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

здобувача Скоропад Євгена Володимировича
(ПІБ)

академічної групи 123-21-1
(шифр)

спеціальності 123 Комп’ютерна інженерія
(код і назва спеціальності)

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

на тему «Комп'ютерна система компанії з продажу та ремонту мобільних телефонів з детальним опрацюванням IoT комплексу робочого місця паяльщика та корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Молодець Б.В., доц.			
спеціальної частини	Панферова Я.В., ас.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« » _____ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Скоропад Є.В. **академічної групи** 123-21-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

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

на тему «Комп'ютерна система компанії з продажу та ремонту мобільних телефонів з детальним опрацюванням IoT комплексу робочого місця паяльщика та корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел показати актуальність завдання, сформулювати мету та задачі виконання кваліфікаційної роботи	10.02.2025
Розробка апаратної частини	Сформулювати найменування й призначення комп'ютерної системи, висунути технічні вимоги до неї. Виконати розробку апаратної частини комп'ютерної системи.	20.04.2025
Розробка корпоративної мережі	Побудувати в Packet Tracer типову мережну топологію компанії з продажу та ремонту мобільних телефонів	07.05.2025
Розробка компонента системи	Розробити IoT комплекс робочого місця паяльщика	31.05.2025

Завдання видано _____ доц. Молодець В.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання _____ Скоропад. Є.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 64 с., 32 рис., 9 табл., 1 дод., 10 джерел.

КОМП’ЮТЕРНА СИСТЕМА, КОРПОРАТИВНА МЕРЕЖА, IoT, МЕРЕЖЕВА ІНФРАСТРУКТУРА, VLAN, OSPF, NAT, DHCP, DNS, ACL, БЕЗПЕКА МЕРЕЖІ

У роботі розглянуто проєктування комп’ютерної системи для підприємства, що спеціалізується на продажу та сервісному обслуговуванні мобільних телефонів. Центральне місце займає впровадження кіберфізичної підсистеми, призначеної для моніторингу параметрів робочого середовища паяльника з використанням технологій Інтернету речей (IoT).

Метою дослідження є побудова цифрової інфраструктури, що поєднує функції збирання, обробки й аналізу даних з IoT-пристроїв та забезпечує централізоване керування інформаційними потоками. Архітектура проєкту орієнтована на підтримку високого рівня керованості, адаптивності та інформаційної безпеки.

Система реалізована з урахуванням принципів логічного розділення трафіку (VLAN) та можливості подальшого масштабування без значних фінансових витрат. Усі елементи інфраструктури об’єднані в єдину корпоративну мережу з централізованим адмініструванням.

Для забезпечення стабільної експлуатації запропоновано набір апаратного та програмного забезпечення, адаптованого до умов цілодобового функціонування. Ефективність системи перевірено шляхом моделювання в середовищі Cisco Packet Tracer. За результатами віртуального тестування підтверджено її надійність, гнучкість у налаштуванні та відповідність сучасним вимогам до функціональності.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КС – комп’ютерна система;

LAN – локальна обчислювальна мережа;

WAN – глобальна обчислювальна мережа;

IoT – англ. Internet of Things, концепція підключення пристроїв для збору і обміну даними;

VLAN – віртуальна локальна мережа, що дозволяє логічно розділяти мережеві сегменти;

DHCP – англ. Dynamic Host Configuration Protocol, протокол автоматичної видачі IP-адрес;

DNS – англ. Domain Name System, система доменних імен для ідентифікації пристроїв у мережі;

Wi-Fi – бездротова технологія передачі даних.

ACL – англ. Access Control List, список контролю доступу до мережевих ресурсів;

PoE – англ. Power over Ethernet, передача електроживлення разом із даними через мережевий кабель;

HTTPS – захищена версія протоколу HTTP;

TFTP – англ. Trivial File Transfer Protocol, простий протокол передачі файлів;

MAC – англ. Media Access Control, апаратна адреса мережевого інтерфейсу;

NAT – англ. Network Address Translation, трансляція мережевих адрес;

UPS – англ. Uninterruptible Power Supply, джерело безперебійного живлення.

MQTT – англ. Message Queuing Telemetry Transport, протокол передачі даних для IoT-пристроїв.

ВСТУП

Сучасні умови розвитку бізнесу потребують високого ступеня автоматизації та ефективного управління інформаційними потоками з метою забезпечення стабільності та конкурентоспроможності підприємств. Організації, що здійснюють продаж і ремонт мобільних пристроїв, демонструють сталу потребу у впровадженні інноваційних цифрових рішень, зокрема в галузі інформаційних технологій.

Актуальність обраної тематики підтверджується активним розвитком наукових досліджень у сфері комп'ютерних та кіберфізичних систем, телеметрії, мережевої безпеки та Інтернету речей. Провідні технологічні компанії – такі як Cisco, Siemens, Huawei – а також дослідницькі центри з інформаційних технологій, фокусуються на побудові адаптивних архітектур для підприємств сервісного типу. Зокрема, вивчаються питання оптимізації структур підключення IoT-пристроїв, безпечної маршрутизації даних та інтеграції з хмарними сервісами.

Світові тенденції демонструють стрімке зростання попиту на рішення, які поєднують традиційні комп'ютерні мережі з IoT-інфраструктурою. Усе більше підприємств переходять до використання розподілених систем збору й аналізу технічних параметрів, що дозволяє оперативно реагувати на зміни та зменшити вплив людського фактора на виробничі процеси. У центрі уваги – безпечний обмін даними, централізоване адміністрування й енергоефективність.

Формування надійної інформаційної інфраструктури є ключовим чинником для безперервного функціонування сервісних підрозділів, вдосконалення логістики, підвищення якості обслуговування клієнтів та створення комфортних умов для персоналу. Застосування IoT-технологій надає можливість у реальному часі контролювати параметри робочого середовища – температуру, вентиляцію, освітлення, – що сприяє підвищенню безпеки та точності виконання технологічних операцій.

У межах дослідження передбачено розроблення архітектури комп’ютерної системи з урахуванням практичних потреб підприємства. Основну увагу зосереджено на проєктуванні корпоративної мережі, впровадженні засобів телеметрії, методах зберігання інформації, кіберзахисті та інструментах для централізованого адміністрування. Також проаналізовано можливості сегментації трафіку, впровадження протоколу HTTP для збору та передавання даних із сенсорів.

Отримані результати можуть бути використані як основа для розбудови подібних систем в інших організаціях, орієнтованих на цифрову трансформацію та автоматизацію сервісних і виробничих процесів.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика галузі та умов застосування КС

Галузь роздрібної торгівлі мобільними телефонами та їх технічного обслуговування тісно пов’язана з використанням сучасних цифрових технологій, які виступають ключовим інструментом забезпечення стабільної та ефективної діяльності підприємств. Успішне функціонування компаній у цій сфері неможливе без впровадження комп’ютерних систем, які дозволяють автоматизувати основні бізнес-процеси.

Сучасні інформаційні рішення охоплюють управління товарними залишками, облік продажів, логістичне планування, аналітику попиту та контроль взаємодії з клієнтами. Єдина інформаційна структура, яка об’єднує головний офіс, філії та сервісні підрозділи, забезпечує оперативний обмін даними та узгоджене виконання завдань усіма структурними елементами підприємства.

Використання CRM-систем сприяє ефективній роботі з клієнтськими запитами, швидкому опрацюванню замовлень і підвищенню рівня сервісу. Водночас у сервісних майстернях активно застосовуються засоби цифрового моніторингу, що забезпечують точний облік ремонтних операцій та результатів діагностики за допомогою спеціалізованого програмного забезпечення.

Також увага приділяється автоматизації сервісних процесів. Робочі місця майстрів обладнані інструментами цифрового моніторингу, що дає змогу вести облік ремонтів та діагностики із використанням профільного ПЗ.

Інтеграція IoT-рішень дозволяє контролювати параметри мікроклімату в майстернях – зокрема, температуру, наявність диму та роботу витяжних систем. Таке технологічне середовище не лише підвищує безпеку, а й забезпечує дотримання стандартів пайки.

Інформаційна система підприємства повинна бути стабільною, гнучкою та адаптованою до поточних і перспективних потреб бізнесу. Основна увага

при цьому зосереджується не на максимальній обчислювальній потужності, а на доступності внутрішніх ресурсів, надійності технічних рішень, зручності адміністрування та можливості безболісного розширення. Це має особливе значення в умовах масштабування бізнесу, відкриття нових філіалів або зміни обсягу послуг.

1.2 Характеристика і структура компанії

Об’єктом розробки є комп’ютерна система компанії, яка спеціалізується на роздрібній торгівлі мобільними телефонами та технічному обслуговуванні електроніки.

Організаційна структура підприємства характеризується чітким розподілом функцій між функціональними підрозділами, що забезпечує ефективну координацію та безперебійне виконання бізнес-процесів. Ключові адміністративні та управлінські функції зосереджені в головному офісі, який виконує завдання стратегічного планування, юридичного супроводу, управління фінансами, маркетингом, логістикою та IT-інфраструктурою.

У центральному офісі облаштована серверна кімната, яка містить телекомунікаційне та мережеве обладнання, необхідне для підтримки безперервної роботи корпоративної мережі.

До складу організаційної структури входять наступні основні відділи (рис. 1.1):

– юридичний відділ, що здійснює правовий супровід господарської діяльності підприємства;

– служба підтримки клієнтів, відповідальна за обробку звернень, надання консультацій та підтримання зворотного зв’язку;

– IT-відділ, який забезпечує функціонування інформаційної інфраструктури, адміністрування мереж і технічну підтримку;

– відділ маркетингу, що формує стратегію просування, аналізує ринок та управляє рекламною діяльністю;

– логістичний сектор, відповідальний за постачання, рух товарів та обслуговування складу;

– робочі місця паяльників, оснащені цифровими та IoT-засобами моніторингу.

Фінансову діяльність координує фінансовий директор, який очолює фінансовий відділ. До його складу входять бухгалтерія, відділ кадрів та економісти-аналітики, що забезпечують бюджетування, облік і кадрову підтримку.

Філіали компанії виконують функції роздрібних магазинів та сервісних центрів. У кожній із них облаштовано зону обслуговування клієнтів і технічну ділянку для ремонту пристроїв. Робочі місця паяльників оснащені сучасним інструментом і сенсорами для моніторингу мікроклімату.

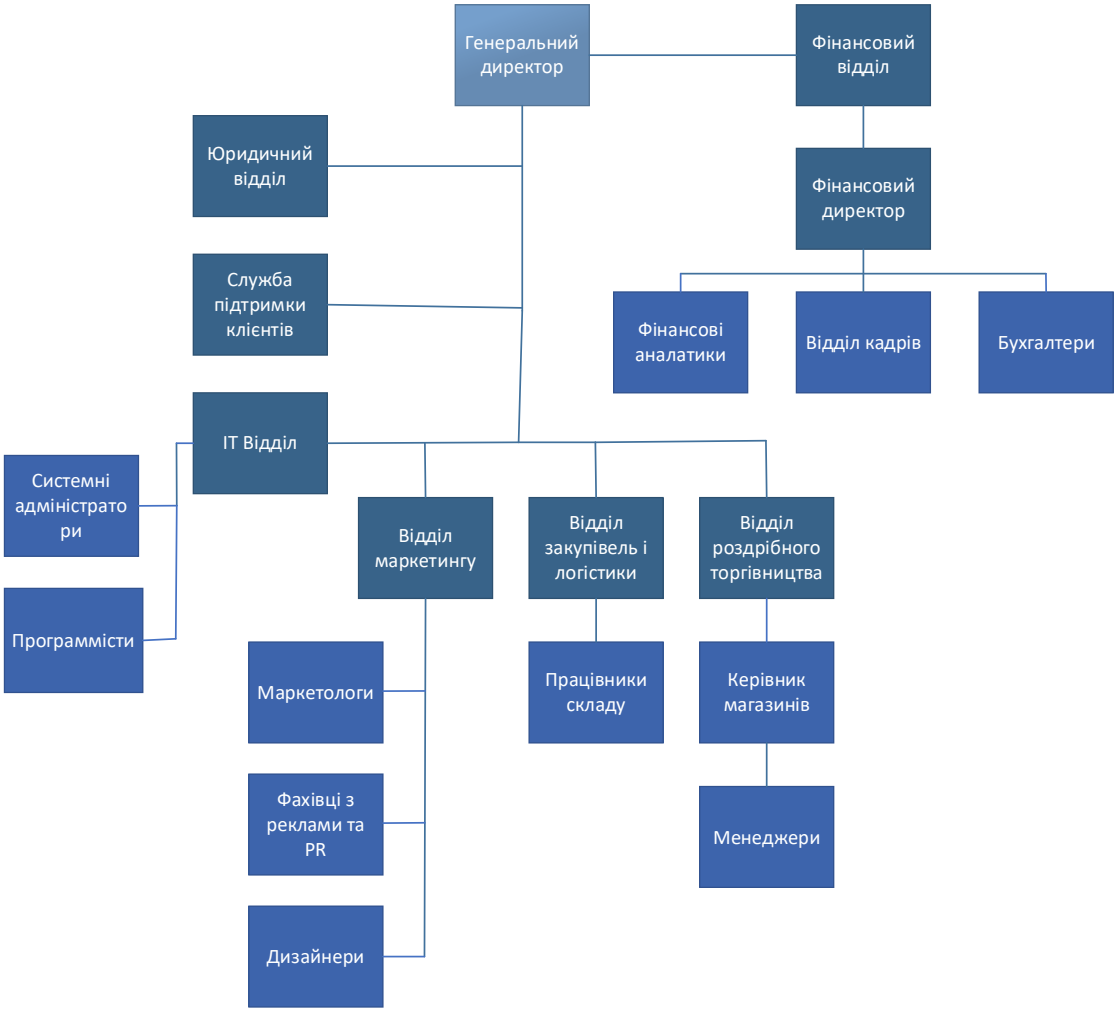


Рисунок 1.1 – Організаційна структура компанії

1.3 Відомості про топологічне розміщення структурних підрозділів

Корпоративна мережа підприємства організована за принципом централізованого об’єднання всіх структурних одиниць у спільне інформаційне середовище. Такий підхід забезпечує цілісність інфраструктури, спрощує адміністрування та сприяє ефективному керуванню цифровими потоками даних.

Локальні мережі, що функціонують на окремих об’єктах, утворюють логічно ізольовані сегменти, які, у свою чергу, інтегруються в загальну систему. Технологічною основою для побудови внутрішніх з’єднань виступає кабельна інфраструктура стандарту Ethernet, доповнена точками доступу Wi-Fi у зонах, що потребують мобільності – зокрема в адміністративних приміщеннях і сервісних ділянках.

Офісна й сервісна мережа компанії має географічно розподілену структуру: підрозділи розташовані у різних мікрорайонах міста Дніпро. Основні філії функціонують за адресами вул. Шевченка, 36 та проспект Науки, 8А (рис.1.2). Обидва об’єкти пов’язані з головним офісом через захищені канали передачі даних і синхронізовані в єдиному операційному середовищі.

Для оптимізації взаємодії між підрозділами реалізовано логічне сегментування мережі. Зокрема, виділені окремі підмережі для адміністративного персоналу, IT-сектору, роздрібних торговельних точок, підключених IoT-пристроїв та складських об’єктів. Така структура забезпечує ізоляцію критично важливих ресурсів, знижує ризики несанкціонованого доступу й дозволяє балансувати навантаження між сегментами з урахуванням специфіки роботи кожного з них.

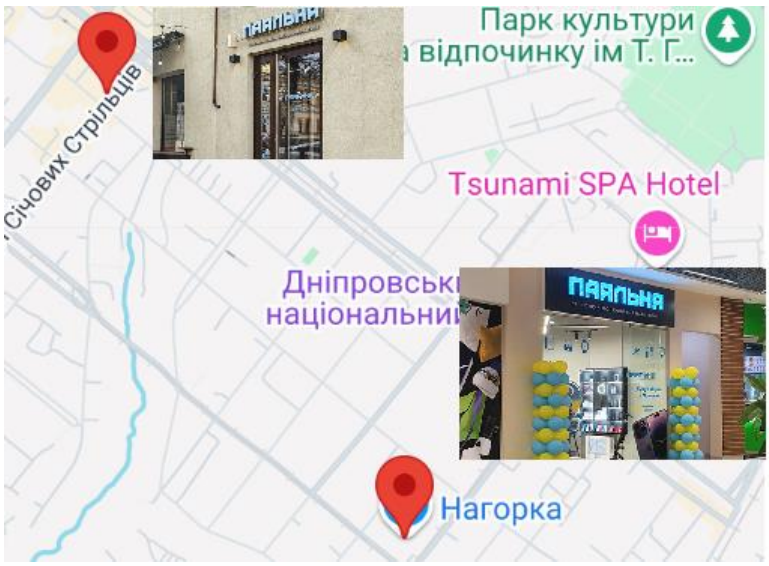


Рисунок 1.2 – Географічне розміщення філіалів компанії у місті Дніпро

На рисунках 1.3 та 1.4 представлено плани приміщень головного офісу компанії та філії компанії з виділенням торгової зони, складу та кімнати паяльника.

