service password-encryption

Перевіряємо шифрування паролів у файлі конфігурації (рисунок 3.9)

```
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
password 7 0822455D0A16
login
```

Рисунок 3.9 – Перевірка шифрування паролів у файлі конфігурації

Як бачимо, замість паролів у файлі конфігурації випадкові символи.

Далі додаємо доменне ім'я та створимо ключ RSA:

ip domain-name Kryvlenia_Router_3 – Встановлення доменного імені для маршрутизатора

crypto key generate rsa – Генерація RSA ключа для шифрування

1024 – Визначення розміру ключа RSA (1024 біти)

На усіх лініях vty налаштуємо використання протоколу ssh:

line vty 0 15

transport input ssh

login local

Створимо користувача:

username 123202_Kryvlenia password admincisco

Ці налаштування вводяться на всіх маршрутизаторах та комутаторах у мережі.

До базового налаштування також входить об'єднання фізичних ліній у мережі амбулаторії №3, з метою збільшення пропускної здатності і надійності каналів:

interface range fa0/1-2 – Обираємо діапазон інтерфейсів FastEthernet 0/1 та FastEthernet 0/2

channel-group 1 mode active – Об'єднуємо їх у канал агрегації (EtherChannel)

interface port-channel 1 – Обираємо канал агрегації

switchport mode trunk – Конфігурація агрегатного каналу у режим транку

switchport trunk allowed vlan all – Дозволяємо проходження всіх VLAN

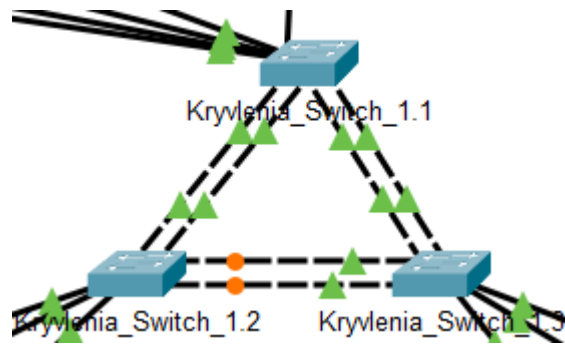


Рисунок 3.10 – Виконане об'єднання фізичних ліній у мережі амбулаторії №3

Як було вказано у таблиці 3.5, усі комп'ютери будуть отримувати IP-адресу за протоколом DHCP.

Налаштування DHCP на прикладі мережі першого поверху амбулаторії №1 приведено нижче.

Налаштування на маршрутизаторі Kryvlenia_Router_4:

ip dhcp pool LAN3 – Створюємо DHCP пул з іменем “LAN3”

network 10.25.56.0 255.255.255.0 – Вказуємо діапазон адрес

default-router 10.25.56.1 – Адреса маршрутизатора за замовчуванням

dns-server 10.25.56.18 – Вказуємо адресу DNS-сервера

ip dhcp excluded-address 10.25.56.1 10.25.56.10 – Виключаємо з пулу перші 10 адреси, які будуть призначені на маршрутизаторі та комутаторах

ip dhcp excluded-address 10.25.56.17 10.25.56.18 – Виключаємо з пулу адреси серверів

Налаштування на комутаторах у мережі першого поверху амбулаторії №1:

interface vlan 1 – Обираємо інтерфейс VLAN 1

ip address 10.25.56.2 255.255.255.0 – Привласнюємо адресу до комутатору
no shutdown

ip default-gateway 10.25.56.1 – Встановлюємо шлюз за замовчуванням

Перевірка роботи DHCP приведена у рисунку 3.11, сторінка 64

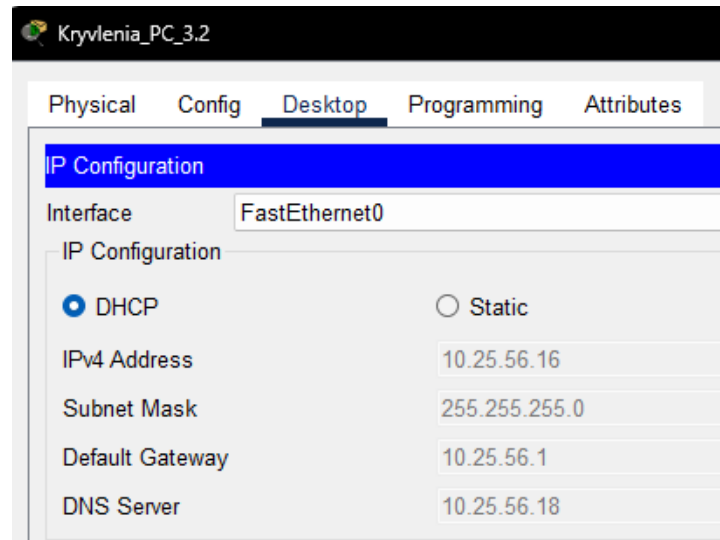


Рисунок 3.11 – Робота протоколу DHCP на PC у мережі LAN_3

3.3.2 Налаштування маршрутизаторів у мережі

На маршрутизаторах необхідно налаштувати протокол динамічної маршрутизації. Для цього був обраний протокол OSPF (Open Shortest Path First), який має високу швидкість конвергенції, масштабованість та може використовуватися на багатьох пристроях.

Налаштування OSPF на прикладі Kryvlenia_Router_5:

router ospf 7 – Вмикаємо ospf з процесом номер 7 (варіант)

network 10.1.7.0 0.0.0.3 area 0 – Оголошуємо мережу 10.1.7.0

network 10.1.7.4 0.0.0.3 area 0

network 10.1.7.8 0.0.0.3 area 0

network 10.25.57.128 0.0.0.127 area 0

passive-interface Gig0/1 – Вимикаємо надсилання OSPF оновлень на мережу LAN

auto-cost reference-bandwidth 1000 – Змінюємо еталонну пропускну здатність на 1000 Мбіт/с на Gigabit-інтерфейсах

Задаємо пропускну спроможність на serial-інтерфейсах = 128 Кб/с та вартість метрики = 7500:

interface Se0/0/0

bandwidth 128 – Встановлення пропускну здатність інтерфейсу на 128 Кб/с

delay 7500 – Встановлення затримки на інтерфейсі на 7500 мікросекунд
 Налаштування статичних маршрутів приведено на прикладі
 Kryvlenia_Router_2

ip route 0.0.0.0 0.0.0.0 209.165.202.1 – Налаштування статичного маршруту за замовчуванням. Використовується для направлення всього невідомого трафіку в Інтернет через шлюз провайдера (ISP)

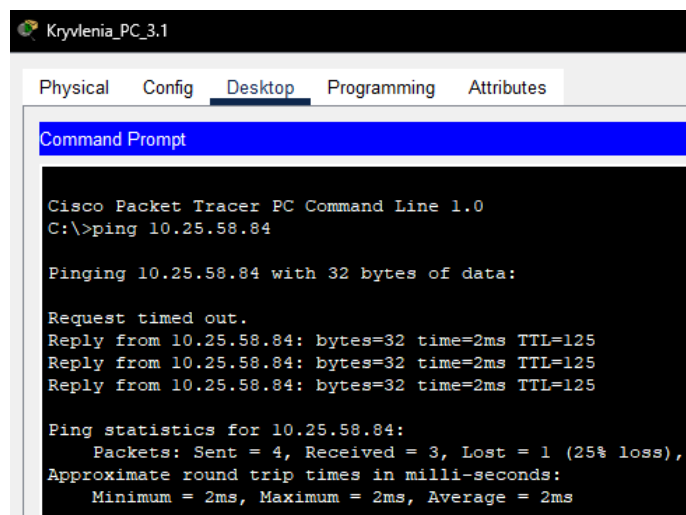
ip route 209.165.201.0 255.255.255.240 209.165.202.1 – Налаштування статичного маршруту до мережі 209.165.201.0, трафік до цієї мережі буде спрямований через IP-адресу 209.165.202.1

ip route 10.25.58.0 255.255.255.192 209.165.202.1

router ospf 7

redistribute static subnets – включення статичних маршрутів до таблиці маршрутизації OSPF

Після цього вузли у основній мережі, окрім мережі, де налаштовується VLAN, повинні мати можливість обмінюватись трафіком між собою. Перевірка представлена на рисунку 3.12 – 3.13



```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.25.58.84

Pinging 10.25.58.84 with 32 bytes of data:

Request timed out.
Reply from 10.25.58.84: bytes=32 time=2ms TTL=125
Reply from 10.25.58.84: bytes=32 time=2ms TTL=125
Reply from 10.25.58.84: bytes=32 time=2ms TTL=125

Ping statistics for 10.25.58.84:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
  
```

Рисунок 3.12 – Пінг з мережі першого поверху до мережі дитячої поліклініки.

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.25.56.22

Pinging 10.25.56.22 with 32 bytes of data:

Reply from 10.25.56.22: bytes=32 time<lms TTL=126
Reply from 10.25.56.22: bytes=32 time<lms TTL=126
Reply from 10.25.56.22: bytes=32 time<lms TTL=126
Reply from 10.25.56.22: bytes=32 time<lms TTL=126

Ping statistics for 10.25.56.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Рисунок 3.13 – Пінг з мережі другого поверху до мережі першого поверху

Далі всі маршрутизатори будуть налаштовані на підтримку служби AAA (Authentication, Authorization, and Accounting), яка дозволяє забезпечити кращий контроль над тим, хто може підключатися до маршрутизатора, що вони можуть робити після підключення, і веде облік всіх дій користувачів.

aaa new-model – Активація нової моделі AAA на маршрутизаторі

В якості RADIUS сервера був обраний сервер TFTP, який знаходиться у мережі дитячої поліклініки.

radius-server host 10.25.58.81 auth-port 1645 key radius123 – Налаштування сервер RADIUS для автентифікації користувачів

aaa authentication login console group radius local – Налаштування AAA для автентифікації користувачів, які підключаються до консолі маршрутизатора. Спочатку намагається автентифікувати користувача через групу серверів RADIUS. Якщо сервер RADIUS недоступний, використовується локальна база даних користувачів

line console 0 – Перехід у режим конфігурації лінії для консолі

login authentication console

aaa authentication login default local – Налаштування AAA для автентифікації користувачів за замовчуванням

username Kryvlenia_Router_2 password admin123 – Додавання користувача з ім'ям *Kryvlenia_Router_2* і паролем *admin123* до локальної бази даних користувачів маршрутизатора

line vty 0 15

login authentication default – Застосування методу автентифікації за замовчуванням, налаштований раніше, до всіх ліній *vtty*.

Додаємо усі маршрутизатори до сервісу AAA на сервері TFTP (рисунок 3.14) та перевіряємо AAA на маршрутизаторах (рисунок 3.15).

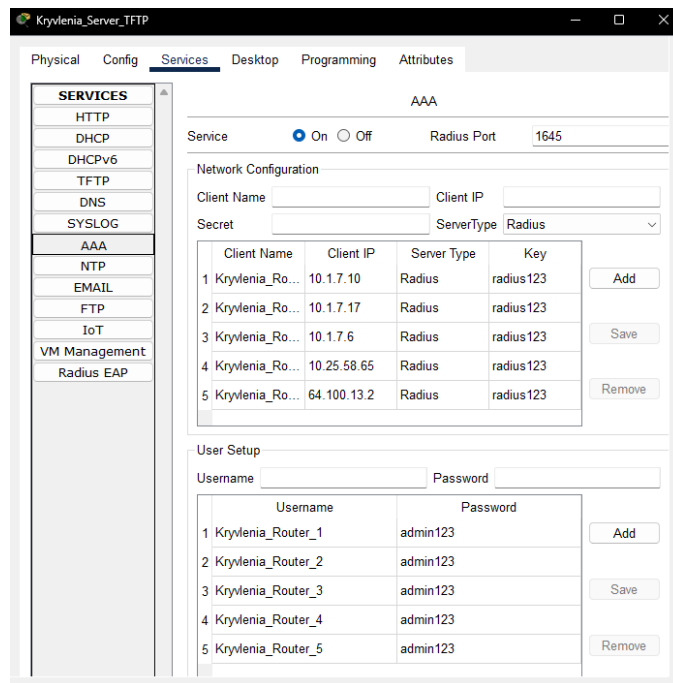


Рисунок 3.14 – Налаштований сервіс AAA на Kryvlenia_Server_TFTP

```
This is Kryvlenia_Router_2

User Access Verification

Username: Kryvlenia_Router_2
Password:
Kryvlenia Router 2>
```

Рисунок 3.15 – Перевірка працездатності AAA на маршрутизаторі
Kryvlenia_Router_2

```

This is Kryvlenia_Router_4

User Access Verification

Username: Kryvlenia_Router_2
Password:
Kryvlenia_Router_4>

```

Рисунок 3.16 – Перевірка працездатності RADIUS на маршрутизаторі
Kryvlenia_Router_4

3.3.3 Налаштування роботи Інтернет

Для налаштування роботи Інтернет необхідно зробити декілька налаштувань на пограничних маршрутизаторах Kryvlenia_Router_1 та Kryvlenia_Router_2.

