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 Костюченка Дениса Олександровича
(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 "Кіберфізична система моніторингу роботи опалення в будинках житлового комплексу з детальним опрацюванням побудови та налаштування корпоративної мережі"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
спеціальної частини	проф. Цвіркун Л.І.			
розділу розробка корпоративної мережі	ас. Панферова Я.В.			
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)

"__" червня 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Костюченка Д.О. **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 " Кіберфізична система моніторингу роботи опалення в будинках житлового комплексу з детальним опрацюванням побудови та налаштування 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 конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2025
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2025
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2025
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2025

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

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 16.06.2025

Прийнято до виконання Костюченко Д.О.

РЕФЕРАТ

Пояснювальна записка: 67 с., 33 рис., 5 табл., 2 дод., 11 джерел.

КІБЕРФІЗИЧНА СИСТЕМА, МОНІТОРИНГ, ОПАЛЕННЯ, БУДИНОК, КОМПЛЕКС, КОРПОРАТИВНА МЕРЕЖА, КОНФІГУРАЦІЯ.

Об’єкт розробки – кіберфізична система моніторингу роботи опалення в будинках комплексу з детальним опрацюванням побудови та налаштування корпоративної мережі.

Мета роботи – створення кіберфізичної системи для моніторингу ефективності роботи опалення та оптимізації енергоспоживання у будинках комплексу.

Здійснено розробку кіберфізичної системи з можливістю гнучкої зміни набору виконуваних функцій шляхом перепрограмування та налаштування мережевих компонентів. Система орієнтована на застосування у багатофункціональному житлово-офісному комплексі для моніторингу параметрів опалення та збору статистичних даних.

Кіберфізична система дозволяє здійснювати технічну і програмну модернізацію системи опалення та забезпечує виконання наступних функцій:

– контроль температурних режимів у реальному часі; – виявлення відхилень від нормативних показників; – оптимізацію режимів роботи опалювального обладнання; – збір і підготовку аналітичної та статистичної інформації для прийняття управлінських рішень.

Розроблена корпоративна мережа забезпечує надійне збирання та передавання даних 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 наведені у пояснювальній записці та додатках.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ , УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КФС – кіберфізична система

IP – Internet Protocol, інтернет-протокол

LAN – Local Area Network, локальна мережа

WAN – Wide Area Network, глобальна мережа

VLAN – Virtual LAN, віртуальна локальна мережа

OSPF – Open Shortest Path First, протокол динамічної маршрутизації

NAT – Network Address Translation, трансляція мережевих адрес

ACL – Access Control List, список контролю доступу

DHCP – Dynamic Host Configuration Protocol, протокол автоматичної конфігурації IP-адрес

PT – Cisco Packet Tracer, середовище симуляції комп’ютерних мереж

IoT – Internet of Things, Інтернет речей

AAA – Authentication, Authorization and Accounting, автентифікація, авторизація і облік

ВСТУП

Сучасні проблеми у сфері енергоспоживання зумовлюють необхідність переходу до більш гнучких та інтелектуальних систем керування опаленням. Традиційні методи регулювання вже не здатні забезпечити необхідний рівень ефективності, особливо в умовах експлуатації на великих житлових об’єктах. Це пов’язано не лише з економічними міркуваннями, а й із потребою точнішого управління тепловими процесами.

У таких умовах доцільно впроваджувати кіберфізичні системи, що поєднують роботу фізичних пристроїв із цифровими інструментами обробки інформації. Їх головна перевага полягає в можливості безперервного моніторингу стану інженерної інфраструктури та оперативного реагування на зміни параметрів у реальному часі. Це забезпечує не лише збір телеметричних даних, але й оптимізацію роботи мережі опалення.

Застосування подібних рішень є особливо ефективним у багатоквартирних житлових комплексах, де потреба в автоматизованому контролі ресурсів є найвищою. Більшість існуючих теплових систем вимагають оновлення, щоб відповідати сучасним стандартам енергоощадності та керованості. Зокрема, важливу роль відіграє реалізація функцій дистанційного доступу до елементів регулювання.