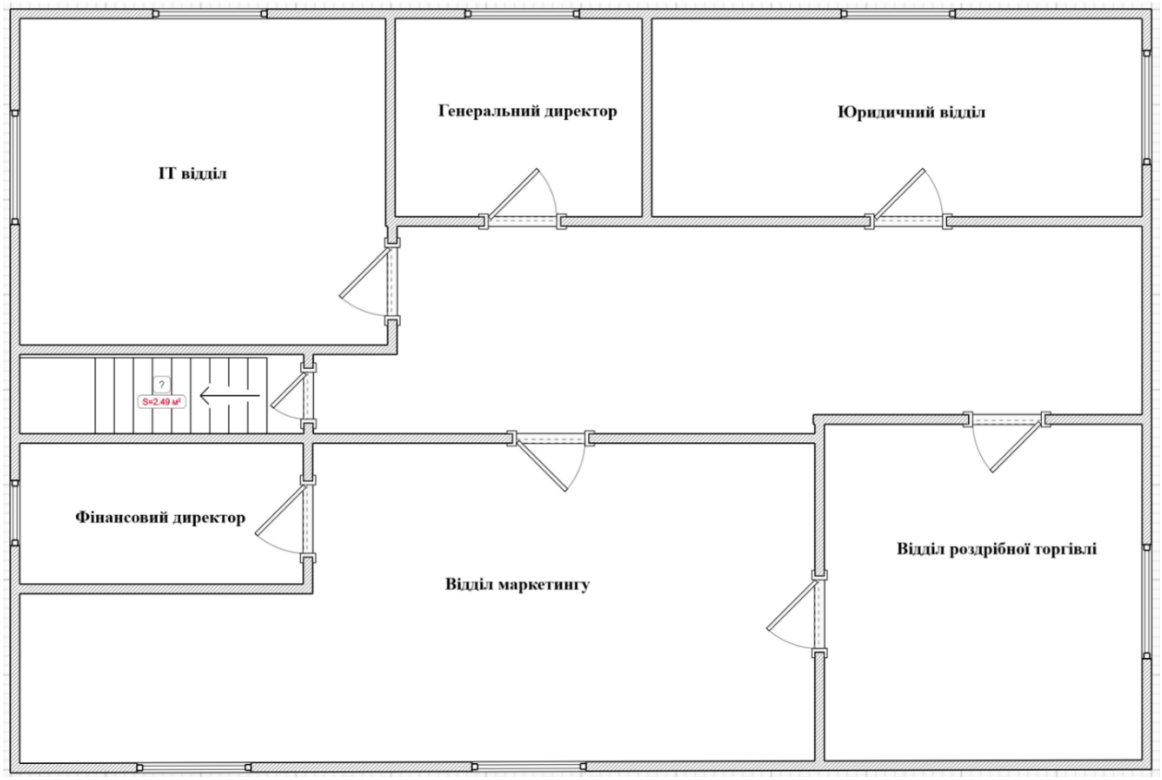


Рисунок 1.3 – План головного офісу компанії з розміщенням структурних підрозділів

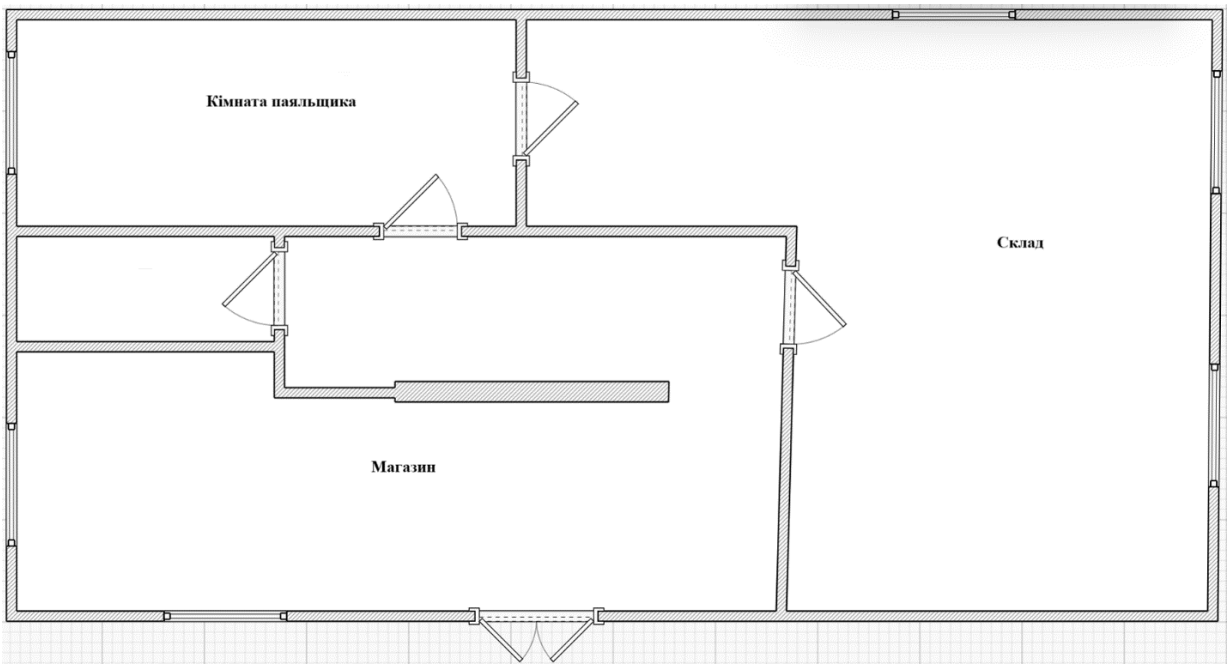


Рисунок 1.4 – План філії компанії з виділенням торгової зони, складу та кімнати паяльника

1.4 Принципи та технічні способи інформаційного забезпечення

Ключовим технічним рішенням виступає логічне сегментування мережі, яке дозволяє ізолювати трафік окремих функціональних зон, оптимізувати маршрутизацію даних і підвищити загальний рівень інформаційної безпеки. Такий підхід дає змогу обмежити доступ до критично важливих ресурсів та мінімізувати ризики витоку інформації.

Інфраструктура побудована з урахуванням подальшого розширення: використання модульного обладнання дозволяє оперативно масштабувати систему без необхідності глибокої реконфігурації. Нові пристрої та сервіси можуть бути інтегровані без переривання роботи діючої мережі, що забезпечує безперервність бізнес-процесів.

Технічне забезпечення охоплює як провідні Ethernet-з’єднання, так і точки бездротового доступу Wi-Fi. Це дозволяє створити стабільне покриття у всіх ключових зонах: адміністративних приміщеннях, сервісних ділянках, торгових залах і місцях взаємодії з клієнтами.

Централізована модель адміністрування гарантує узгоджений обмін інформацією між усіма компонентами мережі, включаючи філіали, головний офіс, серверне обладнання, IoT-пристрої та системи зберігання даних.

1.5 Визначення можливих напрямків рішення поставлених завдань

Для реалізації поставлених завдань одним із найбільш доцільних напрямків є впровадження мережевої інфраструктури з логічним сегментуванням інформаційного середовища. Такий підхід передбачає розподіл мережі на окремі підмережі для офісного обладнання, сервісних зон, пристроїв Інтернету речей та складських приміщень.

Можлива загальна схема архітектури підприємства з розташуванням філій в різних місцях через мережу провайдерів представлена на рисунку 1.5.

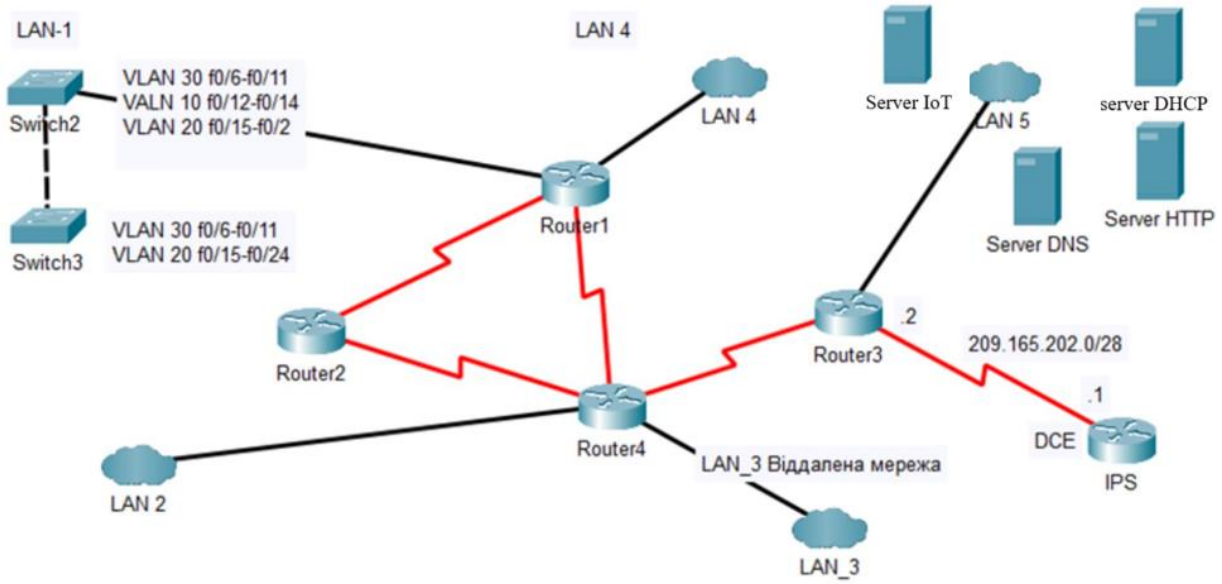


Рисунок 1.5 – Топологічна схема корпоративної мережі

Оцінювання працездатності архітектури можна здійснювати шляхом моделювання у середовищі Cisco Packet Tracer. Це дасть змогу візуалізувати побудовану систему, протестувати її функціональність у різних сценаріях і своєчасно виявити потенційні вузькі місця.

Також доцільним є використання механізмів VLAN (Virtual Local Area Network) для логічного розмежування функціональних зон та впровадження систем контролю доступу (ACL – Access Control List) з метою обмеження несанкціонованого доступу до критичних ресурсів. Систему адміністрування пропонується реалізувати у централізованому вигляді з можливістю моніторингу активності та швидкого реагування на інциденти.

Впровадження IoT-рішень передбачається здійснити на основі сенсорних пристроїв, здатних контролювати температуру, наявність диму та роботу витяжної вентиляції на паяльних робочих місцях. Отримані з них телеметричні дані надходитимуть до аналітичної підсистеми, що дозволить оперативно реагувати на відхилення від нормативних показників, підвищуючи безпеку персоналу та якість виконання ремонтних робіт.

1.6 Постановка завдання

Метою даної роботи є розроблення комп’ютерної системи, адаптованої до специфіки підприємства, що функціонує в галузях реалізації електроніки, сервісного обслуговування та впровадження IoT-рішень для контролю параметрів робочого середовища.

У межах проєкту передбачено формулювання технічних вимог до інформаційної інфраструктури компанії, проєктування локальних мереж, організацію каналів взаємодії між підрозділами, впровадження засобів кіберзахисту та інструментів для дистанційного адміністрування. Пріоритетним напрямом виступає забезпечення стійкої комунікації між філіями та центральним офісом, а також збір, обробка й зберігання даних з пристроїв Інтернету речей.

Для досягнення поставленої мети необхідно реалізувати такі завдання:

– визначити технічні вимоги до інфраструктури підприємства, з урахуванням потреб бізнесу та перспектив масштабування;

– спроєктувати топологію корпоративної мережі з логічною сегментацією функціональних зон;

– організувати канали безпечної взаємодії між географічно розподіленими структурними підрозділами;

– впровадити засоби захисту інформації, у тому числі механізми фільтрації трафіку та шифрування каналів зв’язку;

– забезпечити збір, обробку та зберігання телеметричних даних від пристроїв Інтернету речей, розміщених на робочих місцях сервісних інженерів;

– змоделювати запропоновану архітектуру за допомогою спеціалізованого програмного забезпечення Cisco Packet Tracer для перевірки її працездатності та визначення потенційних вузьких місць.

2 ФОРМУВАННЯ ВИМОГО І РОЗРОБКА ПАПРАТНОЇ ЧАСТИНИ КОМПЬЮТЕРНОЇ СИСТЕМИ КОМПАНІЇ

2.1 Технічні вимоги до КС компанії з продажу та сервісного обслуговування мобільних телефонів

2.1.1 Найменування і призначення КС компанії

Об’єктом професійної діяльності в межах даного проєкту є комп’ютерна система компанії, що здійснює роздрібний продаж і сервісне обслуговування мобільних телефонів, з особливим акцентом на впровадженні IoT-комплексу паяльного робочого місця та створенні надійної корпоративної мережі для обміну інформацією між підрозділами підприємства.

Комп’ютерна система виконує такі основні функції:

– підтримка централізованого зберігання й обміну інформацією між офісом і філіями;

– забезпечення роботи сервісного центру із засобами моніторингу стану мікроклімату;

– збір та передача телеметричних даних із сенсорів, встановлених у зоні пайки, з метою дотримання технологічних норм та гарантування безпечних умов праці;

– забезпечення контролю за станом мережі та обладнанням IT-інфраструктури через централізовану модель адміністрування.

Таким чином, об’єкт проєктування виконує роль комплексного цифрового середовища підприємства, що поєднує в собі засоби телеметрії, аналітики та комунікації між структурними підрозділами, спрямовані на підвищення ефективності бізнес-процесів і рівня технічної безпеки.

2.1.2 Перспективи розвитку КС

У майбутньому розроблена комп’ютерна система може бути розширена як у технічному, так і у функціональному аспектах. Архітектура побудована з урахуванням масштабованості – передбачено можливість додавання нових

сенсорних пристроїв, зон моніторингу, сервісів без необхідності кардинальної перебудови інфраструктури.

Одним з перспективних напрямів розвитку є створення мобільного застосунку для Android або iOS, який дозволятиме відповідальному персоналу в режимі реального часу відстежувати стан системи, отримувати сповіщення про зміни показників з датчиків (наприклад, задимленість, стан витяжки або вікон), а також переглядати історію подій. Це забезпечить більшу гнучкість в управлінні, зручність доступу до даних і підвищення оперативності реагування.

Крім того, можливе впровадження додаткових модулів моніторингу, таких як аналіз вологості повітря, рівня освітлення, наявності небезпечних газів або шумового навантаження. Це дозволить розширити систему до рівня повноцінного комплексу розумного середовища для робочих місць.

2.1.3 Вимоги до структури та функціонування системи

2.1.3.1 Технічні вимоги до корпоративної мережі компанії

Корпоративна мережа компанії повинна забезпечувати надійний, безпечний та масштабований обмін даними між головним офісом, філіями, сервісними центрами та IoT-пристроями на робочих місцях.

У межах розробки передбачено створення п’яти локальних підмереж (табл. 2.1), кожна з яких відповідає окремому структурному підрозділу підприємства. Кількість вузлів у кожній підсистемі визначено з урахуванням 10% резерву, що дає змогу підключати нові пристрої без зміни топології або повторного структурування адресного простору.

Усі сегменти інтегруються в єдину корпоративну мережу за допомогою маршрутизатора, що виконує функції міжмережевої маршрутизації, трансляції адрес (NAT).

Таблиця 2.1 – Вимоги до VLAN

№	Назва сегменту	Позначення	Основні функції та призначення	Кількість вузлів
1	Фінансовий відділ	LAN_1	Обробка фінансової інформації, бухгалтерський облік, бюджетування	54
2	Служба технічної підтримки	LAN_2	Обробка звернень клієнтів, підтримка користувачів, технічний супровід	96
3	Сервісний центр	LAN_3	Управління ремонтними роботами, облік замовлень, взаємодія з IoT-пристроями	86
4	Маркетинговий сегмент	LAN_4	Аналіз ринку, формування рекламних кампаній, управління маркетингом	27
5	IT-відділ	LAN_5	Адміністрування інформаційної інфраструктури, підтримка мережі та серверів	13

Інфраструктурні вимоги:

– використання стандарту Ethernet 1 Gbps для провідних з’єднань і сучасних точок доступу Wi-Fi 6 для бездротової мережі;

– побудова мережі за топологією з централізованим контролем і логічним сегментуванням (VLAN) для розмежування трафіку по табл. 2.1;

– мережева адресація на основі діапазону 10.24.40.0/21, кожна підмережа ізольована логічно та фізично, обслуговується окремим керованим комутатором;

– можливість масштабування інфраструктури з підтримкою додаткових вузлів і підмереж без перебоїв.

Інтеграція з IoT:

– підтримка протоколів передачі даних IoT-пристроїв у відповідних VLAN;

– забезпечення низької латентності і високої надійності передачі для телеметрії паяльних робочих місць;

– реалізація централізованої системи збору, обробки та аналізу IoT-даних із подальшою взаємодією з CRM та аналітичними платформами.

Взаємодія між підсистемами здійснюється через керовані комутатори та маршрутизатори. Інформаційний обмін відбувається через комбіновану модель з'єднань, яка включає дротову інфраструктуру на основі технології Ethernet, бездротові точки доступу Wi-Fi, та протоколи захищеної передачі даних (зокрема HTTPS та SSH).