Почнемо з налаштування динамічного NAT. NAT буде перетворювати локальні адреси на глобальні. Налаштування NAT проходить за такими даними:

- ім'я пула: Internet;
- адреси: 209.165.200.5 – 209.165.200.30
- список доступу: NAT7.

Налаштування NAT на пограничному маршрутизаторі Kryvlenia_Router_2:
ip access-list extended NAT7 – Створення розширеного списку доступу для NAT з назвою NAT7

deny ip 10.25.56.0 0.0.0.255 10.25.58.0 0.0.0.63 – Блокування адрес, які потім будуть використовуватися у списку VPN

deny ip 10.25.57.0 0.0.0.127 10.25.58.0 0.0.0.63

deny ip 10.25.57.128 0.0.0.127 10.25.58.0 0.0.0.63

deny ip 10.25.58.64 0.0.0.31 10.25.58.0 0.0.0.63

deny ip 10.1.7.0 0.0.0.255 10.25.58.0 0.0.0.63

permit ip 10.25.56.0 0.0.0.3.255 any – Дозволяє адреси з мережі

permit ip 10.1.7.0 0.0.0.255 any

ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 –

Створення пулу “Internet” зовнішніх IP-адрес для NAT

ip nat inside source list NAT7 pool Internet – Використання пулу "Internet" для NAT відповідно до списку доступу NAT7

interface Se0/0/0

ip nat outside – Встановлення інтерфейсу Se0/0/0 як зовнішній для NAT

interface Se0/0/1

ip nat inside – Встановлення інтерфейсу Se0/0/1 як внутрішнього для NAT

interface Se0/1/0

ip nat inside

На пограничному маршрутизаторі віддаленої мережі також налаштуємо NAT, але пул "Internet" матиме адреси: 209.165.200.32 - 209.165.200.62.

Далі налаштуємо сервер HTTP, щоб на всіх вузлах, при вводі в рядку браузера `http://123.dnipro.ua` (`http://209.165.200.4`) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу.

Зробимо запис у службі DNS на сервері DNS (рисунок 3.17)

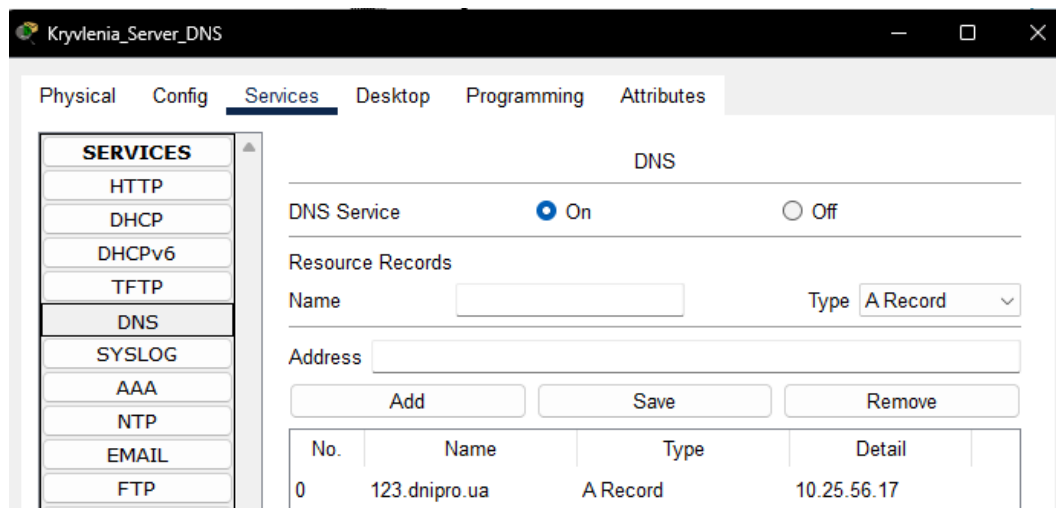


Рисунок 3.17 – Додавання IP-адреси HTTP серверу з доменним ім'ям
123.dnipro.ua

Далі на пограничних маршрутизаторах додамо статичні адреси NAT:

ip nat inside source static 10.25.56.17 209.165.200.4 – Створюємо статичне відображення внутрішньої IP-адреси HTTP-серверу на зовнішню IP-адресу 209.165.200.4

ip nat inside source static 10.25.56.18 209.165.200.3 – Створюємо статичне відображення внутрішньої IP-адреси DNS-серверу на зовнішню IP-адресу 209.165.200.4

У віддаленій мережі міняємо адресу у налаштуваннях DHCP на DNS-server:

ip dhcp pool LAN1

dns-server 209.165.200.3

Також додаємо нові статичні маршрути на Kryvlenia_Router_2 та Kryvelnia_Router_ISP:

Kryvlenia_Router_2:

ip route 209.165.200.32 255.255.255.224 209.165.202.1

Ця адреса дозволить відсилати відповідь з DNS та HTTP серверів до віддаленої мережі.

На Kryvlenia_Router_ISP залишаємо тільки 2 маршрути за замовчуванням:

ip route 209.165.200.0 255.255.255.224 209.165.202.2

ip route 209.165.200.32 255.255.255.224 64.100.13.2

Перевіряємо працездатність NAT та серверів:

```
Kryvlenia_Router_2#show ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
---  209.165.200.3      10.25.56.18        ---                 ---
---  209.165.200.4      10.25.56.17        ---                 ---
tcp  209.165.200.4:80   10.25.56.17:80     209.165.201.5:1025 209.165.201.5:1025
tcp  209.165.200.4:80   10.25.56.17:80     209.165.201.5:1026 209.165.201.5:1026
```

Рисунок 3.18 – Перевірка працездатності NAT через таблицю трансляцій NAT

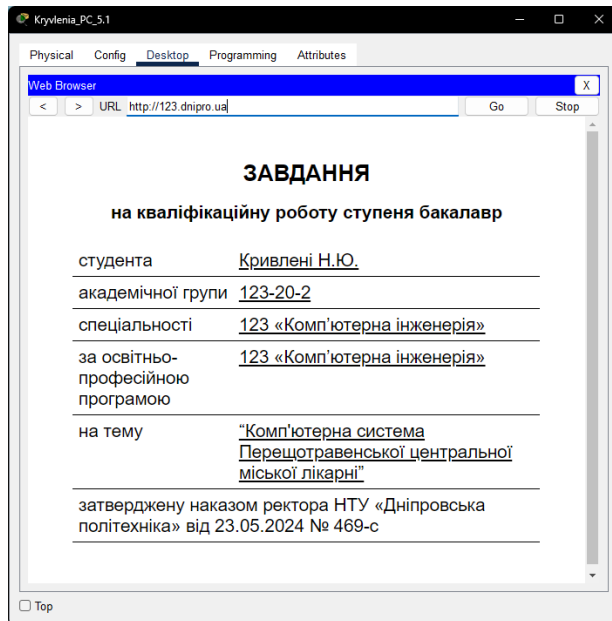


Рисунок 3.19 – Приєднання до сайту 123.dnipro.ua через комп'ютер в основній мережі

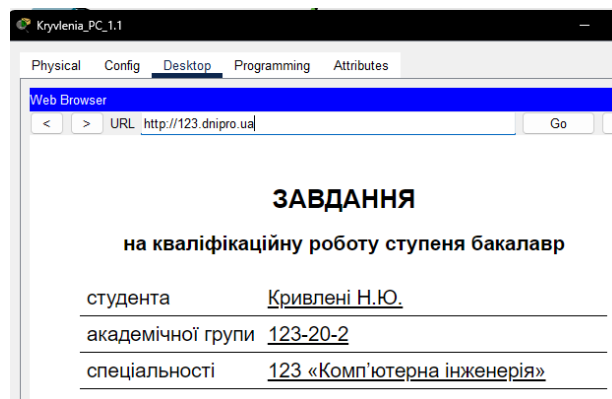


Рисунок 3.20 – Приєднання до сайту через комп'ютер у віддаленій мережі

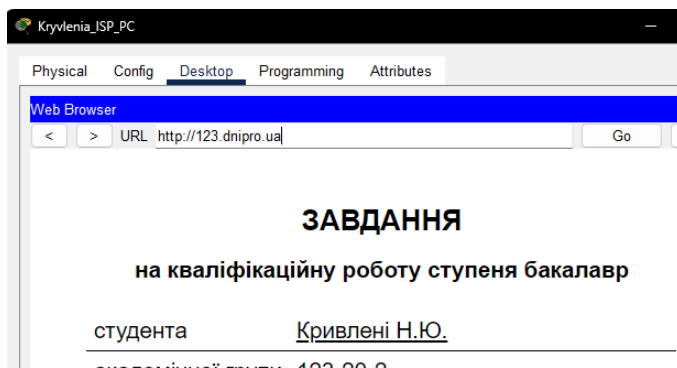


Рисунок 3.21 – Приєднання до сайту через комп'ютер в інтернеті

Зазначимо, що комп'ютер, який під'єднаний до ISP-маршрутизатору, не може з'єднуватися з вузлами у мережі лікарні, але усі вузли з мережі лікарні можуть посилати запити до комп'ютера в інтернеті.

Налаштуємо віртуальну приватну мережу site-to-site VPN з використанням IPsec для трафіку, що проходить між основною мережею та віддаленою мережею лікарні через Internet. Це потрібно для забезпечення додаткової безпеки у мережі та забезпечення віддаленої мережі безпечно під'єднуватися до основної мережі.

Спочатку створимо пул адрес VPN7, у який включимо усі виключені адреси з пулу NAT7:

```
ip access-list extended VPN7  
permit ip 10.25.56.00.0.0.255 10.25.58.0 0.0.0.63  
permit ip 10.25.57.00.0.0.127 10.25.58.0 0.0.0.63  
permit ip 10.25.57.128 0.0.0.127 10.25.58.00.0.0.63  
permit ip 10.25.58.64 0.0.0.31 10.25.58.0 0.0.0.63  
permit ip 10.1.7.00.0.0.255 10.25.58.00.0.0.63
```

Далі вмикаємо ліцензію для пакету безпеки:

```
license boot module c2900 technology-package securityk9
```

Після цього з'явиться ліцензійна угода (рисунок 3.22, сторінка 73).
Погоджуємося з ним.


```
Kryvlenia_Router_1(config)#license boot module c2900 technology-package securityk9
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.
```

Use of this product feature requires an additional license from Cisco, together with an additional payment. You may use this product feature on an evaluation basis, without payment to Cisco, for 60 days. Your use of the product, including during the 60 day evaluation period, is subject to the Cisco end user license agreement

http://www.cisco.com/en/US/docs/general/warranty/English/EULKEN_.html

If you use the product feature beyond the 60 day evaluation period, you must submit the appropriate payment to Cisco for the license. After the 60 day evaluation period, your use of the product feature will be governed solely by the Cisco end user license agreement (link above), together with any supplements relating to such product feature. The above applies even if the evaluation license is not automatically terminated and you do not receive any notice of the expiration of the evaluation period. It is your responsibility to determine when the evaluation period is complete and you are required to make payment to Cisco for your use of the product feature beyond the evaluation period.

Your acceptance of this agreement for the software features on one product shall be deemed your acceptance with respect to all such software on all Cisco products you purchase which includes the same software. (The foregoing notwithstanding, you must purchase a license for each software feature you use past the 60 days evaluation period, so that if you enable a software feature on 1000 devices, you must purchase 1000 licenses for use past the 60 day evaluation period.)

Activation of the software command line interface will be evidence of your acceptance of this agreement.

```
ACCEPT? [yes/no]: Yes
% use 'write' command to make license boot config take effect on next boot
%LICENSE-6-EULA_ACCEPTED: EULA for feature securityk9 1.0 has been accepted.
UDI=CISCO2911/K9:FTX1524DXE5-; StoreIndex=0:Evaluation License Storage
```

Рисунок 3.22 – Ліцензійна угода після вмикання пакету безпеки

Далі перезавантажуємо маршрутизатор, перед цим зберігши конфігурацію, та продовжуємо налаштування VPN:

crypto isakmp policy 10 – Створюємо політику ISAKMP з пріоритетом 10

encryption aes – Вказуємо використання AES для шифрування

authentication pre-share – Використовуємо попередньо поділений ключ для аутентифікації

group 2 – Встановлюємо групу DH (Diffie-Hellman) 2 для обміну ключами

crypto isakmp key kryvlenia address 64.100.13.2 – Встановлюємо попередньо поділений ключ "kryvlenia" для IP-адреси 64.100.13.2

crypto ipsec transform-set Set esp-aes esp-sha-hmac – Створюємо набір перетворень IPsec з назвою "Set", шифруванням AES та HMAC-SHA

crypto map MAP 10 ipsec-isakmp – Створює криптографічну карту з ім'ям "MAP" і пріоритетом 10

description VPN connection to Kryvlenia_Router_1 – Додаємо опис
set peer 64.100.13.2 – Встановлюємо IP-адресу віддаленого VPN-партнера,
 з яким буде встановлено IPsec з'єднання

set transform-set Set – Вказуємо, що для цього з'єднання буде
 використовуватися трансформаційний набір "Set"

match address VPN7 – Вказуємо, що для цього з'єднання буде
 використовуватися список доступу "VPN7"

interface Se0/0/0

crypto map MAP – Призначаємо криптографічну карту "MAP" інтерфейсу
 Serial0/0/0

Після налаштувань з'явиться системний лог (рисунок 3.23), яке вказує, що
 ISAKMP був увімкнений.

```
Kryvlenia_Router_2(config)#crypto map MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Kryvlenia_Router_2(config-crypto-map)#description VPN connection to
Kryvlenia_Router_1
Kryvlenia_Router_2(config-crypto-map)#set peer 64.100.13.2
Kryvlenia_Router_2(config-crypto-map)#set transform-set Set
Kryvlenia_Router_2(config-crypto-map)#match address VPN7
Kryvlenia_Router_2(config-crypto-map)#interface Se0/0/0
Kryvlenia_Router_2(config-if)#crypto map MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Kryvlenia_Router_2(config-if)#
```

Рисунок 3.23 – Системний лог після налаштування VPN на Kryvlenia_Router_2

3.3.4 Захист інформації в комп'ютерній мережі від несанкціонованого доступу

Для захисту інформації, у LAN_2, яка являється мережею бухгалтерського відділу будуть налаштовані мережі VLAN. Мережа буде поділена на чотири менші мережі, назви яких приведені у таблиці 3.6, сторінка 75.