При проєктуванні таких систем слід враховувати особливості конкретного об’єкта: структуру теплової мережі, розподіл навантажень, типи доступного обладнання. Не менш важливо закласти основу для стабільної інформаційної інфраструктури, яка б забезпечувала безперервний і надійний обмін даними.

Таким чином, впровадження подібної архітектури може стати важливим кроком до створення повноцінного елементу «розумного будинку». Це стосується не лише опалювальних систем, а й усієї технічної інфраструктури сучасного житлового комплексу.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика об'єкта дослідження та умови впровадження кіберфізичної системи моніторингу

У сучасних умовах підвищення вартості енергоресурсів та зростання вимог до енергоефективності все більшої актуальності набуває впровадження систем моніторингу й автоматичного керування інженерними мережами будівель. Особливо це стосується систем опалення, які є одним із найбільших споживачів енергії в будівлях. Ефективна робота таких систем залежить не лише від якості встановленого обладнання, а й від здатності постійно контролювати його технічний стан, виявляти відхилення та оптимізувати параметри роботи.

Об’єктом дослідження є житловий комплекс, який включає кілька будівель різного призначення - адміністративні корпуси, технічні приміщення, а також частину, що використовується під житло. Усі ці споруди мають власну систему опалення, побудовану на базі водяного теплоносія, що подається від автономного теплогенератора. У системах використовуються циркуляційні насоси, розподільні вузли, засоби обліку тепла та регулювання температури.

На момент дослідження контроль за станом опалювального обладнання здійснюється переважно вручну – за показниками термометрів, манометрів та аналогових лічильників. У разі виникнення несправностей обслуговуючий персонал виявляє їх із запізненням, що призводить до енергетичних втрат, погіршення умов експлуатації та збільшення витрат на технічне обслуговування. Крім того, відсутність єдиної системи збору даних не дозволяє проводити аналіз роботи обладнання в динаміці або планувати заходи з енергоефективності.

У таких умовах доцільним є впровадження кіберфізичної системи моніторингу, яка поєднує фізичну інфраструктуру об’єкта з цифровими засобами збору, передавання та обробки даних. Основними функціями цієї системи будуть:

- Безперервний моніторинг температури теплоносія;
- Автоматична передача даних до центрального вузла або на хмарний сервер;
- Візуалізація показників у реальному часі через інтерфейс оператора;
- Сповіщення про критичні стани, аварійні ситуації або погіршення ефективності системи;
- Аналіз даних з можливістю формування звітів і графіків.

Умови для впровадження такої системи в комплексі є загалом сприятливими. По-перше, будівлі вже мають базову IT-інфраструктуру, включаючи локальні мережі та точки доступу до інтернету. Це значно полегшує інтеграцію нових пристроїв та модулів збору інформації. По-друге, технічний персонал комплексу має достатній рівень кваліфікації для обслуговування електронного обладнання та програмного забезпечення. По-третє, адміністрація комплексу зацікавлена у скороченні витрат на енергоресурси та готова інвестувати у впровадження інноваційних рішень.

Окрему увагу під час впровадження слід приділити побудові корпоративної мережі передачі даних. Оскільки кіберфізична система передбачає встановлення десятків або навіть сотень сенсорів у різних приміщеннях та на різних рівнях будівель, необхідно забезпечити надійне, стабільне та захищене передавання інформації. Оптимальним рішенням є використання гібридної мережевої інфраструктури, що включає як дротові, так і бездротові технології (наприклад, Ethernet, Wi-Fi, LoRaWAN), із централізованим вузлом обробки, який може бути як локальним сервером, так і хмарним рішенням.

Отже, характеристика об'єкта дослідження дозволяє зробити висновок, що комплекс має всі необхідні передумови для впровадження сучасної кіберфізичної системи моніторингу. Це рішення дозволить не лише підвищити ефективність роботи системи опалення, але й створить основу для подальшої автоматизації та цифровізації інженерної інфраструктури об'єкта.

1.2 Огляд існуючих інженерних рішень у сфері кіберфізичних систем для моніторингу

У сучасній практиці управління будівлями та інженерними системами все ширше застосовуються кіберфізичні системи (КФС), які поєднують фізичні компоненти (сенсори, актуатори) із цифровими платформами обробки даних та прийняття рішень. Особливо актуальні такі системи для моніторингу та управління життєво важливими інженерними мережами – зокрема, системами опалення, вентиляції, кондиціонування, водопостачання та електропостачання.