Система має бути сумісною з хмарними платформами та програмним забезпеченням сторонніх виробників, зокрема CRM-системами, ERP-рішеннями, програмами бухгалтерського обліку (1С), електронного документообігу (M.E.Doc) тощо. Це дозволить інтегрувати інформаційні потоки з різних джерел в єдиний корпоративний простір.

Режим роботи системи визначається як безперервний (24/7), із забезпеченням постійного функціонування критичних сервісів. Для оперативного реагування на неполадки реалізується система автоматизованого моніторингу, журналювання подій та механізми сповіщення відповідальних адміністраторів у разі виявлення відхилень або збоїв у роботі.

Інфраструктура повинна підтримувати підключення нових філій, додаткових підсистем або IoT-пристроїв без потреби у суттєвій реконструкції. Передбачається технічна можливість оновлення серверного обладнання, модифікації топології мережі та розширення функціоналу шляхом впровадження нових технологій.

2.1.3.2 Технічні вимоги до робочого місця паяльника та IoT-системи

Робоче місце паяльника повинно бути оснащене комплексом апаратних та програмних засобів для забезпечення високої якості ремонтних робіт, моніторингу умов мікроклімату та інтеграції з корпоративною інформаційною системою.

Функціональні вимоги:

– забезпечення безпечних умов праці відповідно до санітарних і технологічних норм (ДСТУ, ДБН, ISO 45001);

– постійний контроль мікрокліматичних показників: температури, , наявності диму чи шкідливих газів;

– автоматизоване реагування на тривожні події (перегрів, задимлення) шляхом активації витяжної вентиляції, відкривання вікон, подачі звукових сигналів;

– збір і передача телеметричних даних у реальному часі для подальшого аналізу й зберігання в базі даних;

– відображення поточних параметрів на локальному або веб-інтерфейсі.

Апаратні вимоги:

– паяльна станція з цифровим управлінням температурою, що підтримує стандарти пайки сучасних мобільних телефонів;

– температурний датчик для контролю стану робочої зони;

– сенсор диму для виявлення потенційних небезпек;

– витяжна вентиляція з цифровим керуванням та моніторингом працездатності;

– мікроконтролер або шлюз IoT для збору та передачі телеметричних даних до центральної аналітичної системи;

– монітор або планшет із встановленим програмним забезпеченням для відображення та управління даними IoT.

Програмні вимоги:

– ПЗ для управління паяльною станцією з можливістю налаштування та збереження профілів пайки.

– система збору та обробки телеметричних даних у режимі реального часу з відображенням поточних показників мікроклімату.

– модуль інтеграції із корпоративною CRM-системою для фіксації ремонтних операцій та зв’язку з замовленнями.

– механізми оповіщення та аварійного повідомлення у випадку виходу параметрів за задані нормативи.

– функції історичного зберігання даних для подальшого аналізу та аудиту.

Інтеграційні вимоги:

– підключення до локальної мережі підприємства із забезпеченням безперервної передачі даних;

– підтримка стандартних протоколів IoT (HTTP) для сумісності з іншими системами;

– забезпечення кібербезпеки даних: шифрування переданих повідомлень, автентифікація пристроїв.

2.1.4 Показники призначення

Для забезпечення відповідності системи її функціональному призначенню встановлюються наступні експлуатаційні та якісні показники:

– час обробки запитів у локальній мережі – не повинен перевищувати 2–5 мс при типовому навантаженні, що забезпечує комфортну роботу з внутрішніми сервісами та мінімізує затримки в обміні даними між підсистемами;

– стабільність та здатність каналів зв’язкумає підтримуватись на рівні не нижче 1 Гбіт/с для внутрішньої мережі, з можливістю масштабування при зростанні навантаження;

– рівень доступності сервісів – не нижче 99.8% у середньому за рік, що відповідає сучасним вимогам до високодоступних інформаційних систем;

– маштабованість за кількістю пристроїв – система повинна стабільно підтримувати не менше 300 одночасно підключених користувацьких і мережевих пристроїв (ПК, смартфони, IoT-сенсори, точки доступу тощо).

Для забезпечення якісного контролю параметрів робочого середовища на робочому місці паяльника та в системі загалом, використовуються спеціалізовані технічні засоби контролю. Таблиця 2.2 містить перелік основних пристроїв, їх тип, характеристики інтерфейсів, швидкодію та функціональне призначення.

Таблиця 2.2 – Перелік та характеристика засобів контролю

Засіб контролю	Тип/ модель	Інтерфейс/ протокол	Швидкодія	Призначення
Температурний сенсор	Цифровий	UART/I2C	1 вимір/2 с	Контроль температури/вологості
Сенсор диму	Аналоговий	ADC	1 вимір/сек	Виявлення диму
Контролер вентиляції на базі реле	Електронний	GPIO/HTTP API	Затримка ≤ 100 мс	Управління витяжкою
Паяльна станція з цифровим контролем	Hakko FX-951	RS-232	Затримка ≤ 1с	Моніторинг температури жала
IoT-шлюз	Wi-Fi/BLE	HTTP	10–50 мс	Збір та передача сенсорних даних

Окремим компонентом виступає підсистема збору телеметрії, яка фіксує та передає дані з IoT-пристроїв (сенсорів температури, диму, вентиляції). Передача повинна здійснюватись із мінімальними затримками на центральний сервер, де інформація візуалізується для оперативного аналізу персоналом. За потреби – реалізується автоматичне інформування у разі виявлення відхилень від нормативних показників. Таблиця 2.3 містить параметри, що підлягають контролю в межах IoT-комплексу робочого місця паяльника, із зазначенням припустимих меж, точності та періодичності їх моніторингу, а також пріоритетності.

Таблиця 2.3 – Перелік та характеристика параметрів, що контролюються і регулюються

Параметр	Припустимі межі	Точність контролю	Періодичність контролю	Пріоритет
Температура повітря у зоні пайки	18–30 °C	±0,5 °C	кожні 10 секунд	Високий
Рівень диму в повітрі	≤ 5 ppm	±1 ppm	кожні 5 секунд	Високий

Продовження табл. 2.3.

Параметр	Припустимі межі	Точність контролю	Періодичність контролю	Пріоритет
Стан витяжної вентиляції	Вкл/Викл	–	кожні 10 секунд	Середній
Температура паяльного жала	280–380 °C	±2 °C	кожні 15 секунд	Високий

Система має підтримувати як одиночні умови, так і комбіновані сценарії спрацювання, що базуються на значеннях температурних сенсорів та сигналів тривоги з димових детекторів. Зокрема, розробити наступну логіку:

– у разі перевищення температури в приміщенні понад 30 °C або за наявності сигналу про дим у повітрі, система повинна автоматично відкрити вікна для природного охолодження приміщення;

– при досягненні температурою критичного значення понад 75 °C та одночасному спрацюванні датчика диму, запускається автоматична система пожежогасіння, а також активується звукове оповіщення персоналу через сигнал тривоги;

– якщо після небезпечного інциденту температура знижується до рівня нижче 50 °C і димовий детектор більше не фіксує диму, то система деактивує пожежогасіння та вимикає сирену, повертаючись до нормального режиму;

– у разі підвищення температури понад 35 °C, незалежно від інших параметрів, система повинна вмикати кондиціонер або витяжну вентиляцію для підтримання допустимих умов мікроклімату;

– якщо температура знижується нижче 28 °C і при цьому датчик диму не фіксує аномалій, система зобов’язана вимикати кондиціонер і зачиняти вікна, щоб знизити енерговитрати.

2.1.5 Логування та моніторинг системи

Для забезпечення своєчасного реагування на зміни параметрів середовища та подій у системі критично важливим є впровадження механізмів логування (журналювання подій) та моніторингу в реальному часі.

Усі ключові дії, включно зі спрацюванням сенсорів, активацією виконавчих пристроїв (витяжка, кондиціонер, сирена), а також змінами стану системи фіксуються у відповідному журналі на центральному сервері. Це дозволяє:

– відстежувати історію подій для аналізу інцидентів;

– виявляти відхилення у роботі пристроїв або затримки в спрацюванні;

– налагоджувати профілактичне обслуговування технічних засобів.

Моніторинг стану пристроїв реалізується через регулярні пінги, перевірку відповідей від сенсорів та передачу телеметрії через IoT-протокол TCP. При виявленні нештатної ситуації система може вивести сповіщення на диспетчерську панель, а в перспективі – надіслати повідомлення через email/SMS.

Для гнучкості аналізу журнал подій може містити такі поля: час події, тип пристрою, ID сенсора, значення параметра, спрацювання правила або сценарію, ID користувача (при ручному втручанні).

2.1.6 Вимоги до експлуатації, обслуговування та збереження

Інформаційна система розрахована на експлуатацію в стандартних офісних умовах із дотриманням наступних кліматичних параметрів (табл.2.4):

Таблиця 2.4 – Характеристика умов зовнішнього середовища

Розташування	Температурний режим	Вологість	Особливості
Серверна кімната	20–24 °C	30–50%	Примусова вентиляція, кондиціонування
Торгові зали	18–26 °C	35–55%	Висока прохідність, постійна робота терміналів
Майстерні/кімнати паяльників	18–28 °C	30–60%	Наявність диму, високі локальні температури
Складські приміщення	10–30 °C	20–60%	Необхідність захисту від пилу та вологи

Технічне обслуговування системи включає щомісячну перевірку працездатності обладнання, а також щоквартальні регламентні процедури: оновлення програмного забезпечення, створення резервних копій та тестування механізмів відновлення. Всі операції мають виконуватись кваліфікованим IT-персоналом у складі не менше двох спеціалістів, які володіють практичними навичками роботи з операційними системами Windows Server, мережевим обладнанням Cisco, службами Active Directory та базовими інструментами моніторингу.

Мережеве та серверне обладнання розміщується у спеціально облаштованих приміщеннях з обмеженим фізичним доступом, відповідно до вимог безпеки. Резервні одиниці (комутатори, маршрутизатори, IoT-сенсори тощо) мають зберігатися в готовності до оперативної заміни у разі відмови основного обладнання.

2.1.7 Організація навчання користувачів системи

Успішне впровадження корпоративної комп’ютерної системи та IoT-рішень неможливе без належного рівня підготовки персоналу, який працює з цією інфраструктурою. Для забезпечення ефективної експлуатації, а також дотримання вимог безпеки, передбачено організацію навчання користувачів на декількох рівнях.

Первинне навчання проводиться для всіх нових співробітників, що залучені до роботи з корпоративною мережею, ERP-системами, IoT-контролерами або інтерфейсами моніторингу. Під час навчання працівники ознайомлюються з інтерфейсами систем, правилами безпечного користування, інструкціями реагування на спрацювання аварійних сценаріїв (пожежа, перевищення температури, виявлення диму).

Періодичне навчання та перевірка знань організовуються не рідше одного разу на пів року. Воно включає оновлення інформації щодо нових функцій системи, зміни у протоколах безпеки, а також відпрацювання дій у

надзвичайних ситуаціях (наприклад, відключення обладнання при тривозі або активація резервного живлення).

Особлива увага приділяється персоналу філій, де встановлено IoT-комплекси. Навчання включає роботу з датчиками, розуміння логіки спрацювання сценаріїв (наприклад, відкривання вікон, пожежогасіння) та вміння взаємодіяти з локальними IoT-шлюзами.

Наявність підготовлених користувачів дозволяє мінімізувати людський фактор при експлуатації системи, скоротити час реагування на інциденти та підвищити загальну надійність роботи комп'ютерної інфраструктури підприємства.

2.2 Розробка апаратної частини

2.2.1 Розробка загальної архітектури мережі компанії

Для забезпечення ефективної та безпечної роботи інформаційної системи підприємства необхідно розробити масштабовану, надійну та безпечну архітектуру корпоративної мережі. Основна мета проєктування мережі компанії – створення інтегрованого інформаційного середовища, що об'єднує головний офіс, філії, сервісні центри і робочі місця паяльників з IoT-пристроями.

Основні завдання архітектури мережі:

– забезпечення високої швидкості та доступності інформаційних сервісів для всіх користувачів;

– логічне сегментування мережевого трафіку з метою підвищення рівня безпеки та оптимізації роботи мережі;

– надійне інтегрування IoT-пристроїв у загальну інфраструктуру без погіршення продуктивності;

– забезпечення централізованого адміністрування та моніторингу мережі;

– підтримка масштабування мережі з можливістю безперебійного додавання нових підрозділів або сервісів.

2.2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Загальна топологія корпоративної мережі (рис. 2.1) реалізована за трирівневою моделлю, що включає ядро, рівень доступу та рівень хостів. Така структура забезпечує централізоване управління, масштабованість і підвищену відмовостійкість.

Рівень ядра (Core Layer) представлений маршрутизаторами R0, R1, R2, R3, які виконують функції міжмережевої маршрутизації та побудови внутрішнього хребта мережі. Для зв'язку між центральним офісом і філіями використано серійні канали WAN-з'єднання (позначені червоним кольором), що забезпечують гарантовану пропускну здатність і резервованість.

Рівень доступу (Distribution Layer) складається з керованих комутаторів SW0–SW6, що забезпечують логічне сегментування мережі за допомогою VLAN, а також виконують функції агрегації трафіку і реалізації політик доступу (ACL). Комутатори об'єднують підмережі LAN_1 (Фінанси), LAN_2 (Техпідтримка), LAN_3 (Сервіс), LAN_4 (Маркетинг), LAN_5 (IT) та адміністративну мережу AdminNet.

Рівень хостів (Access Layer) включає кінцеві пристрої користувачів, серверне обладнання та IoT-сенсори. Всі клієнтські пристрої під'єднані до відповідних портів комутаторів доступу, а IoT-шлюзи, що обслуговують паяльні робочі місця, під'єднані до VLAN сервісного центру (LAN_3). Зібрані з сенсорів дані передаються через IoT TCP-протокол до центрального сервера в LAN_5.

Крім логічної структури, система охоплює такі ключові елементи:

– серверна кімната, у якій розміщено базу даних, CRM-систему, ERP та інші критичні сервіси;

– точки Wi-Fi доступу, встановлені в адміністративних та сервісних зонах для покриття мобільних потреб персоналу;

Технічна основа системи, що включає:

– серверне обладнання з підтримкою віртуалізації та UPS;

– керовані комутатори та маршрутизатори з підтримкою VLAN, QoS, PoE;

– IoT-сенсори температури, диму;

– клієнтські пристрої – ПК, ноутбуки;

– допоміжне обладнання: точки Wi-Fi, джерела резервного живлення (UPS), відеокамери (за потреби).

Детальна IoT-топологія робочого місця паяльника передбачає:

– підключення сенсорів до шлюзу через дротовий або бездротовий інтерфейс;

– передачу даних до локального комутатора VLAN_3;

– централізовану передачу інформації до серверної частини через IoT TCP.

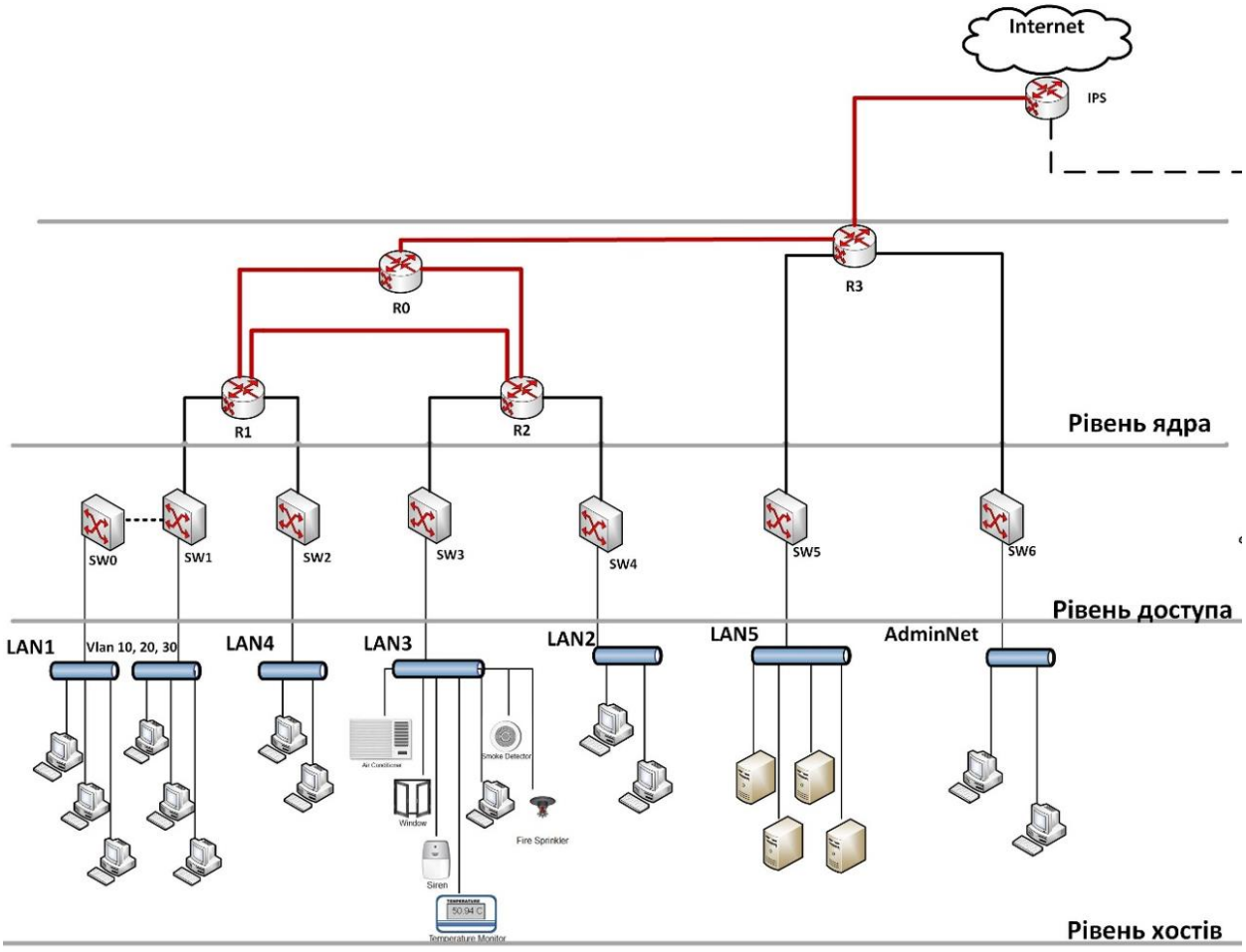


Рисунок 2.1 – Структурна схема комплексу технічних засобів системи

2.2.3 Розробка специфікації апаратних засобів комп'ютерної системи

Для забезпечення стабільного функціонування мережевої інфраструктури компанії, у тому числі її кіберфізичних компонентів, запропоновано використання високонадійного мережевого обладнання, здатного забезпечити високу пропускну здатність, масштабованість та належний рівень безпеки.