Таблиця 3.6 – Список мереж VLAN

Номер VLAN	Ім'я VLAN	Примітка
17	Accounting	Для бухгалтерії
27	Resources Department	Для відділу кадрів
37	Guest	Для гостей
99	Management	Для комутаторів
100	Native	Власна мережа

На маршрутизаторі *Kryvlenia_Router_3* налаштуємо підінтерфейси на кожну з VLAN:

int Gig0/0.17 – Обираємо підінтерфейс GigabitEthernet0/0.17

encapsulation dot1Q 17 – Вмикаємо на ньому інкапсуляцію

ip address 10.25.57.1 255.255.255.224 – Привласнюємо адресу

Таке налаштування робимо з підінтерфейсами *Gig0/0.27*, *Gig0/0.37* та *Gig0/0.99*.

Далі робимо налаштування DHCP для кожного з VLAN, окрім VLAN 99, виключаючи перші 10 адрес:

ip dhcp pool poolvlan17

network 10.25.57.0 255.255.255.224

default-router 10.25.57.1

dns-server 10.25.56.18

ip dhcp excluded-address 10.25.57.1 10.25.57.10

Після всіх налаштувань на маршрутизаторі вмикаємо сам інтерфейс:

int Gig0/0

no shutdown

Далі переходимо до налаштувань комутаторів у мережі бухгалтерського відділу.

Налаштування для *Kryvlenia_Switch_2.1*:

int vlan 99 – Обираємо інтерфейс VLAN 99

ip address 10.25.57.98 255.255.255.224 – Привласнюємо IP-адресу комутатору

ip default-gateway 10.25.57.97 – Привласнюємо шлюз за замовчуванням
vlan 17

name Accounting – Даємо назву VLAN 17

vlan 27

name Resources_Department

vlan 37

name Guest

vlan 99

name Management

vlan 100

name Native

int g0/1

switchport mode trunk – Конфігуруємо інтерфейс у режим транку

switchport trunk native vlan 100

switchport trunk allowed vlan 17,27,37,99,100 – Дозволяємо проходження

VLAN-ів

int range Fa0/1-3

switchport mode trunk

switchport trunk native vlan 100

switchport trunk allowed vlan 17,27,37,99,100

int range f0/4-24

shutdown – Вимикаємо діапазон інтерфейсів від Fa0/3 до Fa0/24, так як вони не використовуються

Частина налаштування для *Kryvlenia_Switch_2.2*:

int range f0/5-9

switchport mode access – Включення режиму доступу

switchport access vlan 37 – Привласнюємо портам

```
int range f0/10-14
switchport mode access
switchport access vlan 27

int range f0/15-24
switchport mode access
switchport access vlan 17

int range f0/1-4
switchport mode trunk
switchport trunk native vlan 100
```

Перевірка працездатності VLAN та DHCP:

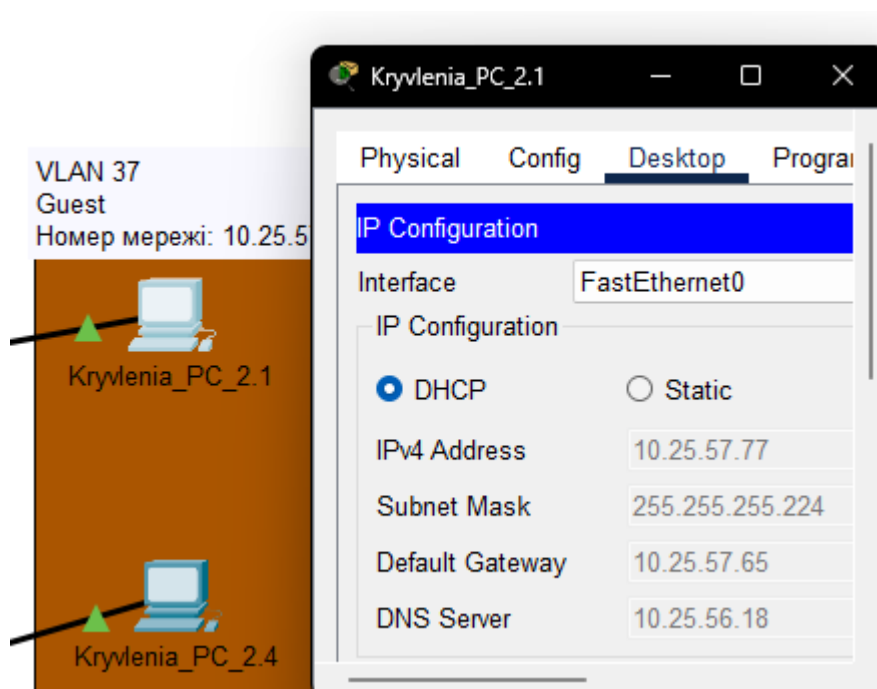


Рисунок 3.24 – IP-адреса на комп'ютері у VLAN 37

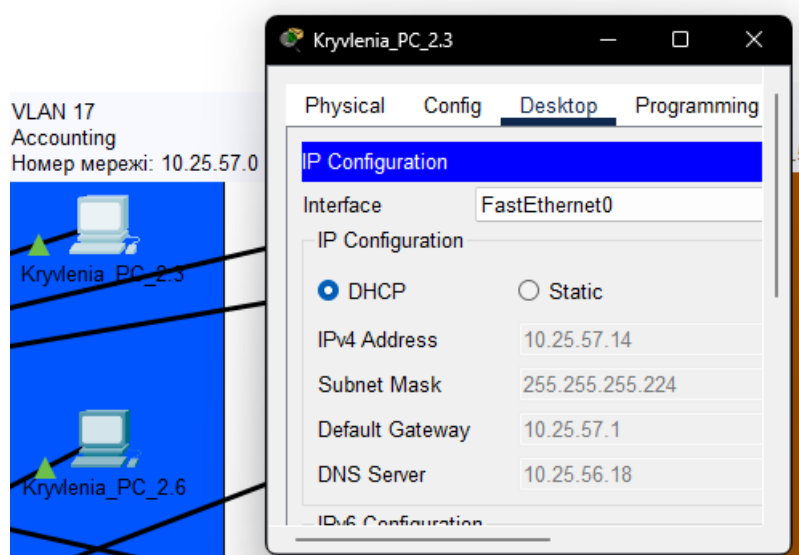


Рисунок 3.25 – IP-адреса на комп'ютері у VLAN 17

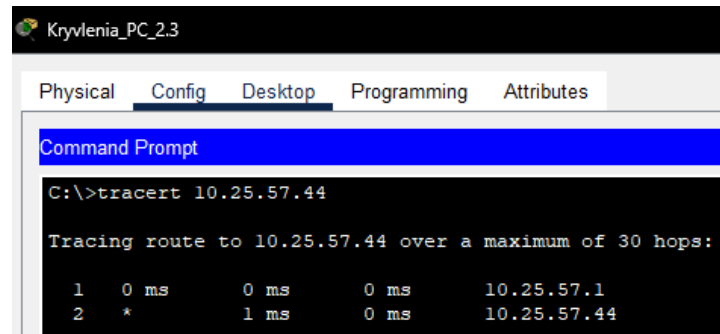


Рисунок 3.26 – Перегляд переміщення пакету за комп'ютера у VLAN 17 до комп'ютера у VLAN 27

Як бачимо з рисунку 3.26, пакет передався до маршрутизатора, а потім до комп'ютера у VLAN 27. Це означає, що VLAN працює.

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Вибір компонента системи

За вимогами, до мережі бухгалтерського відділу, дитячої поліклініки, першого та другого поверхів амбулаторії №1 впроваджені IoT-речі. IoT-речі (Internet of Things) – це фізичні пристрої, підключені до Інтернету, які можуть збирати, обмінюватися та обробляти дані. Ці пристрої оснащені датчиками, програмним забезпеченням, мережею та іншими технологіями, які дозволяють їм взаємодіяти один з одним та з іншими системами через Інтернет. Основна мета IoT – автоматизація та підвищення ефективності різних процесів за рахунок використання технологій, які дозволяють пристроям спілкуватися та приймати рішення без втручання людини.

4.2 Функціонал IoT у мережі лікарні

У мережі дитячої поліклініки був встановлений IoT-сервер, який збирає інформацію з IoT-речей і видає їм команди згідно з сценаріями, встановленими у web-застосунку сервера. Дані з IoT-речей передаються на IoT-сервер для подальшого аналізу та обробки. Для роботи IoT-речей використовуються як хмарні обчислення, організовані на сервері, так і туманні обчислення, що програмуються на мікроконтролерах.

У web-додатку на сервері будуть реалізовані сценарії протипожежної безпеки та система відеоспостереження.

Сценарії налаштовані за такими правилами:

Сценарій системи пожежної безпеки:

- якщо рівень чадного газу перевищує або дорівнює показник у 0.052, тоді вмикається сирена;
- якщо це правило спрацьовує в бухгалтерському відділі, тоді замок на дверях розблоковується.

Сценарій системи відеоспостереження:

- камери вмикаються та починають запис, якщо буде зафіксований рух;
- в бухгалтерському відділі, камери починають вести запис, якщо рух був помічений, коли двері були заблоковані замком.

Камери вимикаються власноруч, крім бухгалтерського відділу, де камери вимикаються самостійно після того, як двері будуть відчинені.