Сучасні кіберфізичні системи для моніторингу опалення зазвичай складаються з таких основних компонентів:

a) Сенсорна мережа – датчики температури, тиску, вологості, витрати теплоносія тощо;
b) Комунікаційна інфраструктура – дротові (Ethernet, RS-485) або бездротові (Wi-Fi, Zigbee, LoRaWAN, NB-IoT) канали зв’язку;
c) Пристрої збору та передавання даних – мікроконтролери, шлюзи або концентратори;
d) Програмна частина – сервери, бази даних, платформи візуалізації, системи аналітики;
e) Інтерфейс користувача – панелі оператора, мобільні або веб-додатки для моніторингу й керування.

Одним із популярних рішень є системи на базі SCADA (Supervisory Control and Data Acquisition), які дозволяють організовувати централізований контроль та управління технологічними процесами. У сфері опалення SCADA-системи застосовуються для візуалізації температурних режимів, керування насосами, клапанами, регуляторами теплової потужності.

Також поширеними є IoT-рішення на базі мікроконтролерів (наприклад, ESP32, Arduino, STM32), які дозволяють дешево й гнучко реалізовувати функції моніторингу та дистанційного керування (див. рисунок 1.1). Дані з таких пристроїв можуть надходити до хмарних сервісів (наприклад, Blynk,

ThingsBoard, Grafana, Home Assistant) для зберігання, аналізу та сповіщень.

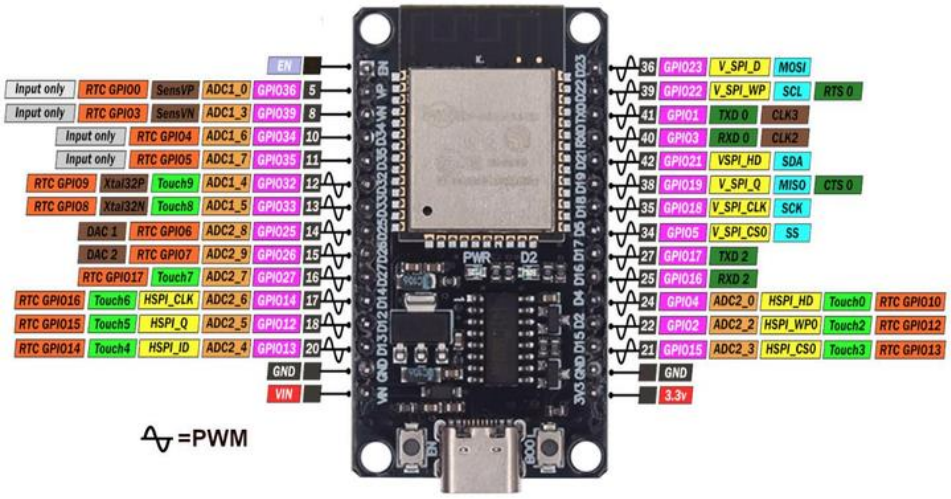


Рисунок 1.1 – Плата розробника ESP32

Ще один перспективний напрям - застосування технологій машинного навчання для прогнозування роботи систем опалення на основі історичних даних. Це дає змогу автоматично підлаштовувати режими роботи обладнання до погодних умов, часу доби або поведінки користувачів.

У великих житлових комплексах дедалі частіше впроваджуються BMS (Building Management Systems) - комплексні системи автоматизації будівель, до складу яких входять модулі моніторингу опалення, кондиціонування, освітлення, безпеки тощо. Прикладами комерційних BMS-рішень є: Siemens Desigo, Schneider Electric EcoStruxure, Honeywell Building Management Systems.

Однак такі комерційні рішення є дорогими й потребують професійного впровадження, тому для багатьох об'єктів середнього масштабу доцільнішими є гібридні або кастомні системи на основі відкритих технологій. У таких випадках розробники можуть самостійно комбінувати сенсори, мікроконтролери та програмне забезпечення, адаптуючи систему під конкретні потреби об'єкта.