В основу побудови системи покладено маршрутизатор Cisco 2911, який належить до серії ISR (Integrated Services Router) другого покоління. Пристрій має три вбудовані гігабітні Ethernet-порти, слоти для розширення інтерфейсів, а також підтримує апаратне прискорення обробки трафіку.

Маршрутизатор забезпечує пропускну здатність до 350 Мбіт/с без додаткових сервісів, та адаптований для роботи з NAT, ACL, що дозволяє ефективно інтегрувати його в корпоративну мережу.

Вибір даної моделі обґрунтований потребами у гнучкому конфігуруванні, розширюваності та стабільності при цілодобовій експлуатації в умовах середнього навантаження.

У ролі комутаторів застосовується модель Cisco Catalyst 2960-24TT, яка має 24 порти Fast Ethernet та підтримує ключові мережеві технології, зокрема VLAN (логічне сегментування), QoS (пріоритетизація трафіку), STP (запобігання петлям у мережі) та ACL (контроль доступу). Такі можливості забезпечують високу керованість трафіком, розширюють функціонал адміністрування та підвищують загальну інформаційну безпеку.

Обрана апаратура дозволяє сформувати модульну, масштабовану архітектуру з централізованим управлінням і можливістю інтеграції нових підрозділів або підсистем у разі розширення компанії. Усі технічні характеристики устаткування відповідають потребам щодо підтримки кіберфізичних систем, включаючи підключення IoT-пристроїв.

Таблиця 2.5 – Специфікація обладнання

Позиція	Найменування	Тип, марка, позначення документа	Одиниці виміру	Кількість
1	Cisco 2911	Skoropad_R0 Skoropad_R1 Skoropad_R2 Skoropad_R3 Skoropad_R4	Од.	5
2	Cisco 2960	Skoropad_SW1 Skoropad_SW2 Skoropad_SW3 Skoropad_SW4 Skoropad_SW5 Skoropad_SW6	Од.	6
3	DLC100	Home Gateway	Од.	1
4	Cable Modem PT	Modem	Од.	1
5	Fire Sprinkler	Sprinkler	Од.	1
6	Smoke Detector	SDetector	Од.	1
7	Window	Window	Од.	1
8	Siren	Siren	Од.	1
9	Temperature monitor	Tmonitor	Од.	1
10	Air conditioner	Conditioner	Од.	1

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розробка логічної топології мережі

Логічна топологія корпоративної мережі підприємства побудована з урахуванням потреб у надійній взаємодії між структурними підрозділами, централізованому доступі до IT-ресурсів та забезпеченні безпечного виходу до глобальної мережі Інтернет.

Архітектура мережі включає п’ять окремих локальних підмереж LAN, які відповідають функціональним зонам компанії (адміністративний відділ, технічна підтримка, сервісний центр, склад, бухгалтерія). Додатково передбачено окрему адміністративну підмережу AdminLAN, яка використовується для управління інфраструктурою та має підвищений рівень захисту.

Для розмежування трафіку між підрозділами впроваджено логічне сегментування за допомогою технології VLAN, що дозволяє забезпечити гнучкість у налаштуванні політик доступу та оптимізацію маршрутизації трафіку.

Взаємодія між географічно рознесеними вузлами компанії організована через WAN-з’єднання, побудовані на основі каналів зв’язку між маршрутизаторами серії Cisco 2911. Для забезпечення ефективної маршрутизації в межах корпоративної мережі використовується протокол OSPF, що працює на третьому рівні моделі OSI. Такий підхід забезпечує швидку конвергенцію маршрутизаторів, автоматичну актуалізацію таблиць маршрутизації та підтримку масштабованої архітектури.

Для виходу користувачів у глобальну мережу Інтернет передбачено окремий канал зв’язку, реалізований через граничний маршрутизатор Skoropad_R4 ISP з використанням механізму трансляції мережевих адрес NAT, що дозволяє оптимізувати використання публічних IP-адрес та захистити внутрішню інфраструктуру.

Структуру побудованої мережі наведено на рисунку 3.1.

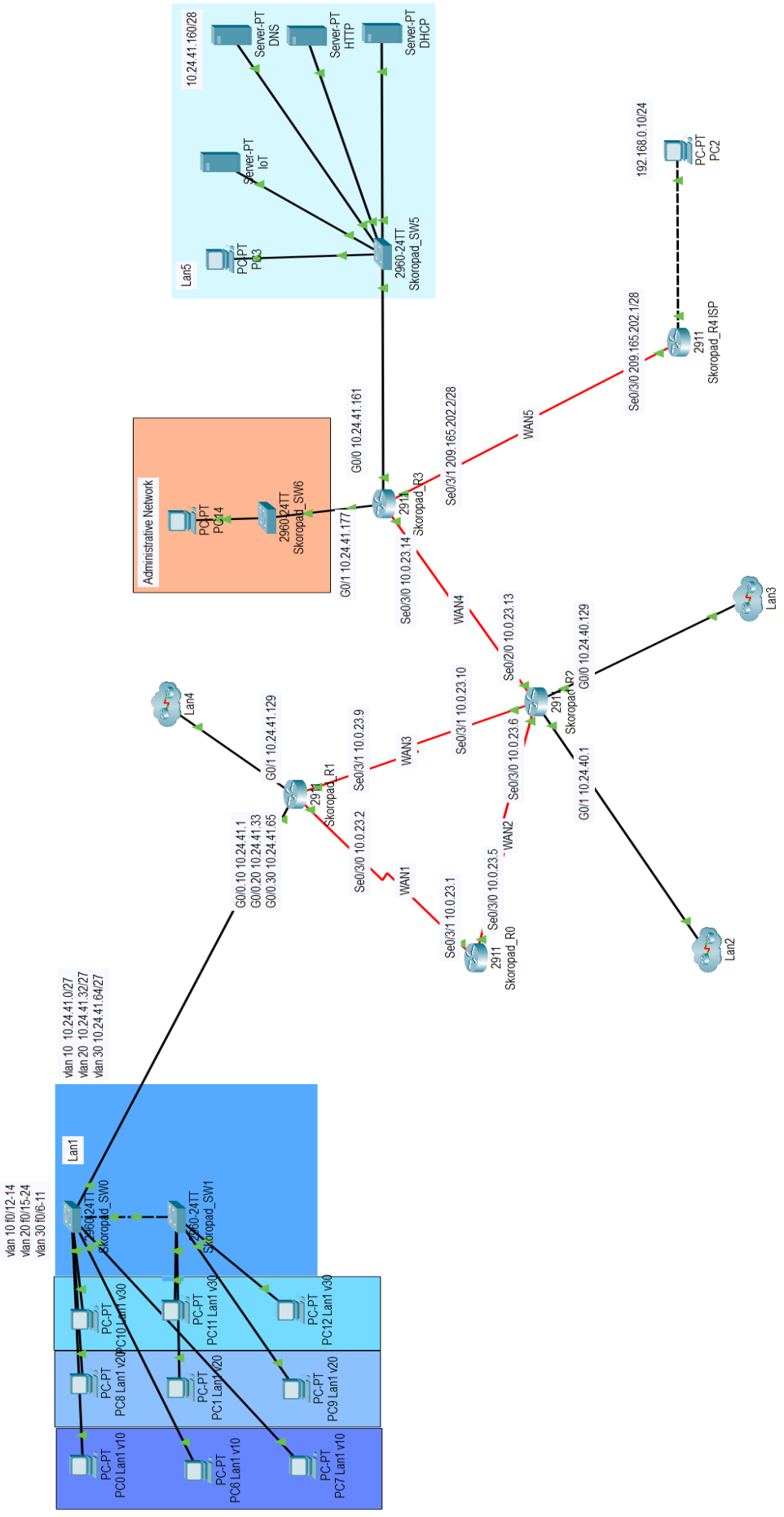


Рисунок 3.1 – Логічна схема корпоративної мережі

3.2 Розрахунок схеми адресації корпоративної мереж

Для побудови корпоративної мережі використано метод VLSM (Variable Length Subnet Masking), що дозволяє оптимально розподілити IP-адресний простір відповідно до кількості вузлів у кожній підмережі.

У таблиці 3.1 наведено розподіл адресного простору між підмережами.

Таблиця 3.1 – Схема адресації мережі

Назва підмережі	Необхідна кількість вузлів	Адреса підмережі	Маска підмережі	Діапазон допустимих ip-адрес
Lan1	54	10.24.41.0	/25	10.24.41.1- 10.24.41.126
Lan2	96	10.24.40.0	/25	10.24.40.1 - 10.24.40.126
Lan3	86	10.24.40.128	/25	10.24.40.129 - 10.24.40.254
Lan4	27	10.24.41.128	/27	10.24.41.129 - 10.24.41.158
Lan5	13	10.24.41.160	/28	10.24.41.161 - 10.24.41.174
AdminLan	13	10.24.41.176	/28	10.24.41.177 - 10.24.41.190

Для організації зв’язку між маршрутизаторами виділено окремий WAN-адресний блок. Схема адресації WAN-з’єднань наведена у таблиці 3.2. У таблиці 3.3 представлено адресацію інтерфейсів маршрутизаторів.

Таблиця 3.2 – Схема адресації каналів між маршрутизаторами.

Назва підмережі	Адреса підмережі	Маска	Призначення
Wan1	10.0.23.0 /30	255.255.255.252	R0 і R1
Wan 2	10.0.23.4 /30	255.255.255.252	R1 і R2
Wan 3	10.0.23.8 /30	255.255.255.252	R2 і R3
Wan 4	10.0.23.12 /30	255.255.255.252	R3 і R4
Wan5	209.165.202.0 /28	255.255.255.240	R4 і ISP

Таблиця 3.3 – Схема адресації інтерфейсів маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска
Skoropad_R0	Se0/3/1	10.0.23.1	255.255.255.252
	Se0/3/0	10.0.23.5	255.255.255.252
Skoropad_R1	Se0/3/0	10.0.23.2	255.255.255.252

Продовження табл. 3.3.

Пристрій	Інтерфейс	IP-адреса	Маска
Skoropad_R1	Se0/3/1	10.0.23.9	255.255.255.252
	G0/0	VLAN	VLAN
	G0/1	10.24.41.129	255.255.255.224
Skoropad_R2	Se0/3/0	10.0.23.6	255.255.255.252
	Se0/2/0	10.0.23.13	255.255.255.252
	G0/0	10.24.40.1	255.255.255.128
	G0/1	10.24.40.129	255.255.255.128
Skoropad_R3	Se0/3/0	10.0.23.14	255.255.255.252
	Se0/3/1	10.0.23.17	255.255.255.252
	G0/0	10.24.41.129	255.255.255.240
	G0/1	10.24.41.177	255.255.255.240
Skoropad_R4	Se0/3/0	209.165.202.1	255.255.255.240

3.3 Базове налаштування та захист доступу

На маршрутизаторах корпоративної мережі попередньо виконується базове налаштування, що включає визначення імені пристрою, налаштування банера вітання, задання доменного імені, а також конфігурацію захищеного віддаленого доступу за допомогою протоколу SSH. Додатково для забезпечення безпеки привілейованого режиму та доступу до глобального режиму конфігурації встановлюється зашифрований пароль. Для шифрування всіх паролів використовується команда service password-encryption.

Крім того, для адміністративного доступу налаштовано окрему підмережу AdminLAN. На інтерфейсі GigabitEthernet0/1 маршрутизатора Skoropad_R3 застосовано розширений список контролю доступу (ACL AdminNet) з забороною несанкціонованого доступу до адміністративної мережі, а також увімкнено інспекцію трафіку (AdminNetIn-Out) для контролю допустимих сесій. Повна конфігурація маршрутизатора із відповідними командами наведена у Додатку А**.**

Для підтвердження коректної роботи ізоляції підмережі AdminLAN було проведено тестування. На рисунку 3.2 продемонстровано результат перевірки: при спробі здійснити ICMP-запити (png) з хоста у LAN1 до вузла в AdminLAN

– запити були заблоковані. Натомість, при зворотній перевірці – з хоста AdminLAN до вузлів LAN1 – з'єднання встановлюється успішно, що відповідає вимогам конфігурації політик доступу.

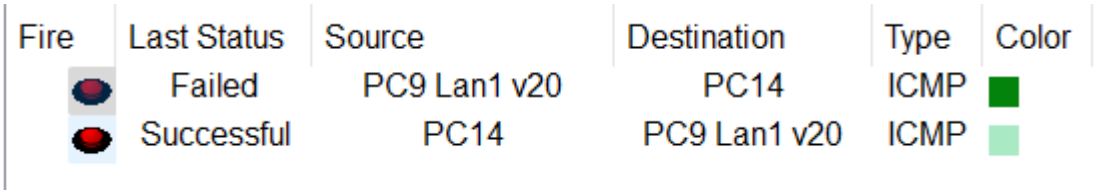


Рисунок 3.2 – Перевірка ізоляції підмережі AdminLAN

3.4 Вибір та налаштування способу маршрутизації

У корпоративній мережі підприємства для організації динамічної маршрутизації було обрано протокол OSPF. Його використання дозволяє ефективно управляти маршрутизацією в середовищі з багатьма підмережами, забезпечуючи швидке зрушення маршрутів у разі зміни топології, а також високу масштабованість. На відміну від протоколів із вектором відстані, OSPF працює на основі стану каналу та підтримує поділ мережі на області areas, що особливо зручно для даної структури корпоративної мережі.