Алгоритми роботи IoT-речей приведені у рисунках 4.1 – 4.4

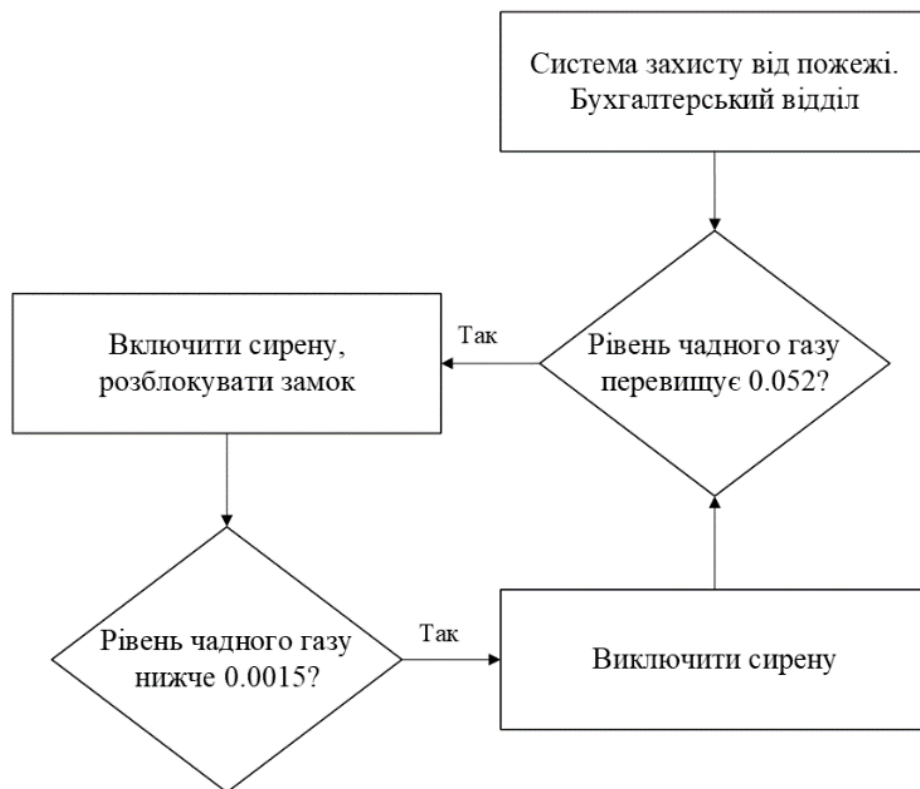


Рисунок 4.1 – Алгоритм роботи системи пожежної безпеки в бухгалтерському відділі

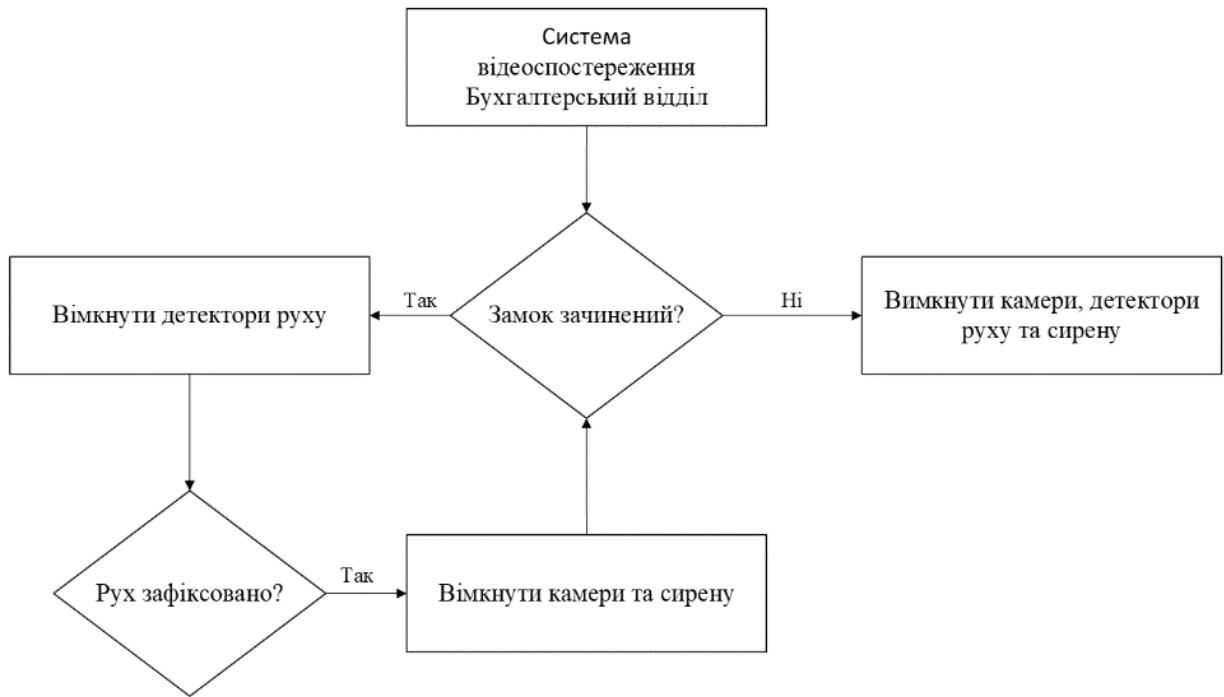


Рисунок 4.2 – Алгоритм роботи системи відеоспостереження в бухгалтерському відділі

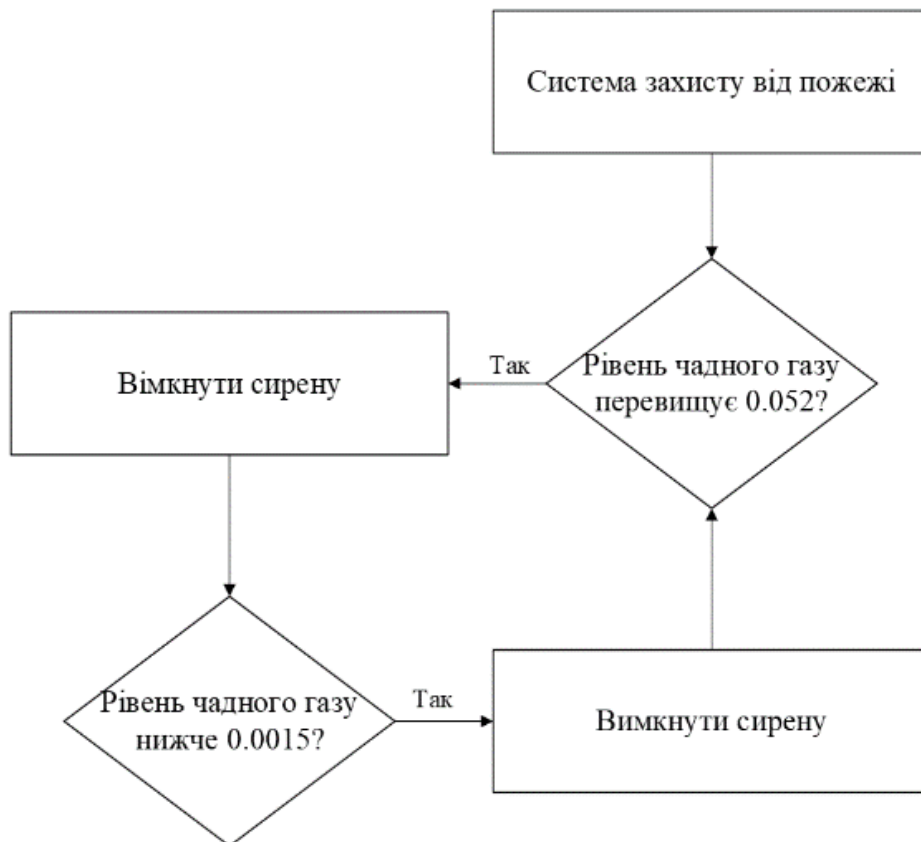


Рисунок 4.3 – Алгоритм роботи системи пожежної безпеки



Рисунок 4.4 – Алгоритм роботи системи відеоспостереження

Також будуть у системі будуть використовуватися мікроконтролери (MCU). Для програмування IoT-компонентів була взята плата Arduino UNO з Wi-Fi модулем на ESP8266. За вимогами, мовою програмування буде Python. На мікроконтролерах будуть запрограмовані сценарії: додаткової безпеки від несанкціонованого доступу через вікна за допомогою віконних сенсорів, система автоматичних жалюзі для амбулаторії №3, та автоматичних дверей для амбулаторії №1.

Контролери запрограмовані таким чином:

Контролери Kryvlenia_MCU_WB_2.1/2.2:

- контролери відповідають за відкриття/закриття жалюзі (window blinds/WB);

- жалюзі зачиняються, коли сонячне світло потрапляє на сенсор природного освітлення, в іншому випадку жалюзі відчиняються;
- статус жалюзі відправляється на IoT-сервер.

Контролери Kryvlenia_MCU_Security_2.1/2.2:

- контролери відповідають за додатковий захист у разі відкриття вікон, коли замок на дверях заблокований;
- якщо віконні сенсори роз'єднуються в разі відкриття вікна та замок на дверях заблокований, тоді активується сирена;
- статус сенсорів відправляється на IoT-сервер (рисунок).

Контролер Kryvlenia_MCU_Auto_Door_3.1:

- контролер відповідає за автоматичні двері в амбулаторії №1;
- двері відчиняються, коли помічається рух;
- двері відчиняються, якщо працює сирена при пожежній тривозі.

Тексти програми мікроконтролерів приведені в Додатку Г.

Алгоритми роботи IoT-компонентів представлені у рисунках 4.5 – 4.7.

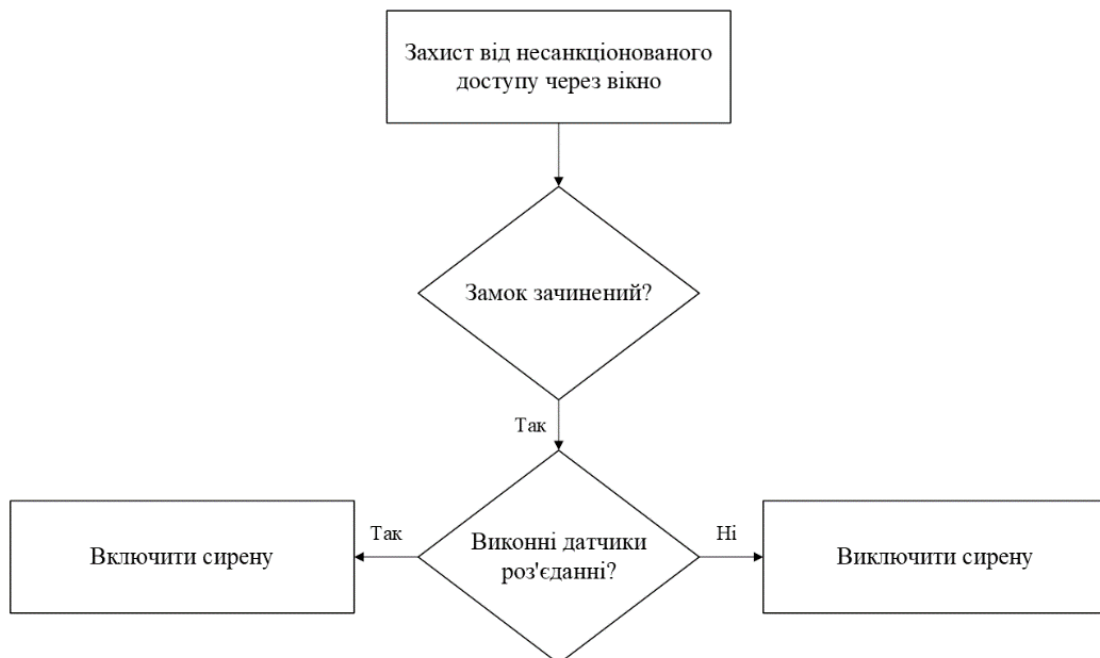


Рисунок 4.5 – Алгоритм роботи захисту від несанкціонованого доступу через вікно



Рисунок 4.6 – Алгоритм роботи автоматичних жалюзі



Рисунок 4.7 – Алгоритм роботи автоматичних дверей

4.3 Реалізація компоненту системи

Для реалізації IoT у мережі, скористаємося можливостями Cisco Packet Tracer. Спершу потрібно розробити схему адресації для IoT-пристроїв та IoT-шлюзів, які будуть використовуватися в мережі. Схема адресації приведена у таблицях 4.1 та 4.2

Таблиця 4.1 – Схема адресації мережі для IoT

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
IoT_LAN_2	13	10.7.2.0	/28	10.7.2.1	10.7.2.14
IoT_LAN_3,4	19	10.7.3.0	/27	10.7.3.1	10.7.3.30
IoT_LAN_5	10	10.7.5.0	/28	10.7.5.1	10.7.5.14

Таблиця 4.2 – Схема адресації пристроїв IoT

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Kryvlenia_IoT_2	Internet	10.25.57.103	/27	10.25.58.97	VLAN17	Fa0/24
	LAN	10.7.2.1	/28	-	-	Wireless
Kryvlenia_CM_Dtector_2.1	Wireless	10.7.2.2	/28	10.7.2.1	-	Wireless
Kryvlenia_Cam_2.1	Wireless	10.7.2.3	/28	10.7.2.1	-	Wireless
Kryvlenia_Cam_2.2	Wireless	10.7.2.4	/28	10.7.2.1	-	Wireless
Kryvlenia_Cam_2.3	Wireless	10.7.2.5	/28	10.7.2.1	-	Wireless
Kryvlenia_MD_2.1	Wireless	10.7.2.6	/28	10.7.2.1	-	Wireless
Kryvlenia_MD_2.2	Wireless	10.7.2.7	/28	10.7.2.1	-	Wireless
Kryvlenia_MD_2.3	Wireless	10.7.2.8	/28	10.7.2.1	-	Wireless
Kryvlenia_Siren_2.1	Wireless	10.7.2.9	/28	10.7.2.1	-	Wireless
Kryvlenia_IoT_Lock_2.1	Wireless	10.7.2.10	/28	10.7.2.1	-	Wireless
Kryvlenia_MCU_WB_2.1	Wireless	10.7.2.11	/28	10.7.2.1	-	Wireless
Kryvlenia_MCU_Security_2.1	Wireless	10.7.2.12	/28	10.7.2.1	-	Wireless
Kryvlenia_MCU_WB_2.2	Wireless	10.7.2.13	/28	10.7.2.1	-	Wireless
Kryvlenia_MCU_Security_2.2	Wireless	10.7.2.14	/28	10.7.2.1	-	Wireless
Kryvlenia_IoT_3	Internet	10.25.56.9	/24	10.25.56.1	-	Fa0/24
	LAN	10.7.3.1	/27	-	-	Wireless
Kryvlenia_CM_Dtector_3.1	Wireless	10.7.3.2	/27	10.7.3.1	-	Wireless
Kryvlenia_CM_Dtector_3.2	Wireless	10.7.3.3	/27	10.7.3.1	-	Wireless
Kryvlenia_CM_Dtector_3.3	Wireless	10.7.3.4	/27	10.7.3.1	-	Wireless
Kryvlenia_Cam_3.1	Wireless	10.7.3.5	/27	10.7.3.1	-	Wireless
Kryvlenia_Cam_3.2	Wireless	10.7.3.6	/27	10.7.3.1	-	Wireless
Kryvlenia_Cam_3.3	Wireless	10.7.3.7	/27	10.7.3.1	-	Wireless
Kryvlenia_MD_3.1	Wireless	10.7.3.8	/27	10.7.3.1	-	Wireless
Kryvlenia_MD_3.2	Wireless	10.7.3.9	/27	10.7.3.1	-	Wireless
Kryvlenia_Siren_3.1	Wireless	10.7.3.10	/27	10.7.3.1	-	Wireless
Kryvlenia_MCU_Auto_Door_3.1	Wireless	10.7.3.11	/27	10.7.3.1	-	Wireless
Kryvlenia_CM_Dtector_4.1	Wireless	10.7.3.11	/27	10.7.3.1	-	Wireless
Kryvlenia_CM_Dtector_4.2	Wireless	10.7.3.12	/27	10.7.3.1	-	Wireless
Kryvlenia_Cam_4.1	Wireless	10.7.3.13	/27	10.7.3.1	-	Wireless