Таким чином, огляд наявних рішень свідчить про широкий вибір як апаратних, так і програмних платформ для впровадження кіберфізичних

систем моніторингу опалення. Конкретний вибір залежить від масштабу об’єкта, бюджету, технічних вимог і наявної інфраструктури. У подальших розділах буде запропоновано власний варіант побудови такої системи для комплексу.

1.3 Розробка схеми організаційної структури житлового комплексу

Житловий комплекс, у межах якого планується впровадження кіберфізичної системи моніторингу опалення, є багатосекційною багатоповерховою забудовою із сучасною інженерною інфраструктурою та облаштованою прибудинковою територією. У його складі передбачено кілька будинків з автономними входами, підземним або наземним паркінгом, комерційними приміщеннями на перших поверхах, а також приміщеннями технічного призначення для розміщення інженерного обладнання.

Функціонально житловий комплекс можна умовно поділити на кілька зон: житлову, комерційну, інженерно-технічну та адміністративну. Кожна з них має власні особливості експлуатації та вимагає специфічного підходу до організації обліку, моніторингу та керування параметрами теплопостачання.

Житлова зона представлена квартирами у багатоповерхових секціях. У кожному під’їзді встановлені лічильники тепла, датчики температури внутрішнього повітря, а також точки доступу до бездротової мережі. Усі пристрої цієї зони повинні бути підключені до системи збору даних з можливістю централізованого моніторингу через диспетчерський центр.

Комерційна зона включає приміщення першого поверху, де можуть функціонувати магазини, офіси, кав’ярні або сервіси. Через підвищену щільність споживання теплової енергії та нерівномірність графіку роботи, кожен комерційний об’єкт підключено до окремого вузла обліку з незалежним опитуванням. Таке рішення дозволяє уникнути конфліктів у розрахунках та контролювати споживання в реальному часі.

Інженерно-технічна зона охоплює підвальні або технічні приміщення, де розташовуються індивідуальні теплові пункти (ІТП), насосне обладнання,

вузли вводу та серверне обладнання. Саме ця зона є ключовою для розміщення основних елементів кіберфізичної системи – комутаторів, маршрутизаторів, IoT-шлюзів, серверів зберігання і обробки даних. Тут створюються оптимальні умови для монтажу та обслуговування техніки: стабільне живлення, вентиляція, обмежений доступ.

Адміністративна зона передбачає окреме приміщення диспетчерської служби або керуючої компанії, де працівники матимуть постійний доступ до програмного забезпечення, інформаційних панелей та журналів подій системи. Через цю зону здійснюється ручне втручання, конфігурація, ведення технічної документації та обслуговування обладнання.

З організаційної точки зору, мережа комплексу складається з декількох підмереж (LAN), об’єднаних через маршрутизатори. Кожна зона функціонує у власному сегменті мережі з підтримкою VLAN-технологій, що дозволяє ізолювати трафік, зменшити навантаження на вузли й забезпечити високий рівень безпеки.

Також у межах комплексу діє система резервного енергоживлення для критичних елементів – серверів, маршрутизаторів, контролерів. Передбачено централізований журнал подій, доступ до історичних показників, формування звітності, а також можливість інтеграції з іншими системами – відеоспостереження, безпеки, контролю доступу.

Загальна топологія мережі передбачає гібридне з’єднання – дротові інтерфейси для ключових вузлів і бездротовий зв’язок для периферійних сенсорів. Це дозволяє зменшити витрати на монтаж, адаптуватися до будівельних обмежень і одночасно зберігати стабільність роботи системи.

Таким чином, організаційна структура житлового комплексу є складною, але логічно впорядкованою , як показано на рисунку 1.2. Це дозволяє створити ефективну та надійну кіберфізичну систему моніторингу, яка охоплює всі функціональні зони комплексу, оперативно збирає дані та забезпечує якісне управління теплопостачанням на базі сучасної мережевої інфраструктури.