Приклад налаштування OSPF на маршрутизаторі Skoropad_R3:

```
router ospf 1
router-id 4.4.4.4
network 10.0.23.12 0.0.0.3 area 0
network 10.24.41.160 0.0.0.15 area 0
passive-interface g 0/0
passive-interface g 0/1
```

Для організації доступу до глобальної мережі Інтернет на маршрутизаторі Skoropad_R3 було додано статичний маршрут за замовчуванням через зовнішній шлюз. На рисунку 3.3 також представлено таблицю маршрутизації, сформовану протоколом OSPF.

```
Skoropad_R3#sh 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 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 15 subnets, 5 masks
O       10.0.23.0/30 [110/192] via 10.0.23.13, 00:39:52, Serial0/3/0
O       10.0.23.4/30 [110/128] via 10.0.23.13, 00:39:52, Serial0/3/0
O       10.0.23.8/30 [110/128] via 10.0.23.13, 00:39:52, Serial0/3/0
C       10.0.23.12/30 is directly connected, Serial0/3/0
L       10.0.23.14/32 is directly connected, Serial0/3/0
O       10.24.40.0/25 [110/65] via 10.0.23.13, 00:39:52, Serial0/3/0
O       10.24.40.128/25 [110/65] via 10.0.23.13, 00:39:52, Serial0/3/0
O       10.24.41.0/27 [110/129] via 10.0.23.13, 00:39:52, Serial0/3/0
O       10.24.41.32/27 [110/129] via 10.0.23.13, 00:39:52, Serial0/3/0
O       10.24.41.64/27 [110/129] via 10.0.23.13, 00:39:52, Serial0/3/0
O       10.24.41.128/27 [110/129] via 10.0.23.13, 00:39:52, Serial0/3/0
C       10.24.41.160/28 is directly connected, GigabitEthernet0/0
L       10.24.41.161/32 is directly connected, GigabitEthernet0/0
C       10.24.41.176/28 is directly connected, GigabitEthernet0/1
L       10.24.41.177/32 is directly connected, GigabitEthernet0/1
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/28 is directly connected, Serial0/3/1
L       209.165.202.2/32 is directly connected, Serial0/3/1
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 3.3 – Таблиця маршрутизації на Skoropad_R3

3.5 Налаштування маршрутизаторів та серверів мережі

Для автоматичної видачі IP-адрес хостам мережі на сервері, розміщеному у підмережі LAN5 (10.24.41.160 /28), було налаштовано DHCP-сервер. Це дозволяє значно спростити адміністрування клієнтських пристроїв і мінімізувати помилки при ручному налаштуванні IP-параметрів.

На сервері створено окремі DHCP-пули для кожної VLAN/підмережі. Для кожного пулу визначено діапазон IP-адрес, шлюз за замовчуванням (default gateway), маску підмережі та параметри DNS (рис.3.4).

У кожному DHCP-пулі було зарезервовано перші 10 IP-адрес для потреб статичної конфігурації мережевих пристроїв та сервісів. Для перевірки коректної роботи DHCP-сервісу на одному з комп’ютерів у мережі LAN1 було змінено режим налаштування IP-адреси на автоматичний DHCP (рис. 3.5). У

результаті перевірки пристрій успішно отримав IP-адресу із відповідного пулу, що підтверджує правильність налаштування DHCP-сервера.

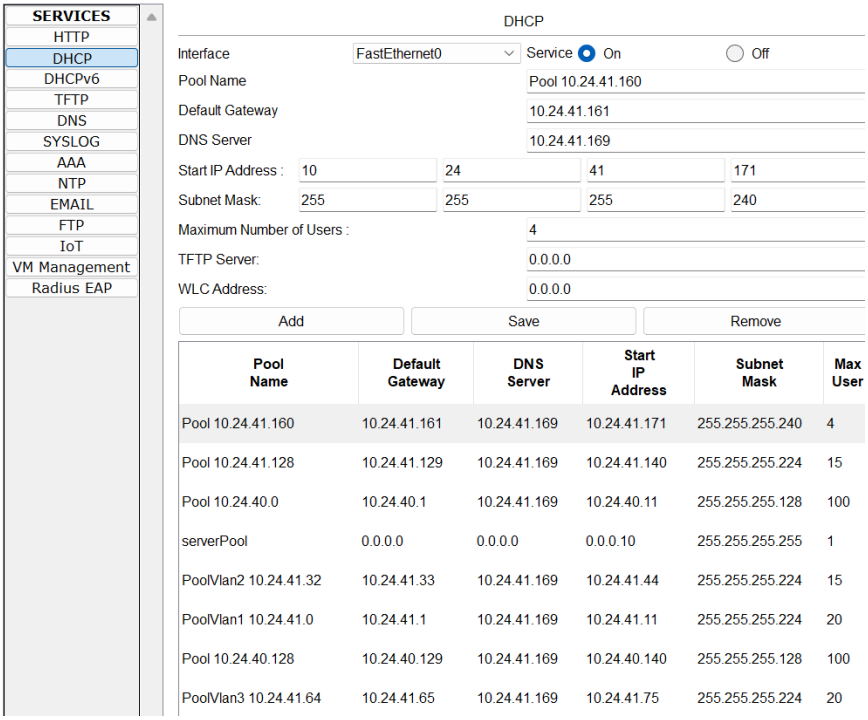


Рисунок 3.4 – Налаштування DHCP–сервера

Рисунок 3.5 – Перевірка отримання IP-адреси за DHCP на комп’ютері мережі LAN1

Для організації веб-сервісів було розгорнуто HTTP-сервер (рис. 3.6). Він використовується для розміщення корпоративних веб-додатків та сервісів, що забезпечують взаємодію між підрозділами компанії. На сервері активовано HTTP-службу на стандартному порту (TCP 80), а також налаштовано доступ до веб-ресурсів з усіх підмереж.

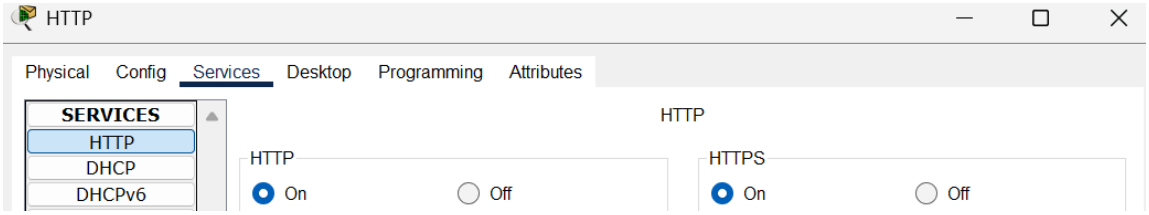


Рисунок 3.6 – Активуємо службу-http

Для забезпечення коректного функціонування доменних імен у корпоративній мережі розгорнуто DNS-сервер (рис. 3.7):

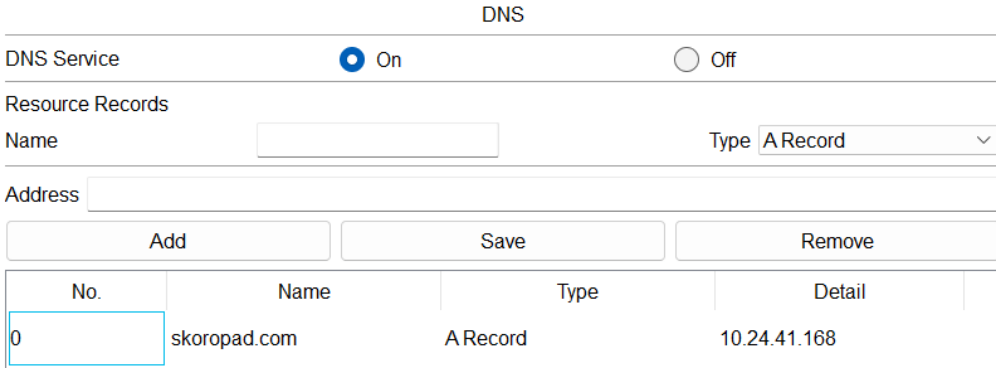


Рисунок 3.7 – Додавання запису в службу-dns

Для перевірки коректної роботи служб DNS та HTTP було виконано доступ до корпоративного веб-сайту за доменним іменем skoropad.com. У результаті запит було успішно оброблено, і веб-ресурс відобразився у браузері, що підтверджує правильність роботи як DNS-сервера, так і HTTP-сервера.

Результати перевірки наведено на рисунку 3.8.

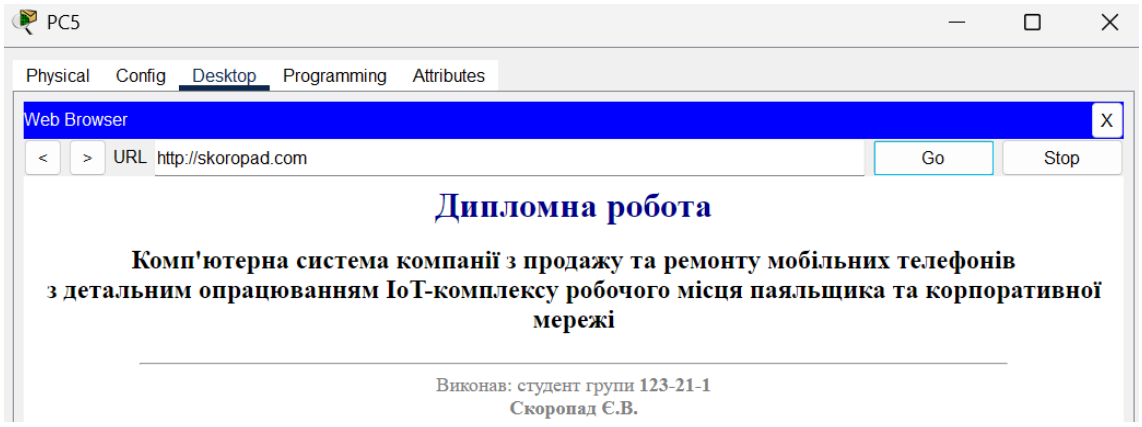


Рисунок 3.8 – Робота HTTP та DNS серверів

3.5.2 Налаштування роботи Інтернет

Для організації виходу користувачів корпоративної мережі до глобальної мережі Інтернет на маршрутизаторі Skoropad_R3 реалізовано трансляцію мережевих адрес (NAT). Це дозволяє внутрішнім приватним IP-адресам здійснювати доступ до Інтернет-ресурсів за допомогою публічної IP-адреси, виділеної провайдером.

У конфігурації застосовано комбінований підхід: використано як динамічну трансляцію NAT pool для підмереж LAN, так і статичну трансляцію для публікації внутрішнього HTTP-сервера у глобальній мережі.

Для забезпечення коректної маршрутизації у глобальну мережу було налаштовано статичний маршрут за замовчуванням через зовнішній шлюз провайдера.

В якості внутрішніх inside та зовнішніх outside інтерфейсів для NAT визначено відповідні інтерфейси маршрутизатора Skoropad_R3.

Повна конфігурація NAT наведена у Додатку А.

Для перевірки коректної роботи динамічного NAT було здійснено вихідний трафік з комп'ютера мережі LAN1 до ресурсів глобальної мережі Інтернет. Як видно з рисунка 3.9, під час передачі пакетів внутрішня приватна IP-адреса коректно транслюється у публічну IP-адресу провайдера.

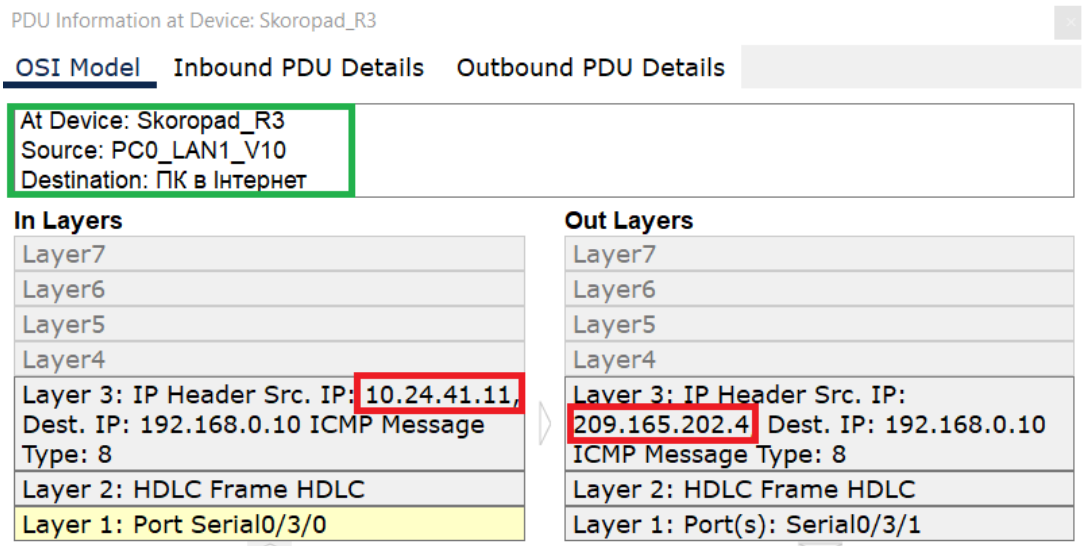


Рисунок 3.9 – Трансляція IP-адреси при виході трафіку з мережі в Інтернет

Додатково для моніторингу активних трансляцій було виконано команду show ip nat translations, результат якої наведено на рисунку 3.10. Таблиця трансляцій підтверджує правильність функціонування механізму динамічного NAT.

```
Skoropad_R3#sh ip nat tr
Skoropad_R3#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.202.3:3   10.24.41.76:3      192.168.0.10:3     192.168.0.10:3
icmp 209.165.202.4:1   10.24.41.11:1      192.168.0.10:1     192.168.0.10:1
icmp 209.165.202.4:2   10.24.41.11:2      192.168.0.10:2     192.168.0.10:2
---  209.165.200.4     10.24.41.168       ---                ---
```

Рисунок 3.10 – Вивід таблиці трансляцій NAT

Для перевірки роботи статичного NAT було здійснено підключення з хосту у глобальній мережі Інтернет до внутрішнього HTTP-сервера за публічною IP-адресою, призначеною статичним NAT. Як показано на рисунку 3.11, веб-сайт успішно завантажився у браузері, що підтверджує коректність налаштувань статичної трансляції.

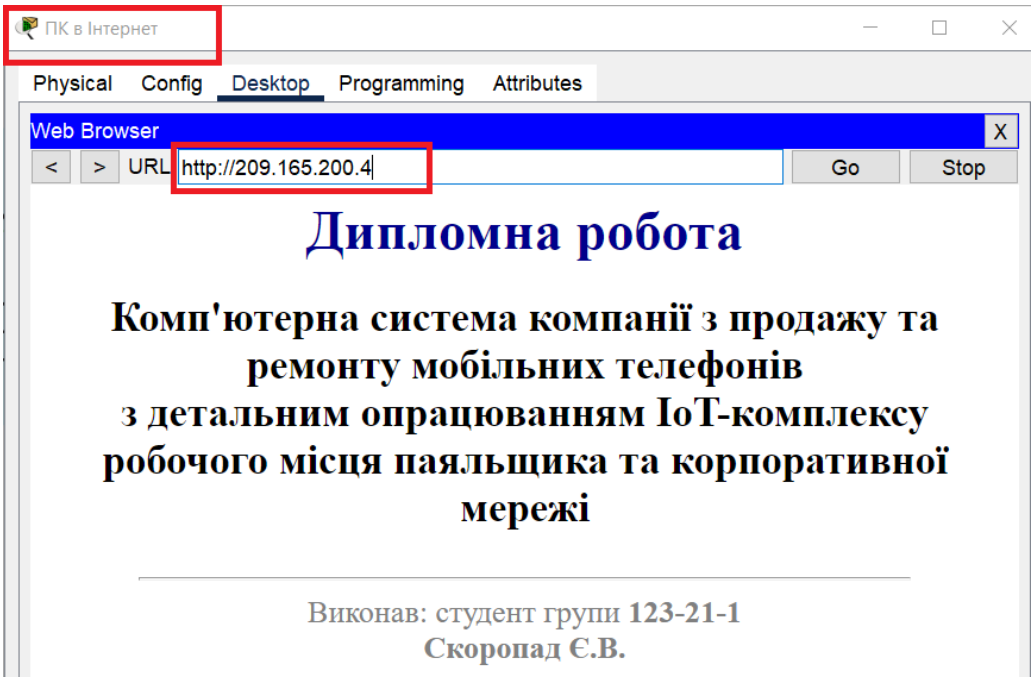


Рисунок 3.11 – Перевірка роботи статичного NAT для доступу до HTTP-сервера з Інтернету

3.5.3 Налаштування мереж VLAN, маршрутизації між VLAN

Для підвищення ефективності управління мережею та забезпечення її безпеки у корпоративній мережі було впроваджено технологію віртуальних локальних мереж. Це дозволило логічно розділити мережу Lan1 на окремі сегменти відповідно до функціональних підрозділів підприємства.

Використання VLAN забезпечує ізоляцію трафіку між різними групами користувачів без необхідності фізичного розділення мережевої інфраструктури, що спрощує адміністрування та підвищує загальний рівень захищеності.

У мережі було створено три підмережі, які відповідають функціональним підрозділам підприємства. Адресація цих VLAN представлена у таблиці 3.4.

Таблиця 3.4 – Адресація мереж VLAN

Назва	Мережева адреса	Маска	Діапазон використання
10	10.24.41.0	/27	10.24.41.1 - 10.24.41.30
20	10.24.41.32	/27	10.24.41.33 - 10.24.41.62
30	10.24.41.64	/27	10.24.41.65 - 10.24.41.94

Рисунок 3.12 демонструє план розміщення хостів у мережі із логічним розбиттям.

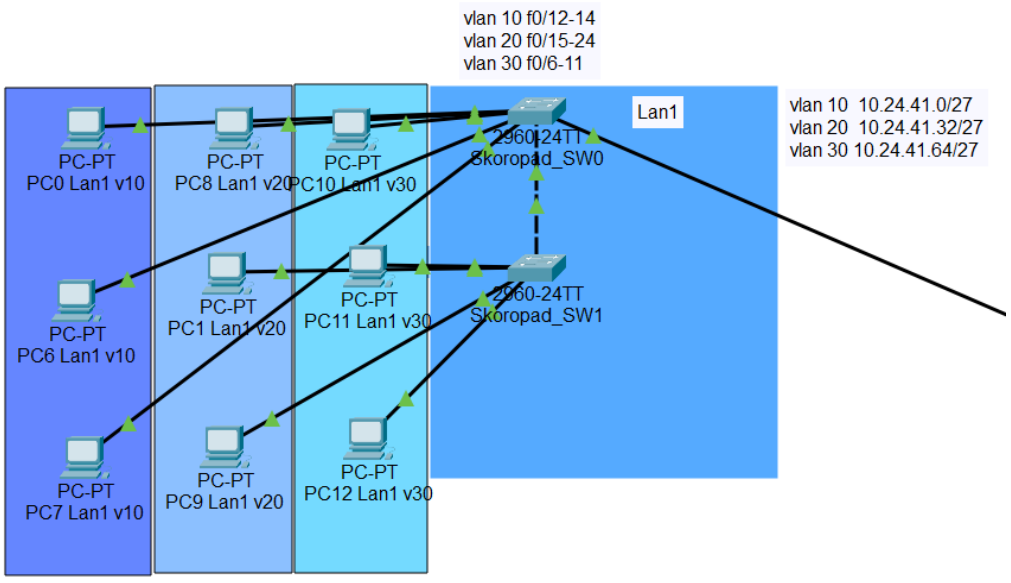


Рисунок 3.12 – План розміщення хостів у LAN1 та логічне розбиття на VLAN

Створення VLAN та налаштування портів було виконано на комутаторах Skoropad_SW0-1. Для візуального підтвердження стану VLAN використано команду show vlan brief, результати якої наведено на рисунку 3.13.