Продовження таблиці 4.2

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Kryvlenia_Cam_4.2	Wireless	10.7.3.14	/27	10.7.3.1	-	Wireless
Kryvlenia_Cam_4.3	Wireless	10.7.3.15	/27	10.7.3.1	-	Wireless
Kryvlenia_Cam_4.4	Wireless	10.7.3.16	/27	10.7.3.1	-	Wireless
Kryvlenia_MD_4.1	Wireless	10.7.3.17	/27	10.7.3.1	-	Wireless
Kryvlenia_MD_4.2	Wireless	10.7.3.18	/27	10.7.3.1	-	Wireless
Kryvlenia_Siren_4.1	Wireless	10.7.3.19	/27	10.7.3.1	-	Wireless
Kryvlenia_IoT_5	Internet	10.25.58.67	/27	10.25.58.65	-	Fa0/24
	LAN	10.7.5.1	/28	-	-	Wireless
Kryvlenia_CM_Dtector_5.1	Wireless	10.7.5.2	/28	10.7.5.1	-	Wireless
Kryvlenia_CM_Dtector_5.2	Wireless	10.7.5.3	/28	10.7.5.1	-	Wireless
Kryvlenia_CM_Dtector_5.3	Wireless	10.7.5.4	/28	10.7.5.1	-	Wireless
Kryvlenia_Cam_5.1	Wireless	10.7.5.5	/28	10.7.5.1	-	Wireless
Kryvlenia_Cam_5.2	Wireless	10.7.5.6	/28	10.7.5.1	-	Wireless
Kryvlenia_Cam_5.3	Wireless	10.7.5.7	/28	10.7.5.1	-	Wireless
Kryvlenia_Cam_5.4	Wireless	10.7.5.8	/28	10.7.5.1	-	Wireless
Kryvlenia_MD_5.1	Wireless	10.7.5.9	/28	10.7.5.1	-	Wireless
Kryvlenia_MD_5.2	Wireless	10.7.5.10	/28	10.7.5.1	-	Wireless
Kryvlenia_Siren_5.1	Wireless	10.7.5.11	/28	10.7.5.1	-	Wireless

Додамо IP-адресу IoT сервера з доменним ім'ям med.iot.ua до DNS сервера. Після цього, заходимо на web-застосунок через будь-який комп'ютер в основній мережі та створюємо акаунт з ім'ям: «KryvleniaNY123202» і паролем: «KryvleniaIoT». Це потрібно для підключення IoT-речей до сервера (рисунок 4.8), з подальшим налаштуванням сценаріїв для них.

IoT Server

None
 Home Gateway
 Remote Server

Server Address
 User Name
 Password

Рисунок 4.8 – Підключення IoT-речі до IoT-сервера

Після підключення IoT-речей, вони з'являться у web-застосунку (рисунок 4.9).

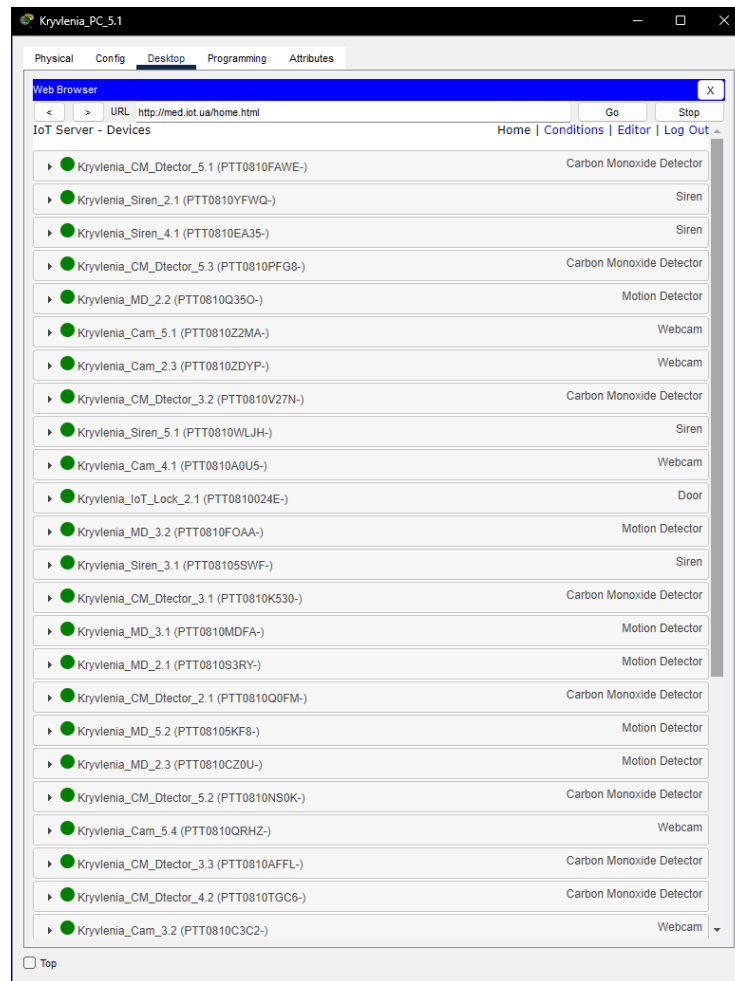


Рисунок 4.9 – Приєднані IoT-пристрої у web-застосунку

Після додавання IoT-пристроїв до серверу, можна починати створювати сценарії, перейшовши до сторінки Conditions у web-застосунку. Налаштування сценаріїв проходить згідно з алгоритмами (рисунки 4.1 – 4.4, сторінки 80 – 82).

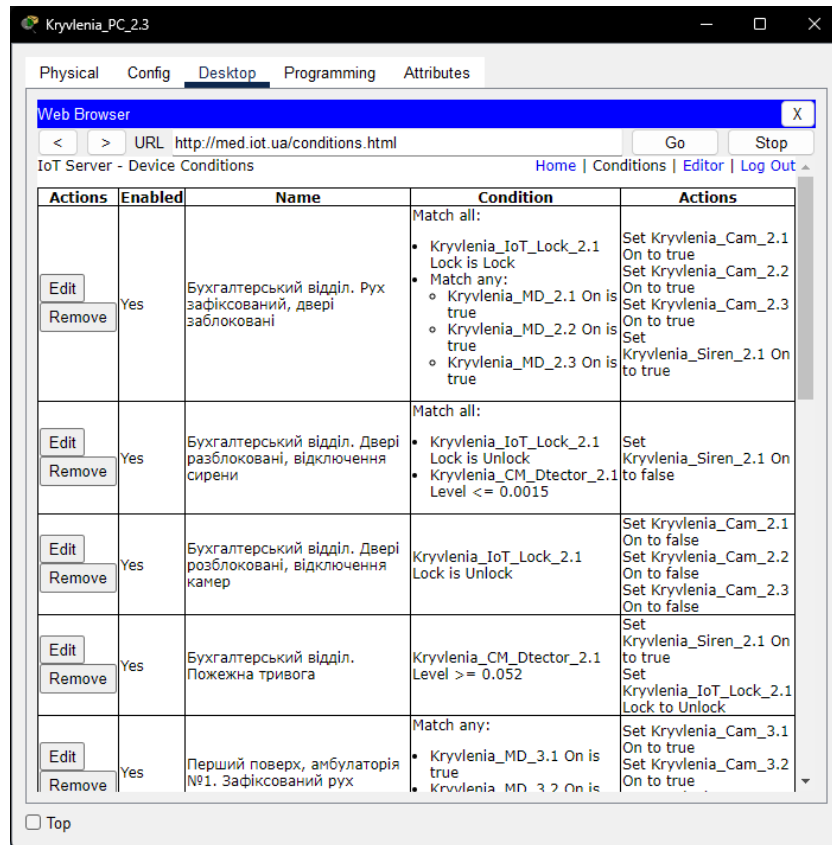


Рисунок 4.10 – Налаштовані сценарії на IoT-сервері

Для програмування мікроконтролерів у Cisco Packet Tracer використаємо вбудований пристрій MCU. Щоб приєднати його до IoT-шлюзу, у вкладці Physical додамо до плати модуль PT-IOT-NM-W1, привласнимо йому IP-адресу та під'єднаємо до сервера. Це потрібно для виведення інформації з IoT-компонентів, які будуть підключені до контролера. Програмування проводиться у вкладці Programming (рисунок 4.11, сторінка 89), де створюємо порожній проект на мові Python.

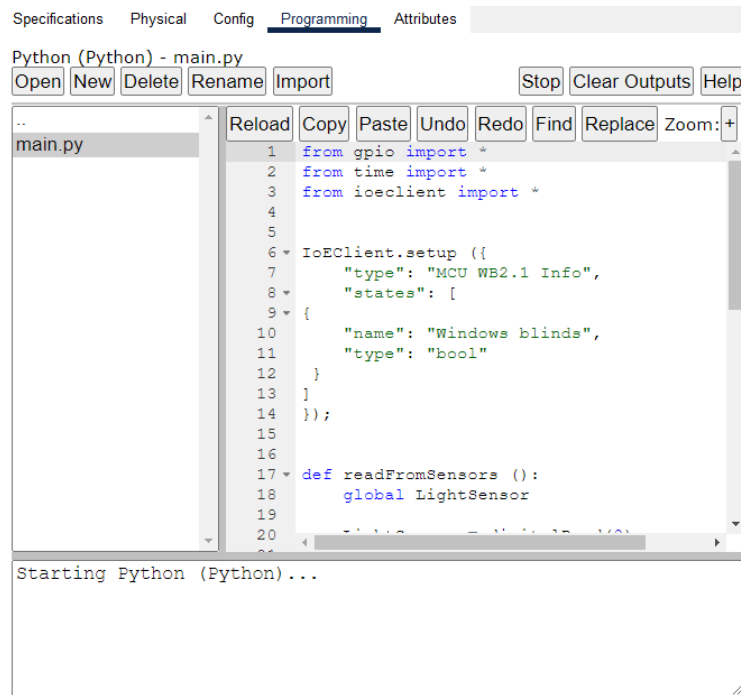


Рисунок 4.11 – Вкладка Programming на MCU

4.4 Перевірка працездатності IoT

Після налаштування сценаріїв на IoT-сервері та програмування контролерів перевіримо, чи працюють вони за заданими алгоритмами.

Перевіряємо систему пожежної безпеки у бухгалтерському відділі. Для збільшення рівня чадного газу додамо пристрій 'Old Car' та включимо його, натиснувши на нього з затиснутою клавішею ALT. Результати перевірки продемонстровані на рисунках 4.12 – 4.13.

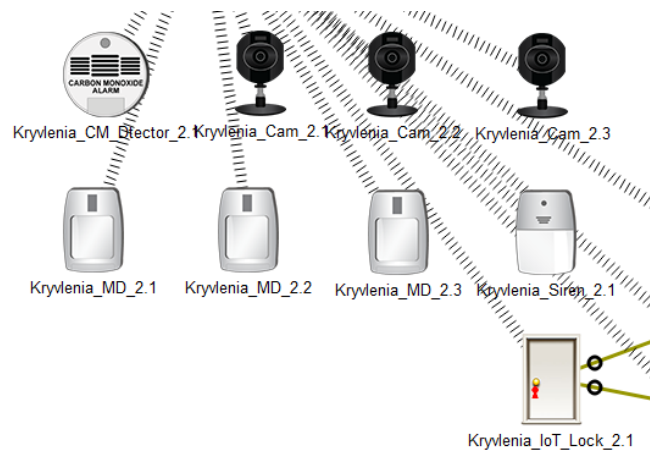


Рисунок 4.12 – Бухгалтерський відділ, двері заблоковані

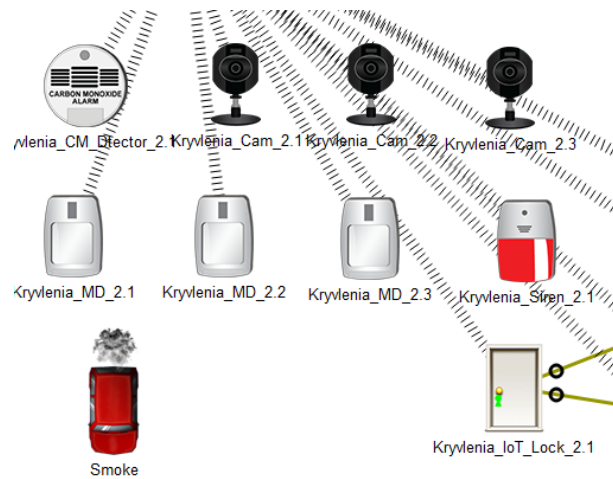


Рисунок 4.13 – Бухгалтерський відділ. При пожежі вмикається сирена та розблоковуються двері

Перевірка системи відеоспостереження при втручанні приведена на рисунку 4.14.