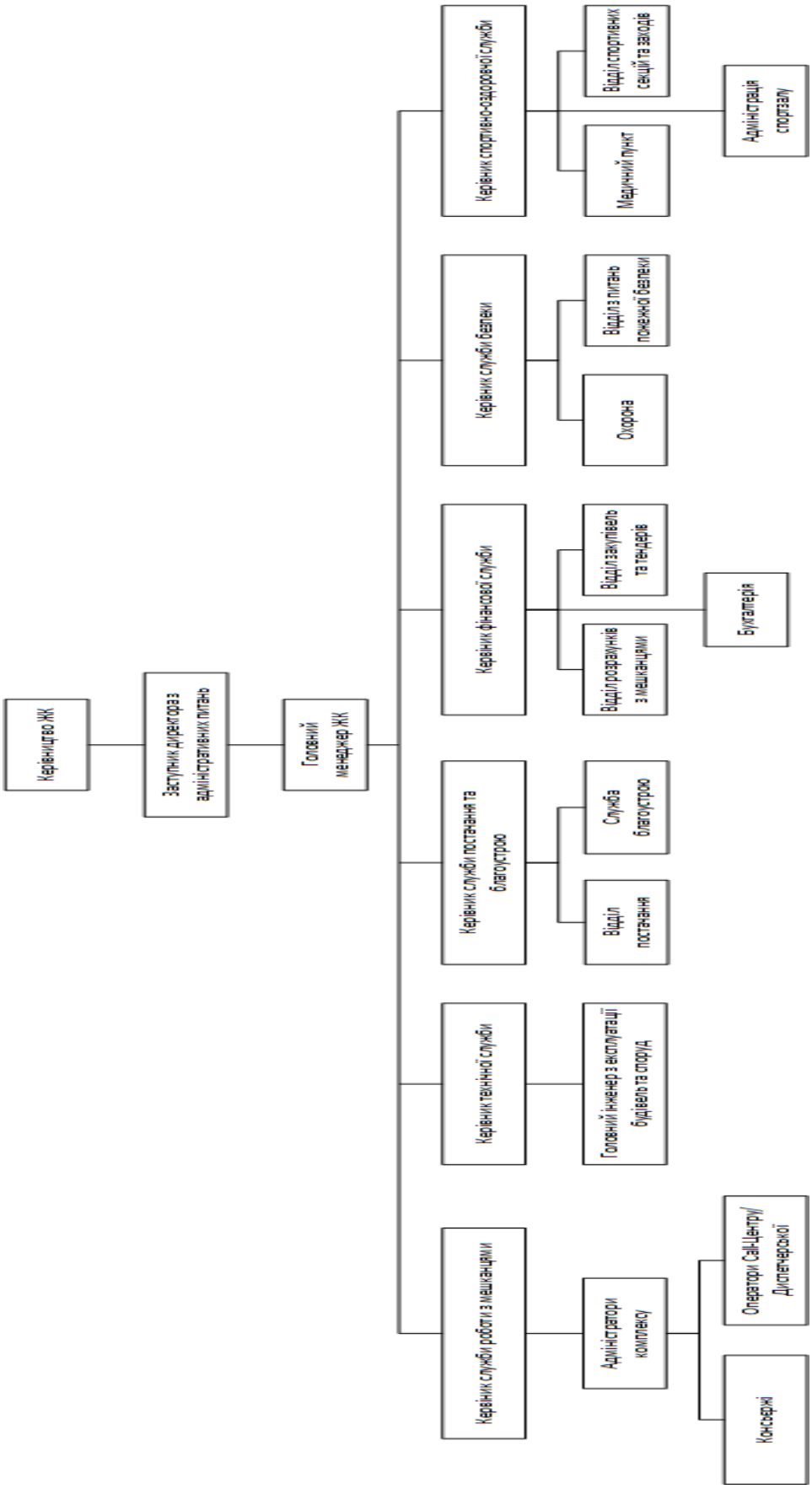


Рисунок 1.2 – Організаційна структура житлового комплексу

1.4 Аналіз недоліків існуючих систем моніторингу опалення

Попри активний розвиток цифрових технологій у сфері автоматизації житлово-комунального господарства, більшість існуючих систем моніторингу інженерних мереж, зокрема систем опалення, залишаються фрагментарними, обмеженими у функціональності та не відповідають сучасним вимогам до гнучкості, надійності та інтеграції. Особливо це стосується житлових комплексів, де інфраструктура включає багато будівель, підсистем та користувачів.