```
Skoropad_SW0#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Gig0/1, Gig0/2
10   Marketers                        active    Fa0/12, Fa0/13, Fa0/14
20   PR                               active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23
30   Designers                        active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 3.13 – Стан VLAN на комутаторах Skoropad_SW0-1

Приклад створення VLAN та налаштування портів у режимі access та trunk:

```
vlan 10
 name Marketers
vlan 20
 name PR
vlan 30
 name Designers

interface range FastEthernet0/12 - 14
 switchport mode access
 switchport access vlan 10

interface range FastEthernet0/15 - 23
 switchport mode access
 switchport access vlan 20

interface range FastEthernet0/6 - 11
 switchport mode access
 switchport access vlan 30

interface FastEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30
```

```
interface FastEthernet0/24
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30
```

Для забезпечення маршрутизації між VLAN на маршрутизаторі Skoropad_R1 були налаштовані підінтерфейси на інтерфейсі GigabitEthernet0/0 із використанням протоколу 802.1Q. Кожен підінтерфейс виконує роль шлюзу для відповідної VLAN.

На рисунку 3.14 показано налаштування підінтерфейсів на маршрутизаторі Skoropad_R1.

```
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 10.24.41.1 255.255.255.224
 ip helper-address 10.24.41.170
 ip access-group AdminNetVlan10 in
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 10.24.41.33 255.255.255.224
 ip helper-address 10.24.41.170
 ip access-group AdminNetVlan20 in
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 10.24.41.65 255.255.255.224
 ip helper-address 10.24.41.170
 ip access-group AdminNetVlan30 in
```

Рисунок 3.14 – Налаштування підінтерфейсів VLAN на маршрутизаторі Skoropad_R1

Для забезпечення ізоляції між VLAN та обмеження небажаного трафіку були налаштовані розширені списки контролю доступу. Завданням цих ACL є блокування прямого обміну трафіком між користувацькими VLAN, при цьому зберігається доступ до загальних корпоративних сервісів (наприклад, DHCP, DNS, HTTP).

Для підтвердження працездатності служби автоматичної адресації у кожній VLAN хости були переведені у режим автоматичного отримання IP-адрес через DHCP. Як показано на рисунку 3.15 – 3.17, комп'ютери успішно отримали IP-адреси з відповідного діапазону своєї підмережі.

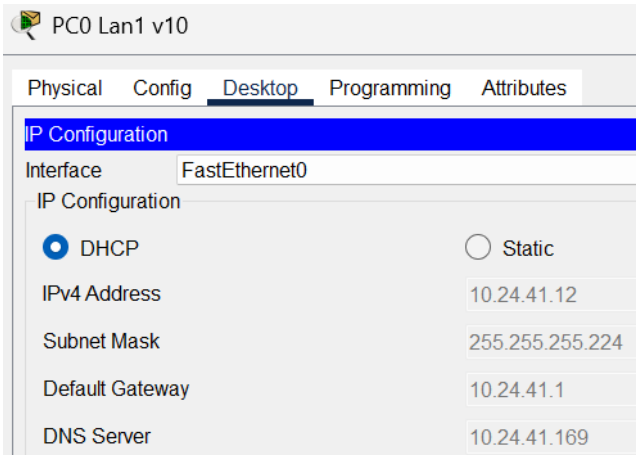


Рисунок 3.15 – Надання автоматичної адресації на 10

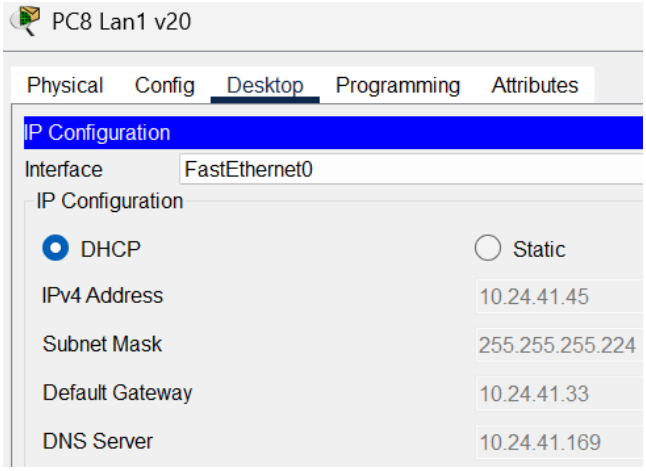


Рисунок 3.16 – Надання автоматичної адресації на 20

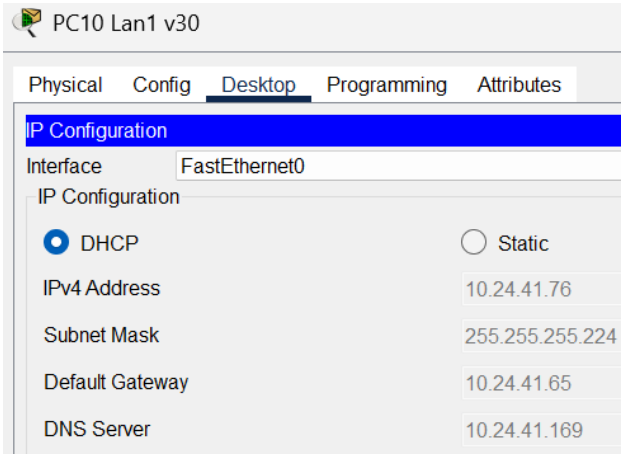


Рисунок 3.17 – Надання автоматичної адресації на 30

У якості налаштування безпеки також можна налаштувати порти на комутаторах, встановивши максимальну кількість MAC-адрес, що можуть бути використані на відповідних портах, “запам'ятовувати” ці адреси, й відхиляти незнайомі, виводячи повідомлення про порушення. Це додасть додаткового захисту на інтерфейси (Рисунок 3.18):

```
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
```

Рисунок 3.18 – Налаштування безпеки на комутаторах

Приклад ACL-списку AdminNetVlan10:

```
ip access-list extended AdminNetVlan10
 deny ip 10.24.41.0 0.0.0.31 10.24.41.32 0.0.0.31
 deny ip 10.24.41.0 0.0.0.31 10.24.41.64 0.0.0.31
 permit ip any any
```

Для перевірки коректної роботи налаштованих VLAN було здійснено тестування взаємодії хостів. Зокрема, було виконано обмін ICMP-пакетами між комп’ютерами, які належать до однієї VLAN.

Як показано на рисунку 2.16, хости в межах однієї VLAN успішно взаємодіють між собою – пакети проходять без втрат.

Для перевірки коректності роботи механізмів ізоляції було також здійснено спробу передати пакети між хостами з різних VLAN, наприклад, з VLAN 10 до VLAN 30. Відповідно до налаштованих політик доступу ACL, такий трафік блокується, що підтверджено відсутністю відповіді на ICMP-запити.

Fire	Last Status	Source	Destination	Type	Colo
	Successful	PC0 Lan1 v10	PC6 Lan1 v10	ICMP	
	Successful	PC8 Lan1 v20	PC1 Lan1 v20	ICMP	
	Successful	PC10 Lan1 v30	PC11 Lan1 v30	ICMP	
	Failed	PC0 Lan1 v10	PC10 Lan1 v30	ICMP	

Рисунок 3.19 – Перевірка взаємодії хостів у VLAN

4 РОЗРОБКА IOT КОМПЛЕКСУ РОБОЧОГО МІСЦЯ ПАЯЛЬЩИКА

4.1 Інженерне рішення для розробки компонента комп'ютерної системи

У якості компонента комп'ютерної системи відповідно до технічного завдання розроблено підсистему Інтернету речей IoT для моніторингу та автоматизованого керування інженерними системами приміщення паяльщика (рис. 4.1).

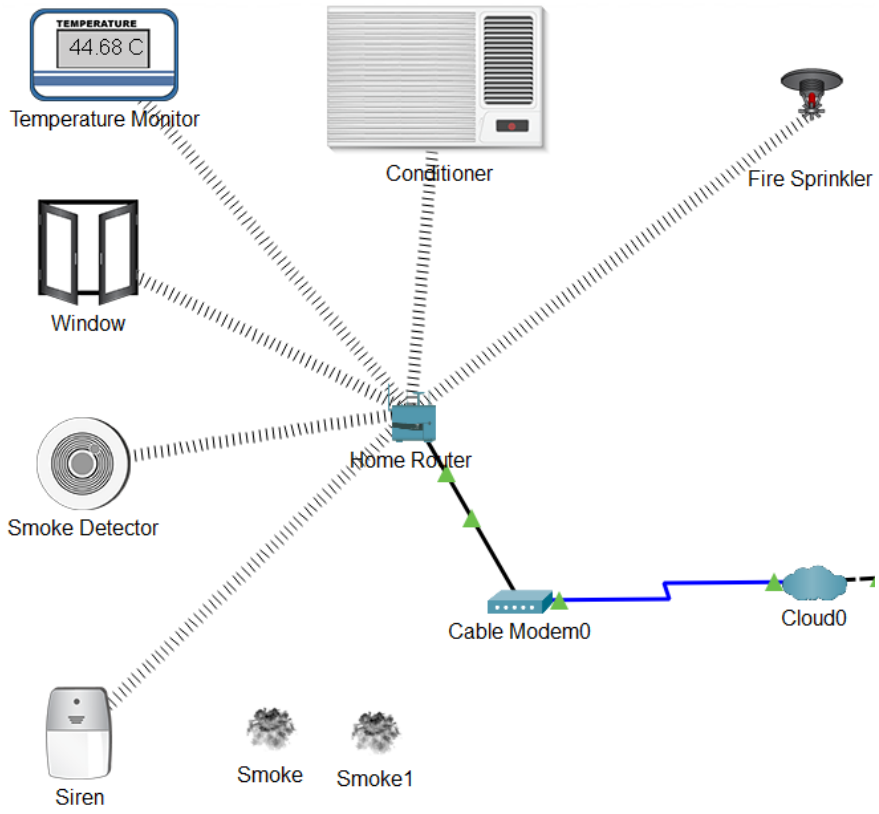


Рисунок 4.1 – IoT-система приміщення паяльщика

Основні функції даної підсистеми включають:

– моніторинг температури у приміщенні за допомогою датчиків Temperature Monitor;

– виявлення диму та попередження пожежної небезпеки з використанням Smoke Detector;

– автоматичне керування системою пожежогасіння за допомогою Fire Sprinkler;

– керування вентиляцією та кондиціонуванням (Conditioner) у залежності від температурних показників та стану повітря;

– автоматизоване відкривання вікон у разі підвищеної температури або виявлення диму;

– звукова сигналізація при фіксації тривожних подій (пожежна небезпека).

На рисунку 4.2 представлено схему алгоритму роботи системи пожежної безпеки на основі даних з температурного сенсора та датчика диму.

На рисунку 4.3 представлено схему реалізації сценаріїв керування мікрокліматом: «Відкривання вікон», «Вентиляція» та «Енергозберігаючий режим», що ілюструє логіку ухвалення рішень у системі відповідно до телеметричних показників.

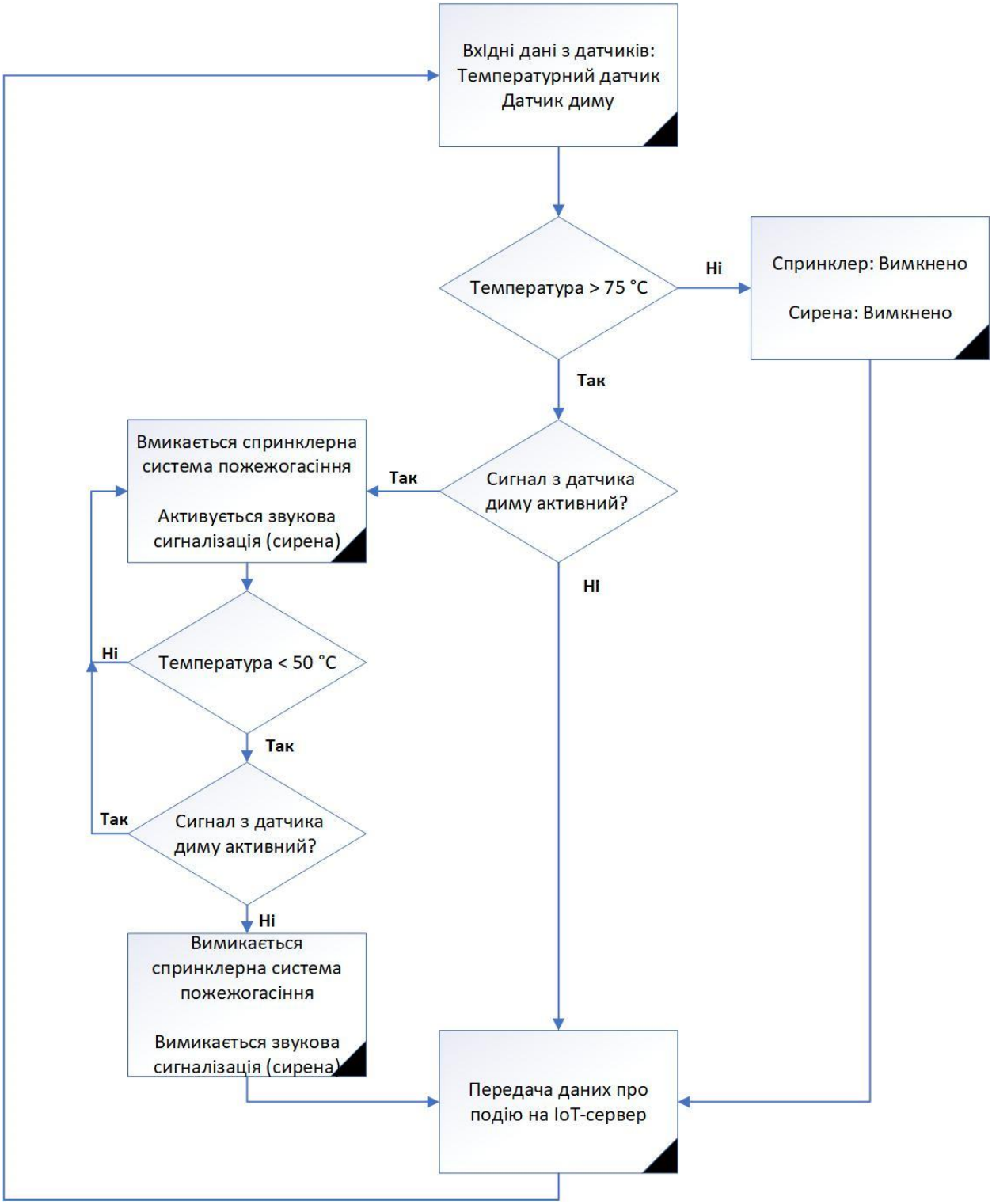


Рисунок 4.2 – Схема алгоритму роботи системи пожежної безпеки

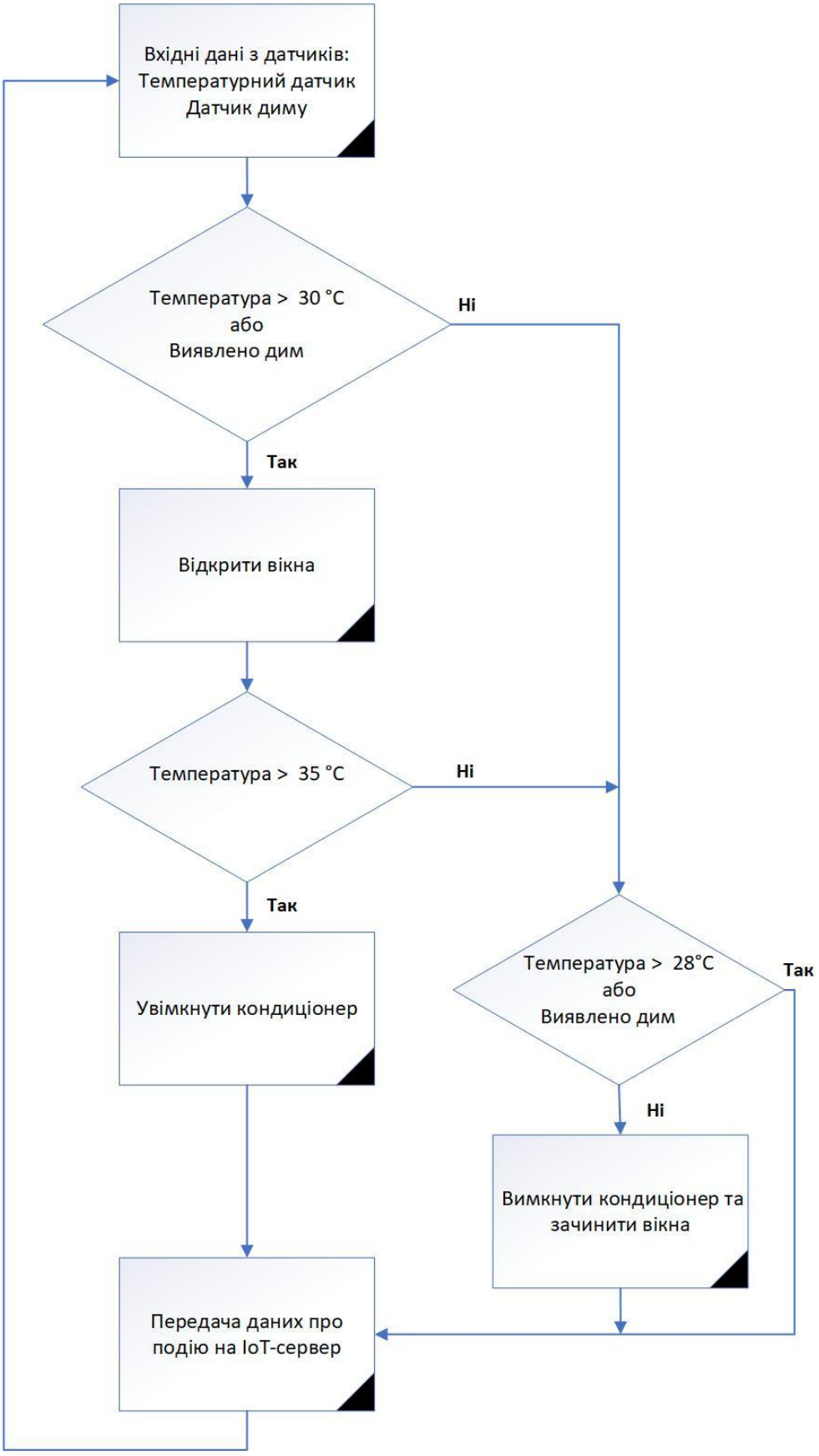


Рисунок 4.3 – Схема реалізації сценаріїв керування мікрокліматом: «Відкривання вікон», «Вентиляція» та «Енергозберігаючий режим»