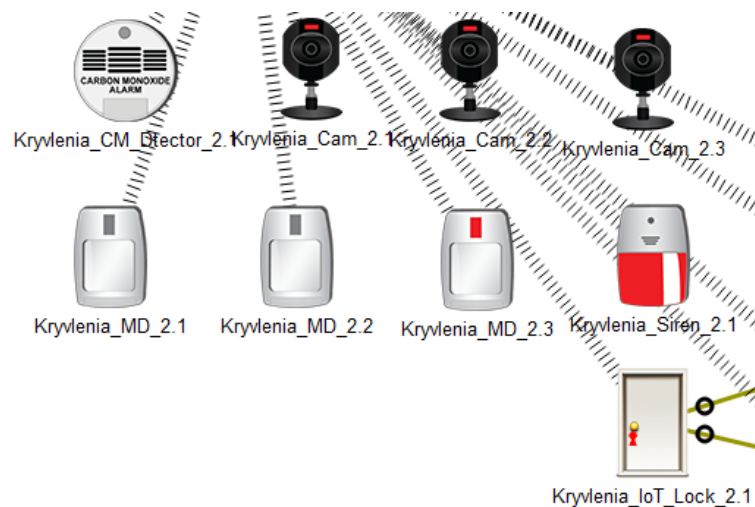


Рисунок 4.14 – Бухгалтерський відділ. Якщо зафіксований рух та заблоковані двері, вмикаються камери та сирена

При розблокуванні дверей, запис на камерах та сирена вимикаються.

Перевірка працездатності автоматичних жалюзі приведена на рисунках 4.15 – 4.16, сторінка 91.

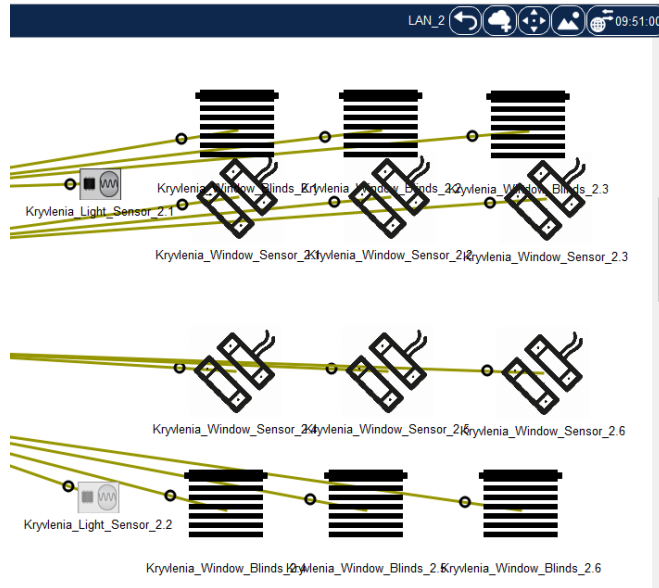


Рисунок 4.15 – Днем жалюзі зачинені

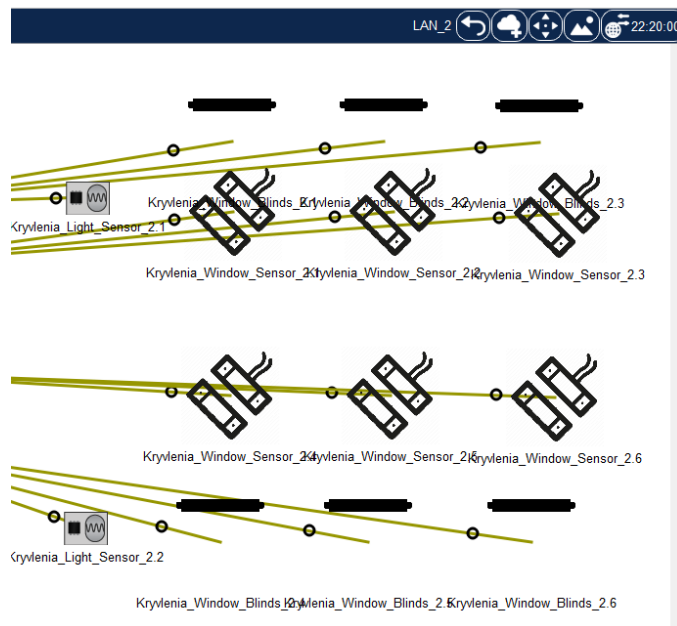


Рисунок 4.16 – Уночі жалюзі відчиняються

Перевірка працездатності системи додаткового захисту від несанкціонованого доступу через вікно приведена на рисунку 4.17, сторінка 92.

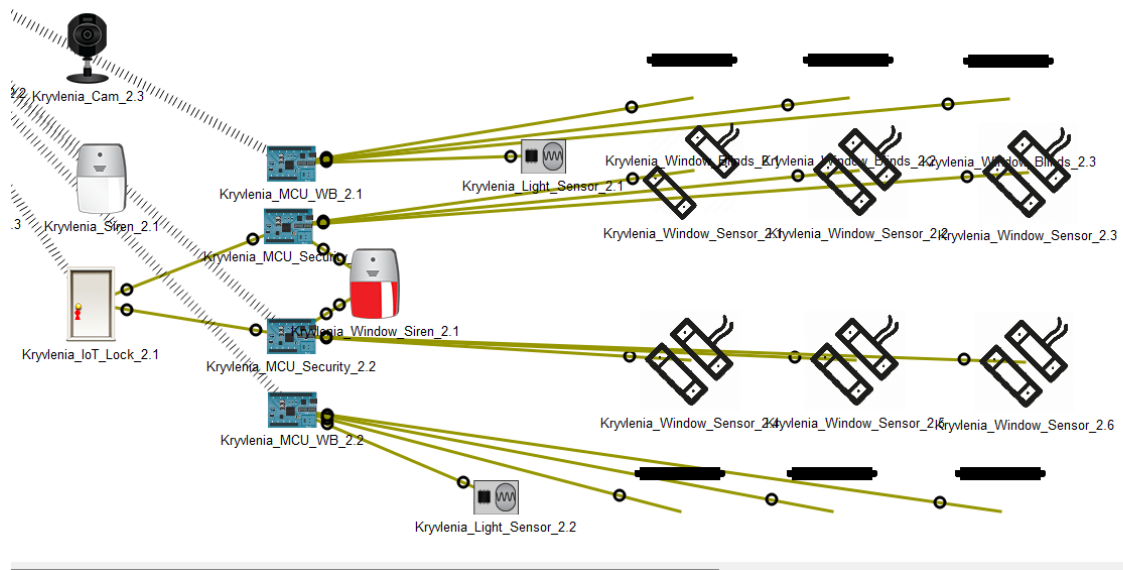


Рисунок 4.17 – При відкритті вікна, коли двері заблоковані, вмикається сирена

Перевірка автоматичних дверей у першому поверсі амбулаторії №1 приведена на рисунках 4.18 – 4.20

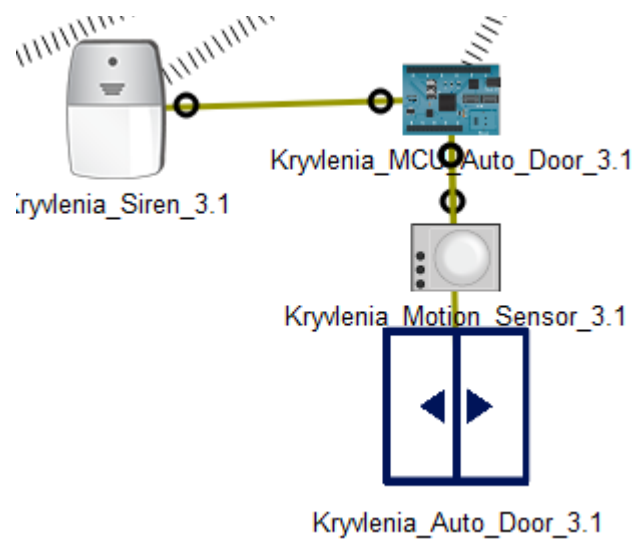


Рисунок 4.18 – Зачинені двері

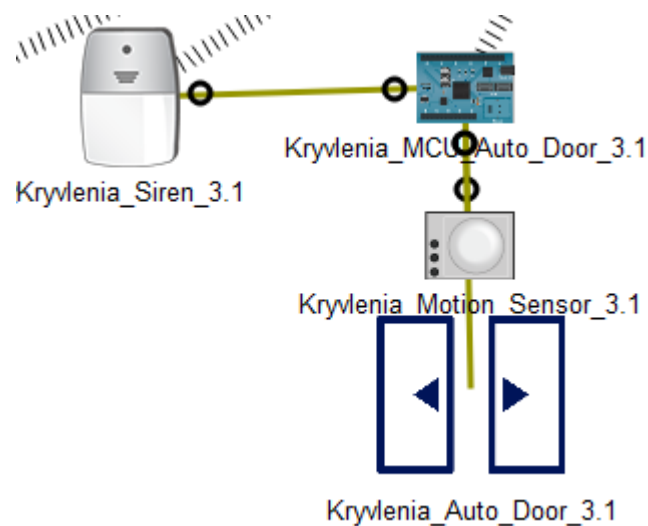


Рисунок 4.19 – Якщо сенсор руху фіксує рух, тоді двері відчиняються

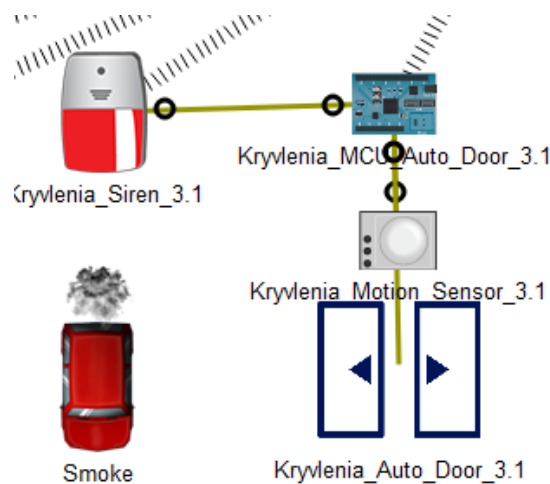


Рисунок 4.20 – При пожежі двері відчиняються автоматично

Система пожежної безпеки та система відеоспостереження на другому поверсі амбулаторії №1 та у дитячій поліклініці працюють так само, як і у бухгалтерському відділі, але камери вимикаються вручну та вмикаються автоматично, якщо були вимкнені під час зафіксування руху датчиками руху.

IoT-пристрої на другому поверсі амбулаторії №1 працюють від IoT-шлюзу на першому поверсі.

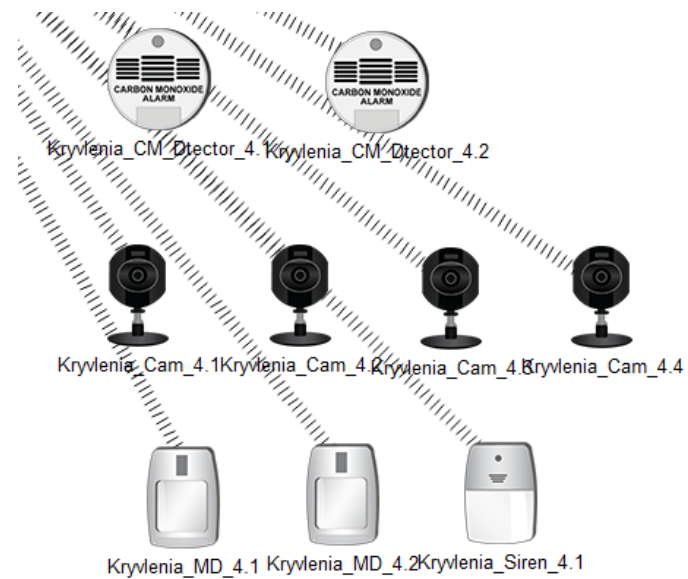


Рисунок 4.21 – IoT-пристрої у мережі другого поверху амбулаторії №1

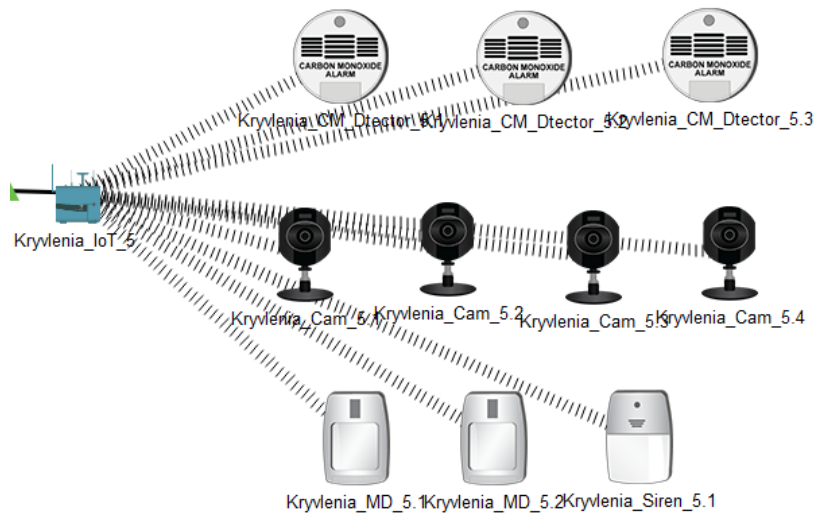


Рисунок 4.22 –IoT-пристрої у мережі дитячої поліклініки амбулаторії №2

Данні з MCU, які передаються на сервер представлені на рисунках 4.23 – 4.25, сторінка 95.