Одним з основних недоліків є відсутність комплексного підходу. Багато систем зосереджені виключно на зборі даних з теплолічильників, ігноруючи потребу в моніторингу додаткових параметрів, таких як температура в приміщеннях, тиск у трубопроводах, рівень вологості, чи робота насосного обладнання. Через це система не може оперативно виявити неефективну роботу вузла або потенційну аварійну ситуацію на ранньому етапі.

Іншою проблемою є відсутність візуалізації даних у реальному часі. Багато наявних систем лише фіксують значення з певною періодичністю, зберігаючи їх у вигляді таблиць або журналів. Такий підхід ускладнює аналіз змін температури або тиску в динаміці, а також унеможливлює швидке прийняття рішень у разі відхилень від норми.

Ще однією характерною слабкістю є незадовільна інтеграція між окремими компонентами. Наприклад, система збору даних з лічильників може бути абсолютно не пов’язана з диспетчерським пунктом або не підтримує обмін інформацією з системою контролю доступу, вентиляції чи відеоспостереження. Відсутність єдиного інформаційного середовища знижує ефективність керування та створює «острови даних».

Також актуальною проблемою є недостатня масштабованість. Більшість впроваджених рішень розроблялися для одного будинку або під’їзду. У разі розширення до рівня цілого житлового комплексу такі системи не витримують навантаження або вимагають повного переоснащення. Це створює додаткові фінансові та часові витрати, особливо коли йдеться про великі житлові об'єкти.

Ще одним важливим фактором є низька адаптивність до змін інфраструктури. Після реконструкції мережі, заміни обладнання або зміни топології системи, частина старих рішень потребує ручної переналаштування або не підтримує оновлення взагалі.

Обмежена гнучкість в обслуговуванні також є недоліком. Багато систем не мають інтерфейсів для віддаленого доступу або не дозволяють одночасну роботу кількох операторів. Це ускладнює адміністрування, а в умовах великих житлових об’єктів - робить оперативне втручання практично неможливим.

Ще один поширений недолік - відсутність підтримки стандартних протоколів обміну (таких як MQTT, SNMP, Modbus TCP). Закриті або специфічні протоколи виробника створюють так званий vendor lock-in - ситуацію, коли замінити окремі компоненти без втрати сумісності з іншими елементами системи стає неможливо.

Крім технічних обмежень, значна кількість систем має недостатній рівень інформаційної безпеки. Відсутність шифрування, централізованої автентифікації, журналів дій користувачів та ізоляції сегментів мережі створює ризики зовнішнього втручання, витоку даних або неконтрольованого доступу до критичної інфраструктури.

У підсумку, наявні рішення часто не відповідають сучасним викликам та не задовольняють вимоги як експлуатаційників, так і мешканців. Це підтверджує актуальність створення нової системи - гнучкої, відкритої, масштабованої, з повноцінною мережею збору, обробки і візуалізації даних у реальному часі. Така система має враховувати усі перераховані недоліки та реалізовувати функціональність на рівні сучасної кіберфізичної інфраструктури.

1.5 Постановка завдання

Завданням кваліфікаційної роботи є розробка інноваційної кіберфізичної системи для моніторингу та управління опаленням у житловому комплексі. Основна мета – створення комплексного рішення, яке поєднує сучасні

технології збору даних для подальшого аналізу і зручні інструменти візуалізації для швидкого прийняття рішень.

Сучасний стан системи опалення комплексу має кілька обмежень, які потребують детального аналізу та вирішення. Основні проблеми – відсутність єдиної автоматизованої системи моніторингу, неефективне використання енергоресурсів та обмежені можливості для оперативного реагування на зміни в параметрах теплопостачання.

В рамках завдання буде проведено комплексний аналіз архітектурних особливостей системи опалення комплексу, вивчено досвід застосування подібних кіберфізичних систем у житлових об'єктах і розроблена модель, що враховує специфіку роботи. Окрему увагу приділено створенню масштабованого рішення, яке можна буде застосувати й до інших житлових комплексів.

Ключовий аспект – розробка алгоритмів обробки даних, які дозволять не лише фіксувати поточний стан системи, а й прогнозувати її поведінку, виявляти збої та пропонувати оптимальні режими роботи. Для цього будуть використані методи поглибленого аналізу історичних даних і виявлення закономірностей в роботі опалення.