Всі пристрої підсистеми реалізовано у бездротовому виконанні та об'єднано через IoT-шлюз DLC100 Home Router, що інтегровано у корпоративну мережу підприємства.

4.2 Порівняння протоколів IoT.

У процесі реалізації IoT-рішення на етапі є вибір протоколу передачі даних, який забезпечує ефективність взаємодії між сенсорами, контролерами та серверною частиною. У цій роботі використовується протокол IoT TCP, що забезпечує стабільність та гарантує доставку телеметричної інформації до локального IoT-сервера. Для повноти техніко-технологічного аналізу доцільно розрахувати порівняльні характеристики одного з найбільш розширених альтернативних протоколів – MQTT.

MQTT (Message Queuing Telemetry Transport) – це легковаговий публікаційно-підписний протокол, оптимізований для роботи в умовах обмеженого каналу зв’язку або з нестабільною доступністю мережі. Завдяки мінімальному розміру заголовків і підтримці Quality of Service, MQTT широко використовується в хмарних середовищах, мобільних застосунках і розподілених системах із великою кількістю вузлів.

У розробленій системі IoT-пристрої знаходяться у філії компанії**,** а IoT-сервер – в головному офісі. Обидві частини з’єднані через захищену корпоративну мережу, тобто дані передаються не через Інтернет, а всередині компанії. У таких умовах не потрібен брокер чи хмарна інфраструктура – достатньо простого прямого обміну між пристроєм і сервером. Саме тому було обрано IoT-TCP.

Цей протокол забезпечує:

– пряму та надійну доставку даних між IoT-пристроями та сервером;

– швидку реакцію системи без зайвих посередників;

– простоту реалізації в умовах, коли сервер і пристрої контролюються всередині однієї мережі.

Натомість протокол MQTT добре підходить для ситуацій, коли:

– пристрої розкидані по різних містах або країнах;

– немає постійного з’єднання з сервером;

– потрібна робота через Інтернет або з використанням хмарних сервісів (наприклад, AWS, Azure).

У нашому випадку все обладнання розміщене у контрольованому середовищі, з гарантованими стабільними каналами зв’язку, тому використання MQTT було б зайвим ускладненням.

4.3 Налаштування моделі системи IoT пристроїв

Архітектура IoT-системи реалізована з використанням багаторівневої моделі. На рівні речей у системі впроваджено інженерні пристрої для моніторингу параметрів середовища та автоматизованого керування. На рівні шлюзів використовується маршрутизатор DLC100, який забезпечує бездротове з’єднання IoT-пристроїв з корпоративною мережею та базовий захист підсистеми. Конфігурацію маршрутизатора DLC100 наведено на рисунку 4.4.

Конфігурація інтерфейсу Wireless маршрутизатора виконана з урахуванням вимог інформаційної безпеки. Параметри бездротового підключення IoT-пристроїв відображено на рис. 4.5.

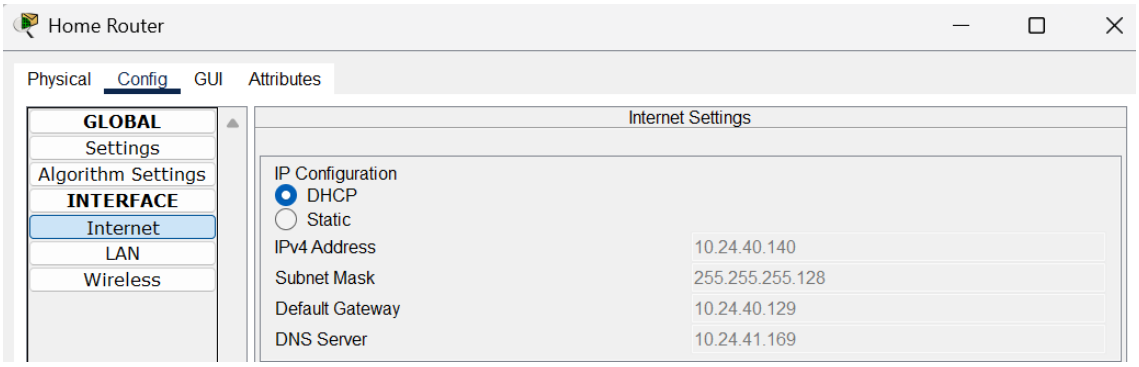


Рисунок 4.4 – Налаштування маршрутизатора DLC100 для IoT-системи

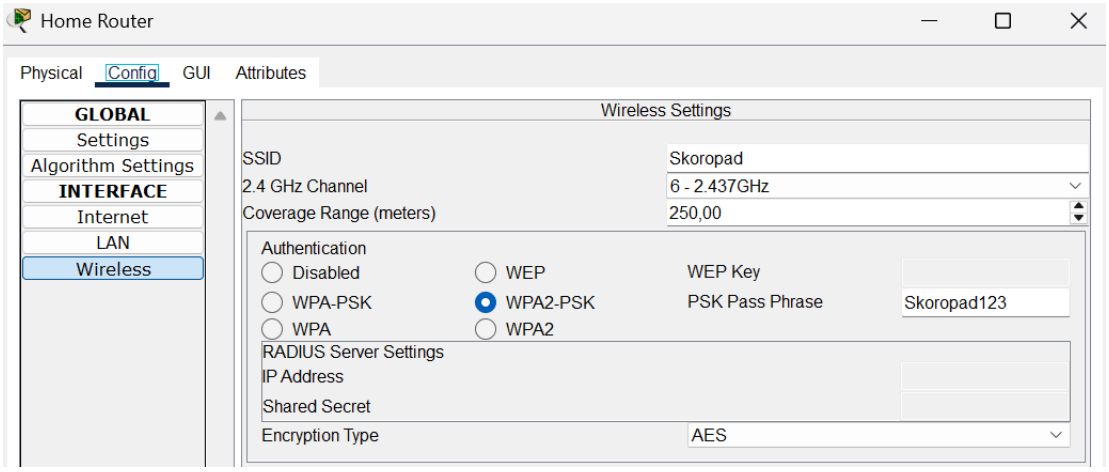


Рисунок 4.5 – Налаштування Wireless-з'єднання IoT-пристроїв

На серверному рівні розгорнуто локальний IoT-сервер, що забезпечує централізоване керування підсистемою. За допомогою веб-інтерфейсу адміністратор має змогу створювати сценарії автоматизації та здійснювати моніторинг роботи пристроїв.

Реєстрація та підключення до сервера показано на рис. 4.6 та рис. 4.7.

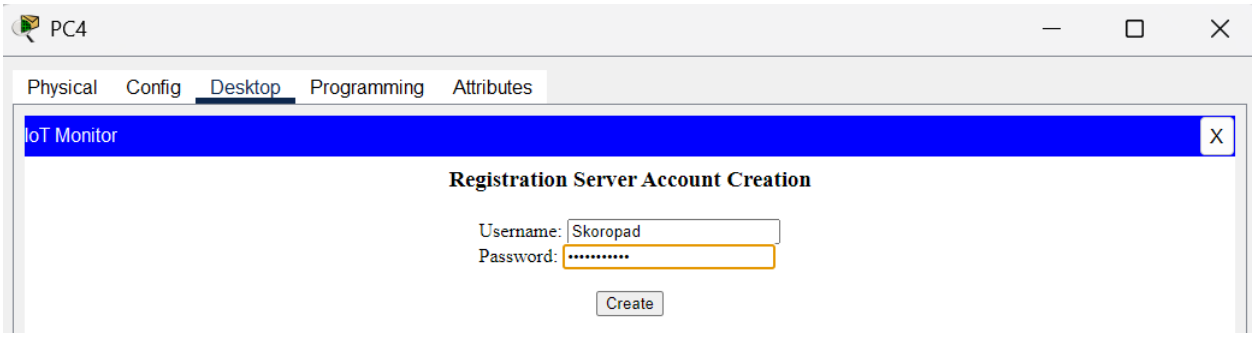


Рисунок 4.6 – Реєстрація на віддаленому IoT-сервері

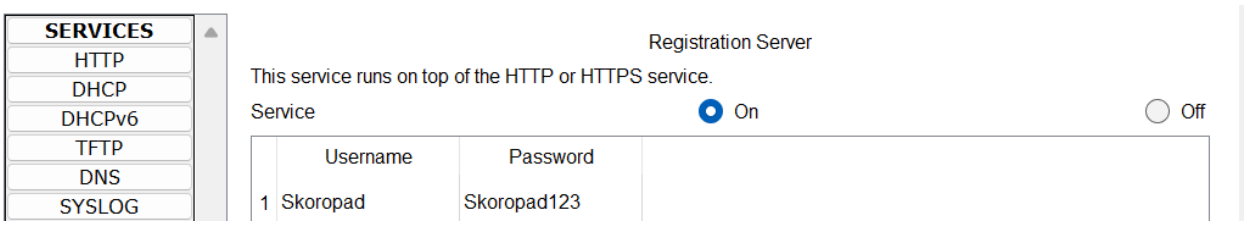
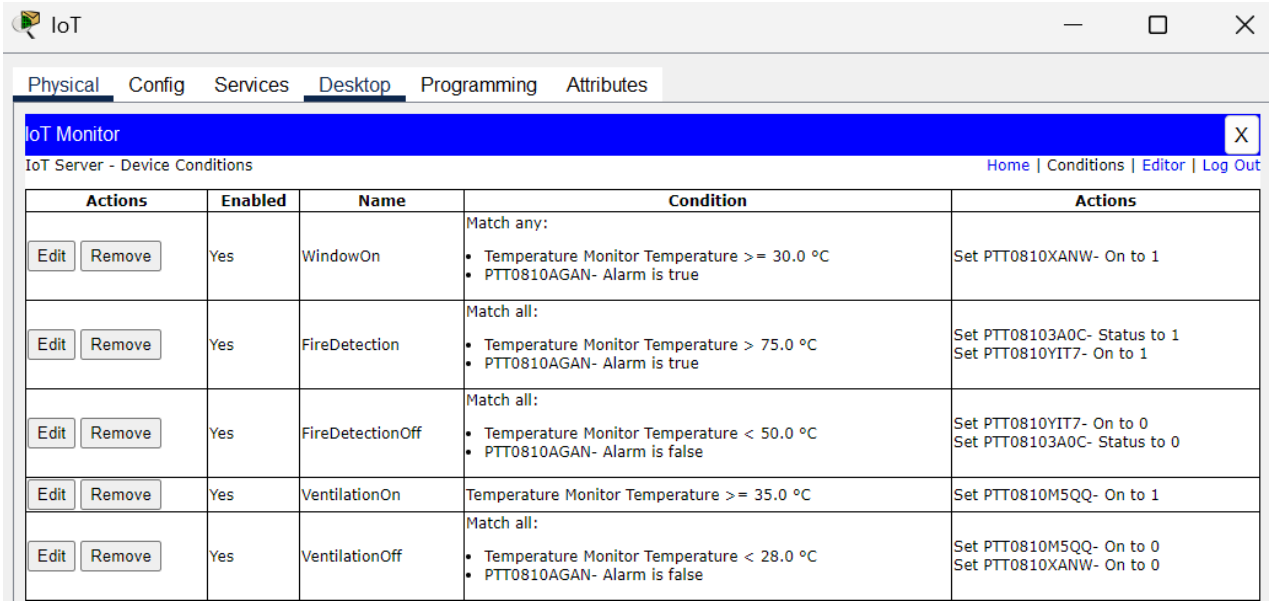


Рисунок 4.7 – Обліковий запис на віддаленому сервері

За допомогою створених сценаріїв (рис. 4.8) у веб-інтерфейсі реалізовано автоматизовану логіку реагування на зміну параметрів середовища (рис. 4.9).



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	WindowOn	Match any: • Temperature Monitor Temperature >= 30.0 °C • PTT0810AGAN- Alarm is true	Set PTT0810XANW- On to 1
Edit Remove	Yes	FireDetection	Match all: • Temperature Monitor Temperature > 75.0 °C • PTT0810AGAN- Alarm is true	Set PTT08103A0C- Status to 1 Set PTT0810YIT7- On to 1
Edit Remove	Yes	FireDetectionOff	Match all: • Temperature Monitor Temperature < 50.0 °C • PTT0810AGAN- Alarm is false	Set PTT0810YIT7- On to 0 Set PTT08103A0C- Status to 0
Edit Remove	Yes	VentilationOn	Temperature Monitor Temperature >= 35.0 °C	Set PTT0810M5QQ- On to 1
Edit Remove	Yes	VentilationOff	Match all: • Temperature Monitor Temperature < 28.0 °C • PTT0810AGAN- Alarm is false	Set PTT0810M5QQ- On to 0 Set PTT0810XANW- On to 0

Рисунок 4.8 – Сценарій для кімнати паяльщика

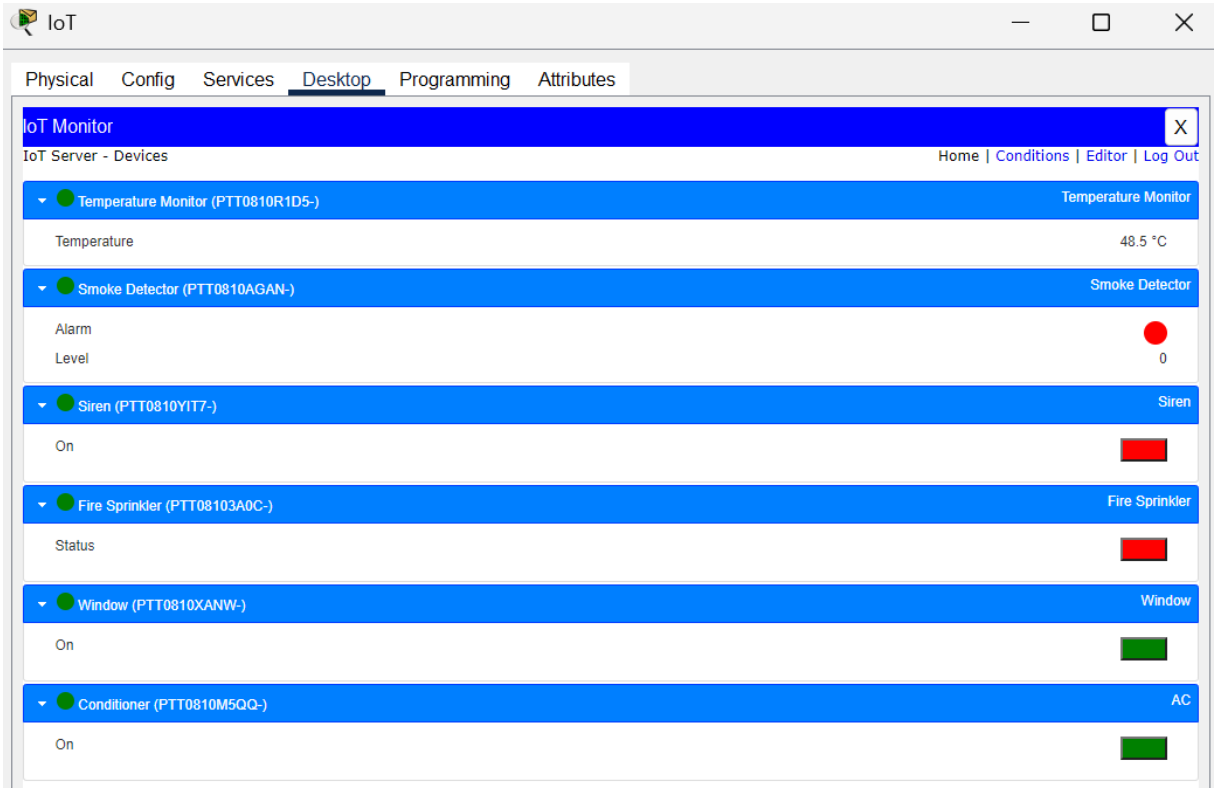


Рисунок 4.9 – Веб-інтерфейс IoT-сервера

4.4 Перевірка роботи IoT-системи

З метою підтвердження працездатності запропонованої IoT-системи було проведено її моделювання та перевірку функціональних сценаріїв у середовищі Cisco Packet Tracer. Основна увага приділялася відповідності реакції інженерних пристроїв умовам, заданим у логічних правилах обробки телеметричних даних.