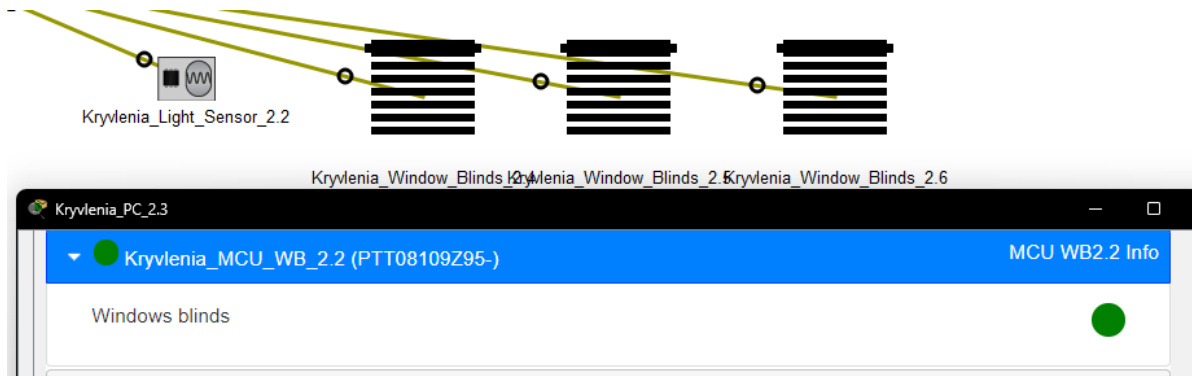


Рисунок 4.23 – Статус жалюзі на сервері IoT

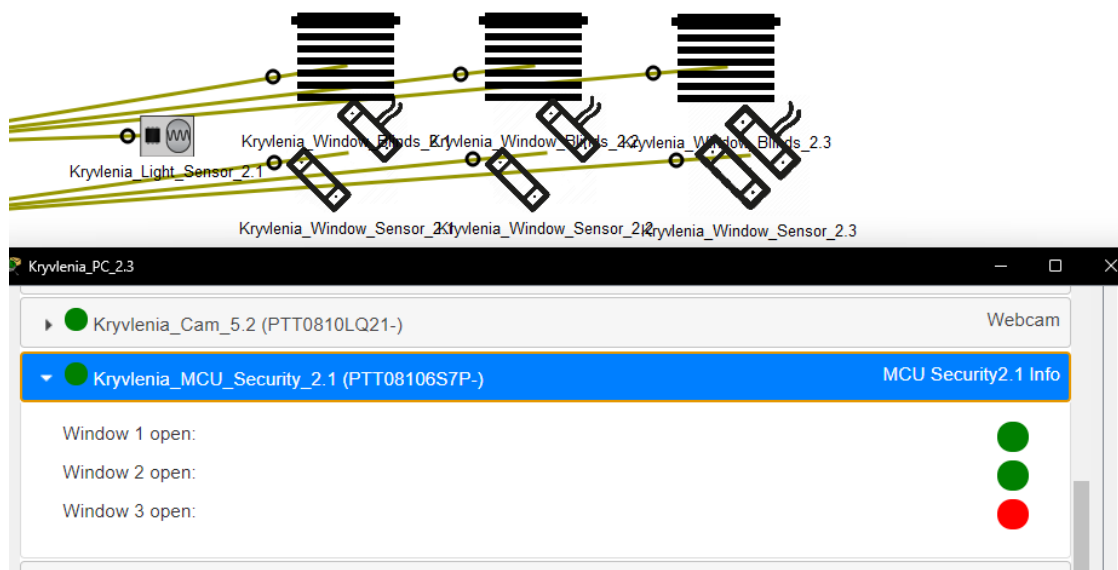


Рисунок 4.24 – Статус вікон на сервері IoT

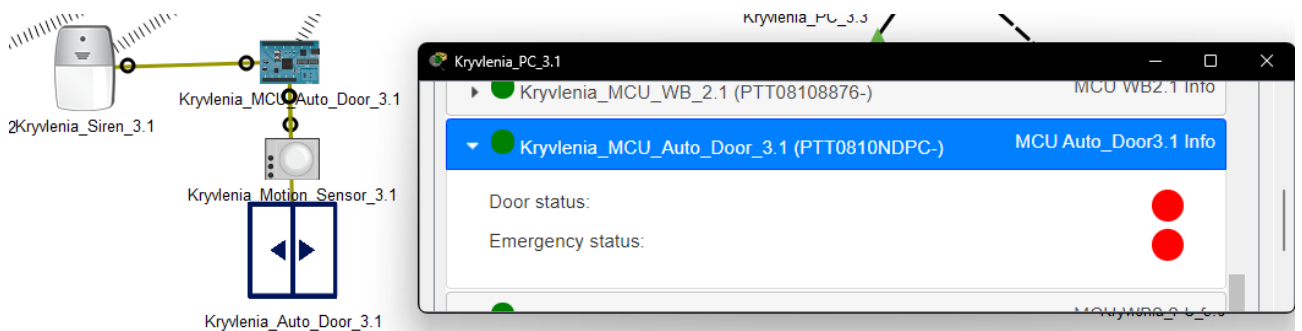


Рисунок 4.25 – Статус автоматичних дверей та надзвичайної ситуації на сервері IoT

Статус надзвичайної ситуації горить зеленим, коли включена сирена.

ВИСНОВКИ

В даному кваліфікаційному проекті була проведений аналіз роботи комп'ютерних мереж в галузі ОЗ та побудована комп'ютерна мережа для КЗ «Першотравенська центральна міська лікарня», з впровадженням систем безпеки та автоматизації за допомогою IoT-речей.

Були написані вимоги, розроблена структурна схема лікарні, розроблена специфікація обладнання.

За вимогами та завданням кваліфікаційної роботи були проведені базові налаштування на мережевих пристроїв, що забезпечують захист терміналу обладнання від несанкціонованого доступу. До всіх підмереж був налаштований протокол DHCP, який автоматично призначає IP-адресу кінцевим вузлам. Був налаштований VLAN для розділення мережі бухгалтерського відділу амбулаторії №2 на віртуальні підмережі для бухгалтерії, відділу кадрів, інших користувачів та мережевих пристроїв. Між маршрутизаторами був налаштований протокол динамічної маршрутизації OSPF. Для безпечного з'єднання між основною мережею та віддаленою був налаштований VPN. Для виходу в інтернет був налаштований NAT.

Після налаштування комп'ютерної мережі лікарні було проведено впровадження IoT-пристроїв, розроблена схема адресації, налаштований IoT-сервер. На IoT-сервері були налаштовані сценарії безпеки в разі виникнення пожежі та системи відеоспостереження. За допомогою контролерів були створені системи автоматичних дверей та жалюзі, система безпеки в разі втручання у будівлю через вікно. Програмування на контролерів проводилося на мові Python.

Усі налаштування проводилися в програмному забезпеченні Cisco Packet Tracer.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про Helsi – [Електронний ресурс] – <https://helsi.me/about> (дата звернення 04.04.2024)
2. Головна сторінка Health24 – [Електронний ресурс] – <https://h24.ua/> (дата звернення 04.04.2024)
3. Головна сторінка E-life – [Електронний ресурс] – <https://e-life.com.ua/> (дата звернення 04.04.2024)
4. Голосна сторінка Ciet – [Електронний ресурс] – <https://ciet-holding.com/> (дата звернення 04.04.2024)
5. Офіційний сайт КЗ "Першотравенська центральна міська лікарня" – [Електронний ресурс] – <https://persh.lic.org.ua/> (дата звернення 06.04.2024)
6. Проект Misto.ua. Підрозділи КЗ "Першотравенська центральна міська лікарня" – [Електронний ресурс] – <https://micto.ua/pershotravenska-tsentralna-miska-likarnia-dnipropetrovskoi-oblasnoi-rady-i158380/> (дата звернення 06.04.2024)
7. 2ip. Рейтинг інтернет-провайдеру «Візит» – [Електронний ресурс] – <https://2ip.ua/ua/services/providers-rating?act=1&asid=52045> (дата звернення 07.04.2024)
8. eSecurity Planet. Ultimate Guide to How VLANs Work – [Електронний ресурс] – <https://www.esecurityplanet.com/networks/what-is-a-vlan/> (дата звернення 15.04.2024)
9. Наказ Міністерства розвитку громад та територій України ДБН В.2.2-10:2022 "Заклади охорони здоров'я. Основні положення" від 26.12.2022 №278 – [Електронний ресурс] – https://dreamdim.ua/wp-content/uploads/2023/03/DBN_V2-2-10_2022.pdf (дата звернення 20.04.2024)
10. Наказ Міністерства охорони здоров'я України «Про затвердження Державних санітарних норм і правил «Санітарно-протиепідемічні вимоги до новозбудованих, реставрованих і реконструйованих закладів охорони здоров'я»

та Змін до деяких нормативно-правових актів Міністерства охорони здоров'я» від 05.04.2023 № 562/39618 – [Електронний ресурс] – <https://zakon.rada.gov.ua/laws/show/z0562-23#Text> (дата звернення 22.04.2024)

11. IT Education Center. Системний адміністратор: обов'язки, ролі, плюси та мінуси професії – [Електронний ресурс] – https://itedu.center/ua/blog/sysadministration/system_administrator/ (дата звернення 22.04.2024)

12. Keenetic. Якісні кабелі - основа надійної передачі даних в мережах Ethernet – [Електронний ресурс] – <http://surl.li/tktzj> (дата звернення 25.04.2024)

13. Router-switch. CISCO2911/K9 Datasheet – [Електронний ресурс] – <https://www.router-switch.com/pdf2html/pdf/cisco2911-dc-k9-datasheet.pdf> (дата звернення 25.04.2024)

14. Router-switch. WS-C2960-24TT-L Datasheet – [Електронний ресурс] – <https://www.router-switch.com/pdf2html/pdf/ws-c2960-24tt-l-datasheet.pdf> (дата звернення 25.04.2024)

Додаток А

Схема першого поверху амбулаторії №1
та мнемосхема приміщення дитячої поліклініки амбулаторії №2