Важливим напрямом є інтеграція розробленої системи з існуючою інфраструктурою комплексу, що вимагає детального аналізу технічних характеристик обладнання, комунікаційних протоколів та інтерфейсів взаємодії. Особлива увага буде приділена питанням кібербезпеки та захисту даних.

Результати мають на меті не тільки підвищити енергоефективність системи опалення, але й створити методологію, яку можна застосувати для інших подібних об'єктів.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КІБЕРФІЗИЧНОЇ СИСТЕМИ МОНІТОРИНГУ РОБОТИ ОПАЛЕННЯ КОМПЛЕКСУ

2.1 Технічні вимоги до кіберфізичної системи

2.1.1 Вимоги до кіберфізичної системи моніторингу роботи опалення

Розгортання кіберфізичної системи моніторингу у сучасному житловому комплексі є важливим кроком до автоматизації управління інженерними мережами. У контексті житлового комплексу, особлива увага приділяється системі опалення як критично важливому компоненту інфраструктури.

Кіберфізична система повинна забезпечити постійний збір, передачу, обробку та зберігання даних про параметри функціонування опалення (температура, тиск, витрати теплоносія тощо), а також забезпечити можливість своєчасного реагування на аварійні або нестандартні ситуації.

Основною метою впровадження є підвищення ефективності та безпеки функціонування тепломереж, зменшення втрат енергії, автоматизація моніторингу стану обладнання, а також підвищення комфорту для мешканців. Завдяки сучасним мікроконтролерам і сенсорним пристроям, система працює автономно та здатна вчасно повідомляти про відхилення.

Основні принципи побудови

Під час розробки та впровадження кіберфізичної системи враховуються такі принципи:

- Надійність – здатність системи функціонувати безперервно, навіть у разі відмови окремих компонентів.
- Масштабованість – можливість легко додавати нові пристрої та вузли без значного переобладнання мережі.
- Безпека – захист як даних, так і самої інфраструктури від зовнішніх загроз.
- Інтеграція – здатність взаємодіяти з іншими цифровими системами або платформами керування будинками (BMS).

Стосовно деталізації вимог до кіберфізичної системи, їх можна поділити

на функціональні та нефункціональні, що наведено в таблиці 2.1:

Таблиця 2.1 – Деталізація вимог до кіберфізичної системи

Категорія	Вимоги
Функціональні	– Безперервний збір температурних і тискових показників у реальному часі – Автоматичне виявлення відхилень від норми та формування сигналів тривоги – Візуалізація параметрів на центральному сервері або в інтерфейсі диспетчера – Формування щоденних, тижневих та аварійних звітів – Можливість перегляду історії показників для аналізу ефективності системи
Нефункціональні	– Висока надійність з урахуванням резервування каналів і живлення – Захист інформації за допомогою шифрування та авторизації користувачів – Простота обслуговування та оновлення програмного забезпечення – Гнучка масштабованість відповідно до зростання житлового комплексу або підключення нових модулів

Зазначені вимоги формують основу для побудови надійної, гнучкої та ефективної системи моніторингу. Вони враховують не лише технічні, а й експлуатаційні потреби житлового комплексу та створюють передумови для подальшої цифровізації об’єкта.

2.1.2 Вимоги до структури та функціонування системи

Кіберфізична система моніторингу роботи опалення повинна мати чітко визначену логічну та фізичну структуру, що забезпечує безперервний контроль параметрів теплозабезпечення в будинках житлового комплексу. Структура системи передбачає наявність декількох функціональних компонентів, взаємопов’язаних між собою через корпоративну мережу.

Основу системи складають сенсорні пристрої (датчики температури, вологості тощо), які встановлюються в ключових технічних зонах будівель. Ці пристрої об’єднані у локальні вузли збору даних, які за допомогою бездротових або дротових засобів зв’язку передають інформацію до центрального вузла – сервера або хмарного рішення, де здійснюється обробка та аналіз показників.

Уся система повинна підтримувати централізоване функціонування з можливістю розширення у випадку розбудови житлового комплексу або зміни архітектури будівель. Передбачено дворівневу ієрархію: рівень збору даних (периферійні пристрої) та рівень обробки даних (сервер або керуючий контролер).