Сценарій «Пожежа» (FireDetection) був протестований за умов, коли температура у приміщенні перевищувала 75 °C і одночасно було зафіксовано сигнал від датчика диму. При досягненні даної умови система коректно активувала спринклерну систему пожежогасіння та звукову сигналізацію). На рисунку 2.24 продемонстровано спрацювання цього сценарію: спринклер перейшов у стан «On», сирена також була активована. Реакція системи була оперативною – з затримкою, що не перевищувала 0,5 секунди.

Крім того, передбачено сценарій «Відключення пожежогасіння» (FireDetectionOff), який спрацьовує після нормалізації ситуації. У випадку, коли температура знижується нижче 50 °C та датчик диму більше не фіксує аномалій, система автоматично деактивує спринклер та вимикає сирену, повертаючись до стандартного режиму роботи.

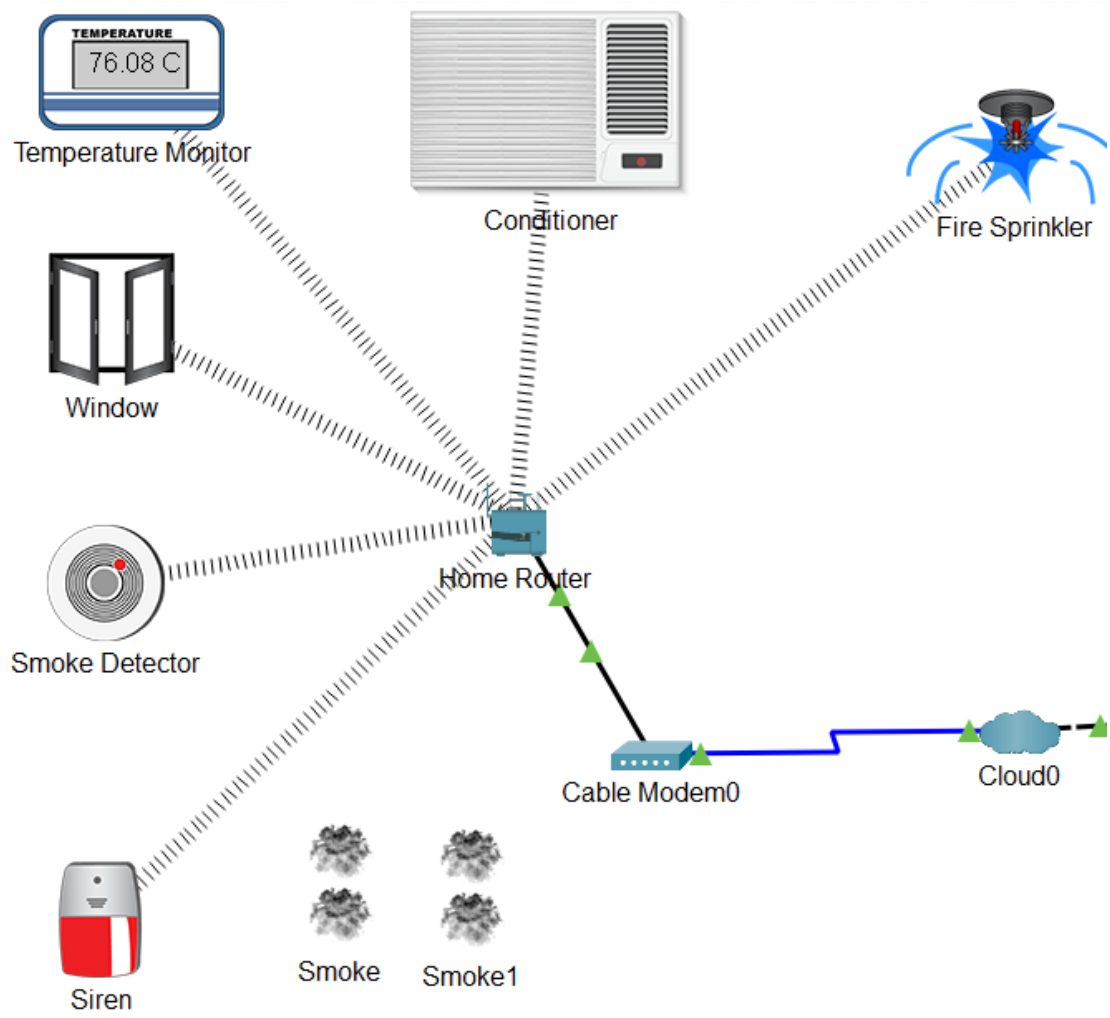


Рисунок 4.10 – Тестування сценарію пожежної безпеки

Сценарій «Відкривання вікон» (WindowOn) було протестовано у випадках:

– при підвищенні температури понад 30 °C;

– або при наявності сигналу від датчика диму.

У ході тестування, при спрацюванні однієї з зазначених умов, система автоматично відкривала вікна для природного охолодження приміщення.

На рисунках 4.11 та 4.12 показано результат тестування – стан вікон було переведено у режим «On»

Сценарій «Вентиляція» (VentilationOn) також успішно пройшов перевірку. При підвищенні температури у приміщенні понад 35 °C система

автоматично активувала кондиціонер для забезпечення належного мікроклімату. На рисунку 4.13 зафіксовано спрацювання цього сценарію – кондиціонер перейшов у стан «On».

Крім цього, у системі передбачено сценарій «Енергозберігаючий режим» (VentilationOff), що спрацьовує за умови зниження температури нижче 28 °C та при відсутності диму. У цьому випадку система автоматично вимикає кондиціонер та зачиняє вікна, оптимізуючи споживання енергії. Результати перевірки підтвердили правильність роботи зазначеного сценарію.

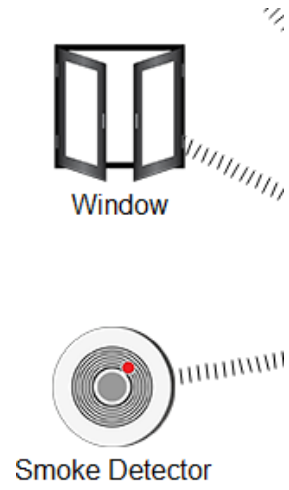


Рисунок 4.11 – Тестування сценарію відкривання вікон

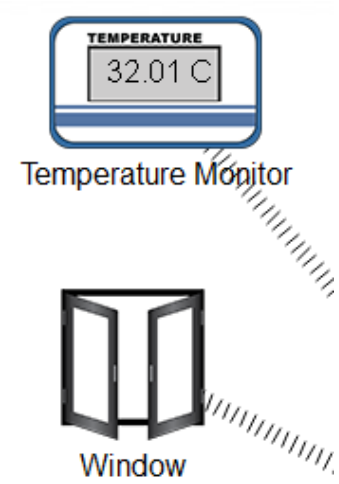


Рисунок 4.12 – Тестування сценарію відкривання вікон

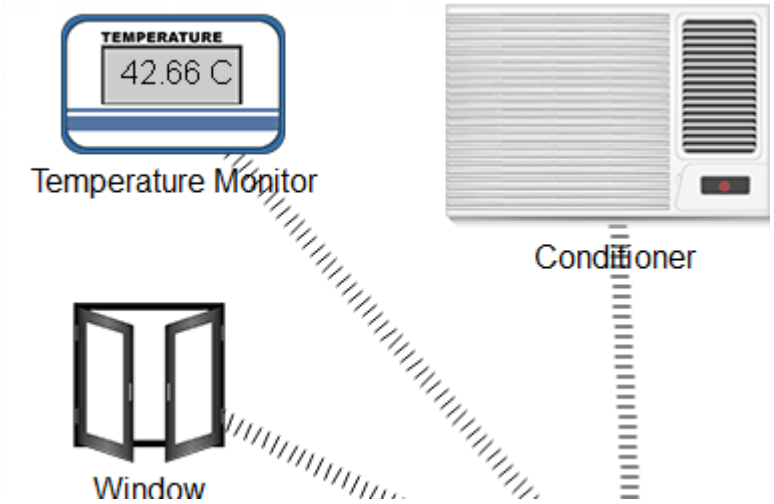


Рисунок 4.13 – Тестування сценарію вентиляції

ВИСНОВКИ

У результаті виконання передатестаційної роботи на тему «Комп'ютерна система компанії з продажу та ремонту мобільних телефонів з детальним опрацюванням IoT комплексу робочого місця паяльщика та корпоративної мережі» досягнуто поставлену мету – розроблено функціонально повну архітектуру комп’ютерної системи, адаптовану до специфіки діяльності підприємства сервісного типу.

У процесі дослідження було здійснено детальний аналіз потреб компанії в автоматизації інформаційних потоків, оптимізації взаємодії між структурними підрозділами, а також контролі параметрів робочого середовища за допомогою IoT-рішень. Реалізована модель корпоративної мережі відповідає сучасним вимогам до надійності, масштабованості та безпеки цифрової інфраструктури.

Отримані результати повністю відповідають актуальному рівню науково-технічних знань у галузі комп’ютерної інженерії. У роботі враховано практики логічного сегментування (VLAN), впровадження телеметричних протоколів (IoT-TCP), та централізованого адміністрування – рішень, що широко застосовуються у сучасних корпоративних системах.

Галузі практичного застосування результатів роботи включають підприємства роздрібної торгівлі, сервісного обслуговування електроніки, логістичні компанії, а також організації, що впроваджують цифрові технології контролю виробничих або робочих умов. Побудована система може бути легко адаптована до потреб малого або середнього бізнесу.

Наукова і технічна значущість роботи полягає у комплексному підході до розробки мережевої архітектури з урахуванням потреб IoT-комплексів. Соціально-економічна цінність проєкту проявляється у підвищенні ефективності внутрішніх бізнес-процесів, зменшенні витрат на обслуговування IT-інфраструктури та поліпшенні умов праці персоналу.

Доцільним є продовження досліджень у напрямку розширення функціональності IoT-систем, впровадження систем штучного інтелекту для аналізу телеметричних даних, а також інтеграції з хмарними сервісами для забезпечення резервного копіювання, масштабування і мобільного доступу до цифрових ресурсів компанії.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2023. – 62 с

2. Маршрутизатор Cisco 2911 (CISCO2911/K9). stack-systems.com.ua - Мережеве обладнання. URL: https://stack-systems.com.ua/marshrutizator-cisco-2911k9?srsltid=AfmBOorxwKHOfG1hTlqePkV5MSJtvbqaiIJ7C1g0WwzUu824Yt26Be02 (дата звернення: 09.05.2025).

3. Комутатори Cisco Catalyst 2960 серії. (Cisco 2960 series) | Stack Systems UA. stack-systems.com. URL: https://stack-systems.com.ua/switch/cisco-switch/cisco-catalyst-2960-series/catalyst-2960?srsltid=AfmBOopVsanvdCTqGD_ZLG0C-tzdM4ghlyVY2bwyFn9x3YtIm9BMogkt (дата звернення: 15.05.2025).

4. All About Computers. How to configure IoT using Cisco Packet Tracer, 2022. YouTube. URL: https://www.youtube.com/watch?v=op2XVCMSj4Y (date of access: 20.05.2025).

5. AI Infrastructure, Secure Networking, and Software Solutions - Cisco. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vlans.pdf (дата звернення: 20.05.2025).

6. Інструкція по експлуатації розумних кондиціонерів – [Електронний ресурс] – URL: https://23c.kh.ua/instrukcija-k-kondicioneru-lg-a09lh-a12lh-a09lh1-a12lh 1-a18lh1(дата звернення: 22.05.2025).

7. Розумні IoT вікна velux – [Електронний ресурс] – URL: https://www.velux.ua/uk-ua/products/mansardni_vikna/premium-integra-ggl-ggu (дата звернення: 22.05.2025).

8. IP-маршрутизація: Керівництво з конфігурації OSPF - Налаштування OSPF [Cisco Cloud Services Router 1000V Series]. Cisco. URL:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xe-16/iro-xe-16-book/iro-cfg.html (date of access: 16.06.2025).

9. Налаштувати та відфільтрувати списки доступу IP. Cisco. URL: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html (дата звернення: 24.06.2025).

10. HexHub. Temperature Monitoring System | Cisco Packet Tracer | Part 1, 2023. YouTube. URL: https://www.youtube.com/watch?v=j6vUCfqzY3E (дата звернення: 25.06.2025).

ДОДАТОК А

Текст програми налаштування граничного маршрутизатора

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ ГРАНИЧНОГО МАРШРУТИЗАТОРА

Текст програми

804.02070743.25023-01 12 01

Листів 6

2025

АНОТАЦІЯ

Дане налаштування належить маршрутизатору Skoropad_R3, який виконує роль граничного маршрутизатора корпоративної мережі. У конфігурації реалізовано сучасні засоби безпеки доступу, включаючи захищений привілейований режим та доступ через SSH. Організовано контроль трафіку з використанням механізмів ACL та інспекції трафіку (CBAC) для адміністративної підмережі.

Для забезпечення виходу у глобальну мережу Інтернет застосовується трансляція мережевих адрес NAT, зокрема комбіноване використання пулу динамічних адрес та статичної трансляції для публікації внутрішніх ресурсів.

Для внутрішньої маршрутизації використано OSPF з чітко визначеною топологією та пасивними інтерфейсами для підвищення безпеки

ЗМІСТ

1. Конфігураційний файл шлюзового маршрутизатора Skoropad_R3

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Skoropad_R3
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
no ip cef
no ipv6 cef
!
!
!
username Skoropad password 7 0822455D0A16
!
!
license udi pid CISCO2911/K9 sn FTX1524O8C4-
license boot module c2900 technology-package securityk9
!
!
no ip domain-lookup
ip domain-name Skoropad_R3
!
!
ip inspect name AdminNetIn-Out http timeout 3600
ip inspect name AdminNetIn-Out tcp timeout 3600
ip inspect name AdminNetIn-Out udp timeout 30
ip inspect name AdminNetIn-Out icmp timeout 10
ip inspect name AdminNetIn-Out telnet timeout 3600
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 10.24.41.161 255.255.255.240
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 10.24.41.177 255.255.255.240
ip access-group AdminNet out
ip nat inside
ip inspect AdminNetIn-Out in
duplex auto
```

```
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 10.0.23.14 255.255.255.252
ip nat inside
clock rate 2000000
!
interface Serial0/3/1
ip address 209.165.202.2 255.255.255.240
ip nat outside
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
router-id 4.4.4.4
log-adjacency-changes
passive-interface GigabitEthernet0/0
passive-interface GigabitEthernet0/1
network 10.0.23.12 0.0.0.3 area 0
network 10.24.41.160 0.0.0.15 area 0
!
ip nat pool NATPool 209.165.202.3 209.165.202.14 netmask 255.255.255.240
ip nat inside source list NATList pool NATPool
ip nat inside source static 10.24.41.168 209.165.200.4
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
!
ip flow-export version 9
!
!
ip access-list extended AdminNet
deny ip any 10.24.41.176 0.0.0.15
permit ip any any
ip access-list standard NATList
permit 10.24.40.0 0.0.0.127
permit 10.24.40.128 0.0.0.127
permit 10.24.41.128 0.0.0.31
permit 10.24.41.160 0.0.0.15
permit 10.24.41.176 0.0.0.15
permit 10.24.41.0 0.0.0.31
permit 10.24.41.32 0.0.0.31
```

```
permit 10.24.41.64 0.0.0.31
!
banner motd ^CSkoropad_R3^C
!
!
!
!
line con 0
login authentication Skoropad
!
line aux 0
!
line vty 0 4
exec-timeout 5 0
logging synchronous
transport input ssh
line vty 5 15
exec-timeout 5 0
logging synchronous
transport input ssh
!
!
!
end
```