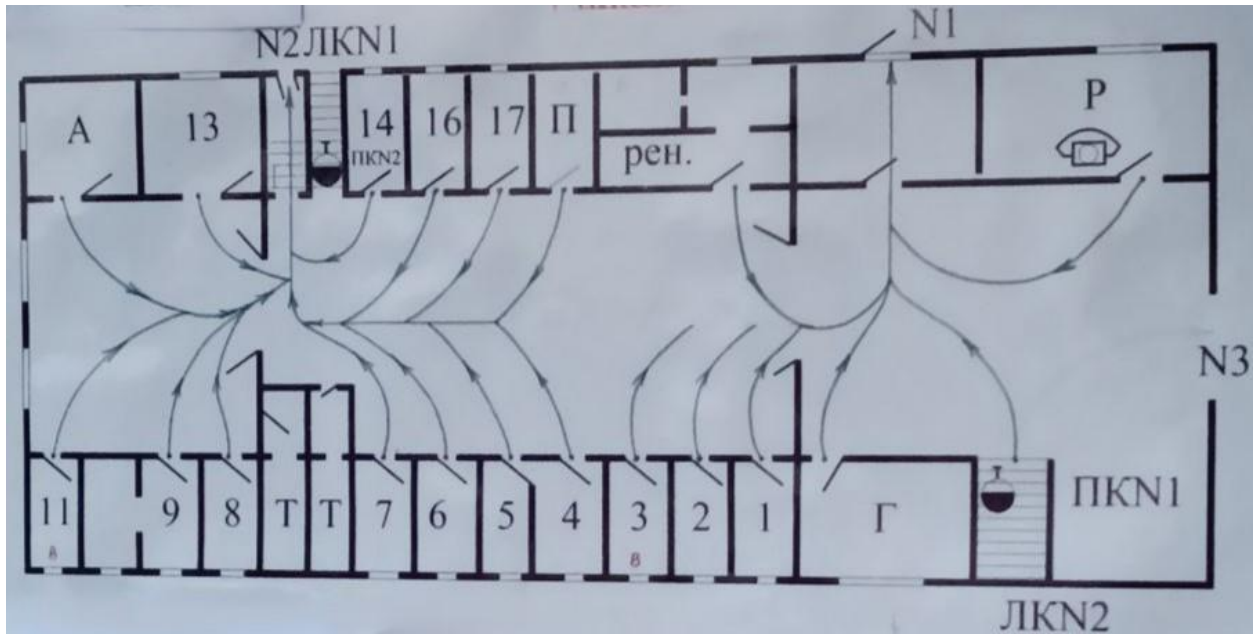


Рисунок А.1 - Схема першого поверху амбулаторії №1

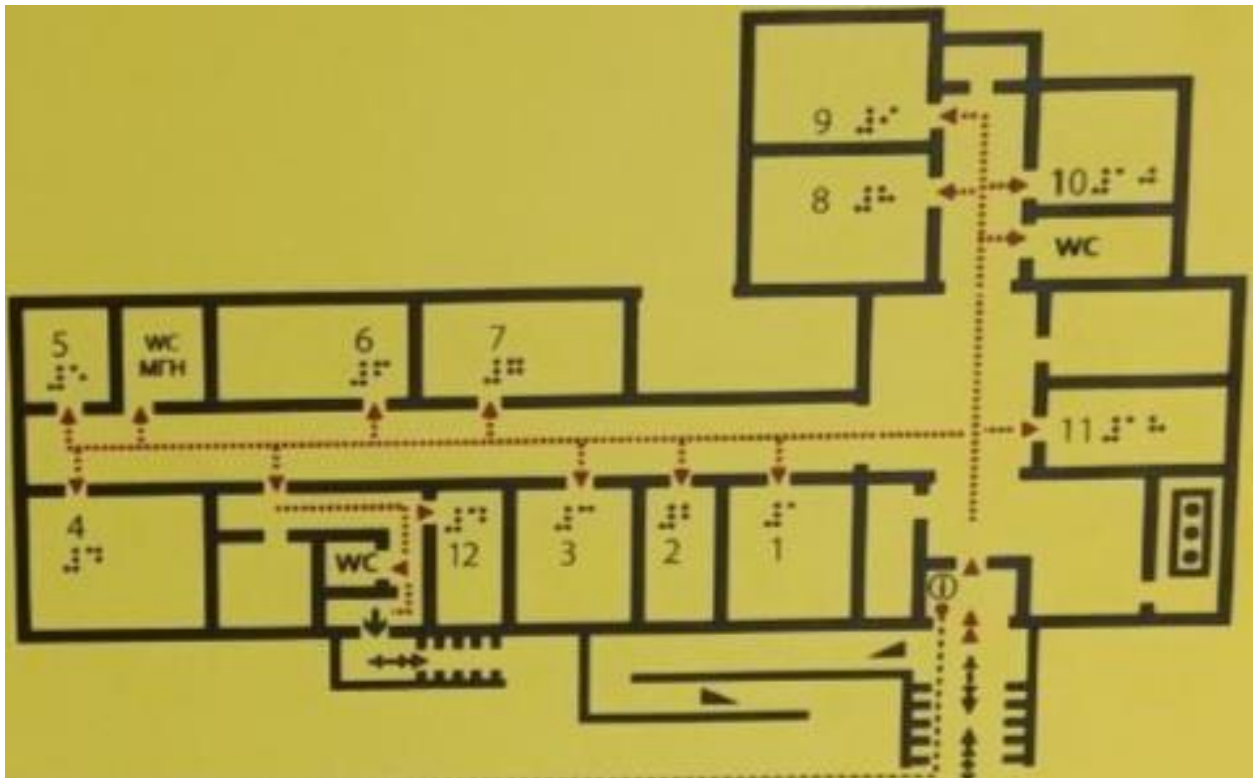
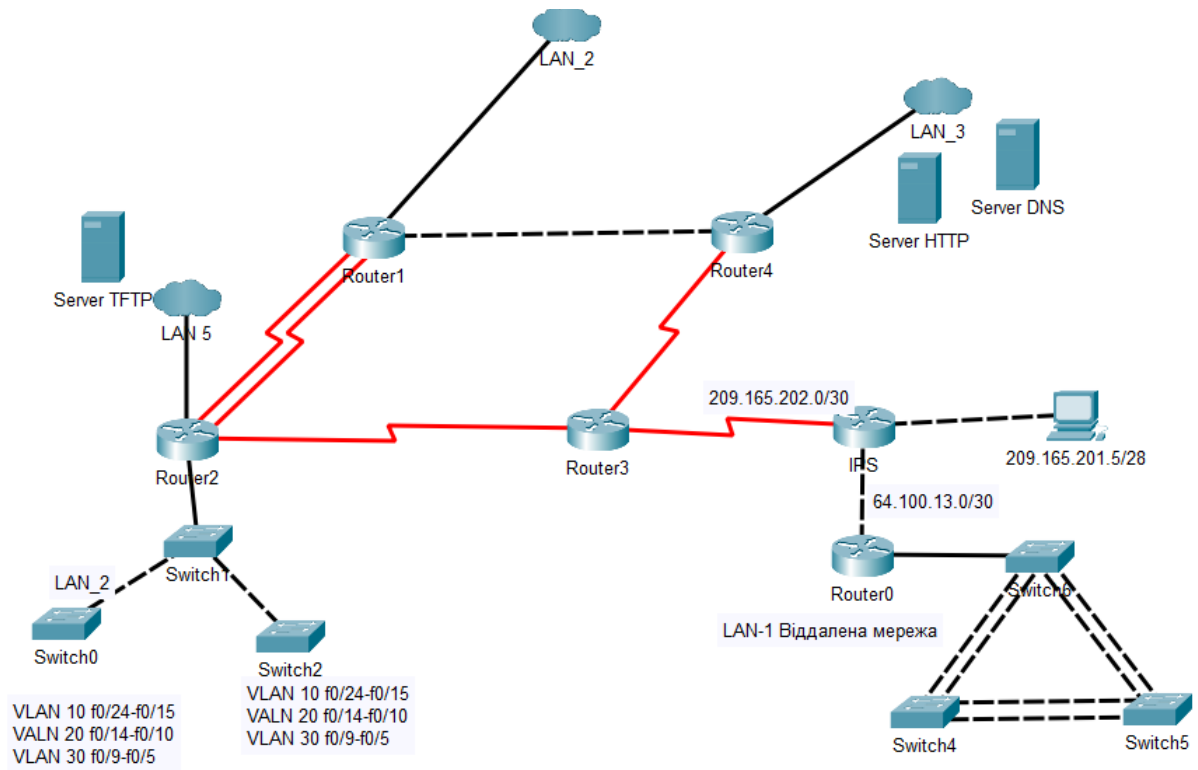


Рисунок А.2 - Мнемосхема приміщення дитячої поліклініки амбулаторії №2

Додаток Б

Загальна архітектура мережі, яка була надана замовником



Додаток В

Текст програми налаштування IoT-пристроїв на мікроконтролері

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

**ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
НАЛАШТУВАННЯ ІОТ-ПРИСТРОЇВ НА
МІКРОКОНТРОЛЕРІ**

Текст програми

804.02070743.24007-01 12 01

Листів 10

АНОТАЦІЯ

Даний додаток містить в собі програмні коди з контролерів для IoT-компонентів для комп'ютерної системи Першотравенської центральної міської лікарні.

Програми призначені для системи автоматичних жалюзі, безпеки з використанням віконних сенсорів та автоматичних дверей.

Програми написані мовою Python, у програмуванні контролеру в Cisco Packet Tracer і призначені для контролерів Arduino.

ЗМІСТ

Kryvlenia_MCU_WB_2.1	4
Kryvlenia_MCU_Security_2.1	5
Kryvlenia_MCU_Auto_Door_3.1	8

Kryvlenia_MCU_WB_2.1

```

from gpio import *
from time import *
from ioeclient import *

# Налаштування клієнта ІоЕ
IoEClient.setup ({
    "type": "MCU WB2.1 Info",
    "states": [
{
    "name": "Windows blinds", # Ім'я стану - жалюзі
    "type": "bool" # Тип стану – булевий
}
]
});

# Функція для читання даних з датчиків
def readFromSensors ():
    global LightSensor # Оголошення глобальної змінної LightSensor

    LightSensor = digitalRead(0) # Читання даних з цифрового входу 0
# Функція для запису даних в актуатори
def writeToActuators():
    global Windows_blinds # Оголошення глоб. змінної Windows_blinds
    if (LightSensor == HIGH): # Якщо датчик світла в стані HIGH
        customWrite(1, 0) # Закрити
        customWrite(2, 0)
        customWrite(3, 0)

```

```

    Windows_blinds = 1 # Встановити стан жалюзі в 1 (закриті)
else: # Інакше відкрити жалюзі
    customWrite(1, 1)
    customWrite(2, 1)
    customWrite(3, 1)
    Windows_blinds = 0

```

```
def main():
```

```
    pinMode(0,IN) # Встановлення режиму для порту 0 як входу
```

```
    pinMode(1,OUT) # Встановлення режиму для порту 1 як виходу
```

```
    pinMode(2,OUT)
```

```
    pinMode(3,OUT)
```

```
    while True:
```

```
        readFromSensors() # Читання даних з датчиків
```

```
        writeToActuators() # Запис даних в актуатори
```

```
        IoEClient.reportStates([Windows_blinds]) # Відправка станів на
```

сервер

```
        delay(100) # Затримка в 100 мс
```

```
if __name__ == "__main__":
```

```
    main()
```

Kryvlenia_MCU_Security_2.1

```
from gpio import *
```

```
from time import *
```

```
from ioecient import *
```

```

IoEClient.setup ({
    "type": "MCU Security2.1 Info",
    "states": [
    {
        "name": "Window 1 open:", # Ім'я стану - відкрите вікно 1
        "type": "bool" # Тип стану - булевий
    },
    {
        "name": "Window 2 open:",
        "type": "bool"
    },
    {
        "name": "Window 3 open:",
        "type": "bool"
    }
    ]
});

```

```
def readFromSensors ():
```

```

    global doorLock # Оголошення глобальної змінної doorLock
    global windowSensor1 # Оголошення глоб. змінної windowSensor1
    global windowSensor2
    global windowSensor3

    doorLock = customRead(0)#Читання даних з корист. входу 0
    windowSensor1 = customRead(1)
    windowSensor2 = customRead(2)
    windowSensor3 = customRead(3)

```

```

def writeToActuators():
    global Window1Info # Оголошення глобальної змінної Window1Info
    global Window2Info
    global Window3Info
    # Якщо двері заблоковані та будь-яке з вікон відкрите
    if (doorLock == "1") and ((windowSensor1 == "0") or (windowSensor2
== "0") or (windowSensor3 == "0")):
        customWrite(4, 1) # Увімкнути сигнал тривоги
    else:
        customWrite(4, 0) # Вимкнути сигнал тривоги
    # Перевірка стану вікон і запис в відповідні змінні
    if windowSensor1 == "0":
        Window1Info = 1 # Вікно 1 відкрите
    else:
        Window1Info = 0 # Вікно 1 закрито

    if windowSensor2 == "0":
        Window2Info = 1
    else:
        Window2Info = 0

    if windowSensor3 == "0":
        Window3Info = 1
    else:
        Window3Info = 0

def main():

```

```

pinMode(0,IN) # Встановлення режиму для порту 0 як входу
pinMode(1,IN)
pinMode(2,IN)
pinMode(3,IN)
pinMode(4,OUT) # Встановлення режиму для порту 4 як виходу
while True:
    readFromSensors() # Читання даних з датчиків
    writeToActuators() # Запис даних в актуатори
    IoEClient.reportStates([Window1Info, Window2Info,
Window3Info]) # Відправка станів вікон на сервер
    delay(100)
if __name__ == "__main__":
    main()

```

Kryvlenia_MCU_Auto_Door_3.1

```

from gpio import *
from time import *
from ioecclient import *

IoEClient.setup ({
    "type": "MCU Auto_Door3.1 Info",
    "states": [
{
    "name": "Door status:", # Ім'я стану - стан дверей
    "type": "bool" # Тип стану - булевий

```

```

    },
    {
        "name": "Emergency status:", # Ім'я стану - стан надзвичайн. ситуації
        "type": "bool"
    }
]
});

```

```
def readFromSensors():
```

```

    global MotionSensor # Оголошення глобальної змінної MotionSensor
    global Emergency # Оголошення глобальної змінної Emergency

```

```

    MotionSensor = digitalRead(0) # Читання даних з цифрового входу 0

```

```

    Emergency = customRead(1) # Читання даних з корист. входу 1

```

```
def writeToActuators():
```

```

    global DoorStatus # Оголошення глобальної змінної DoorStatus

```

```

    global EmergencyStatus # Оголошення глоб. змінної EmergencyStatus

```

```

    # Якщо виявлено рух або виникла аварійна ситуація

```

```

    if (MotionSensor == HIGH) or (Emergency == "1"):

```

```

        customWrite(2, 1) # Відкрити двері

```

```

        DoorStatus = 1 # Встановити стан дверей в 1 (відкриті)

```

```

    else:

```

```

        customWrite(2, 0) # Закрити двері

```

```

        DoorStatus = 0 # Встановити стан дверей в 0 (закриті)

```

```

    # Перевірка стану надзвичайної ситуації

```

```

    if Emergency == "1":

```

```

        EmergencyStatus = 1 # Встановити стан надзвичайної ситуації

```

else:

EmergencyStatus = 0

def main():

pinMode(0,IN) # Встановлення режиму для порту 0 як входу

pinMode(1,IN)

pinMode(2,OUT) # Встановлення режиму для порту 2 як виходу

while True:

readFromSensors()

writeToActuators()

IoEClient.reportStates([DoorStatus, EmergencyStatus])

delay(100)

if __name__ == "__main__":

main()