Для забезпечення стабільної взаємодії між компонентами системи мають бути дотримані вимоги до комунікаційного обміну. Внутрішня передача даних повинна здійснюватися за допомогою надійних протоколів (наприклад, MQTT або HTTP), а пропускна здатність мережі повинна відповідати обсягам телеметричної інформації. Комунікації між окремими модулями мають бути захищені, особливо у випадках передачі даних на віддалені сервери.

Функціонування системи повинно відбуватися в автоматичному режимі з можливістю ручного налаштування через призначений інтерфейс. Важливо забезпечити діагностику працездатності пристроїв, контроль втрати зв’язку з вузлами, відстеження відхилень параметрів від заданих норм та формування відповідних повідомлень або аварійних сигналів.

Система має бути придатною до модернізації, підтримувати оновлення програмного забезпечення пристроїв, зміну логіки обробки даних та

адаптацію до нових вимог користувача. Також важливо передбачити резервування критично важливих вузлів для уникнення повного виходу системи з ладу в разі збоїв окремих її частин.

2.1.3 Вимоги до функцій системи моніторингу

Кіберфізична система моніторингу роботи опалення повинна забезпечувати автоматизоване виконання ряду функцій, спрямованих на підтримання енергоефективної, стабільної та безпечної роботи тепломереж у житловому комплексі. Основні функції мають бути реалізовані з урахуванням вимог до точності, оперативності, надійності та зручності користування.

Першочерговою функцією системи є безперервний моніторинг параметрів опалення, таких як внутрішні та зовнішні температури, вологість повітря в приміщеннях. Збір цих показників має здійснюватися в режимі реального часу з фіксованим інтервалом опитування сенсорів.

Наступною ключовою функцією є аналіз зібраних даних з метою виявлення відхилень від нормальних робочих режимів. Система повинна мати алгоритми для обробки даних, включно з виявленням аномалій, прогнозуванням критичних ситуацій, а також можливістю формувати рекомендації щодо оптимізації роботи опалювального обладнання.

Функція інформування користувача також є критично важливою. У випадку виявлення аварійних або пограничних ситуацій система повинна автоматично формувати повідомлення та доставляти їх відповідальним особам через зручні канали зв'язку – веб-інтерфейс, мобільний застосунок або електронну пошту. Повідомлення мають містити точну інформацію про характер відхилення, місце його виникнення та можливі наслідки.

Ще однією важливою функцією є зберігання історії даних. Усі зібрані показники мають архівуватись із можливістю подальшого аналізу, побудови графіків, формування звітів та оцінки ефективності роботи системи в довготривалій перспективі. Передбачається також доступ до журналів подій, з яких можна простежити перебіг зміни параметрів або переглянути хронологію

спрацювань тривог.

Система повинна передбачати гнучкі налаштування логіки обробки даних та реакцій на ті чи інші події. Це дає змогу адаптувати її під конкретні умови експлуатації житлового комплексу, змінювати порогові значення параметрів та визначати пріоритетність обробки окремих сигналів.

Важливо, щоб усі функції могли працювати синхронно, забезпечуючи своєчасне реагування без затримок, а також щоб результати обробки мали високу достовірність. У разі втрати зв’язку або відмови окремих компонентів система має відреагувати відповідно – активувати резервні механізми або повідомити про збої.

Таким чином, функціональні можливості системи повинні відповідати сучасним вимогам до автоматизованих систем технічного моніторингу і забезпечувати користувачів точними, своєчасними та релевантними даними про стан опалення в житловому комплексі.

2.1.4 Вимоги до забезпечення системи

Для повноцінного функціонування кіберфізичної системи моніторингу роботи опалення необхідно передбачити комплексне забезпечення, яке охоплює технічні, програмні та організаційні компоненти. Всі складові повинні бути узгодженими між собою та адаптованими під специфіку житлового комплексу, де планується впровадження.

Функціонально система організована у вигляді ієрархії, що включає сенсорний рівень, рівень шлюзів, серверний рівень та рівень візуалізації. Нижче на рисунку 2.1 представлено логічну структуру кіберфізичної системи для ЖК:

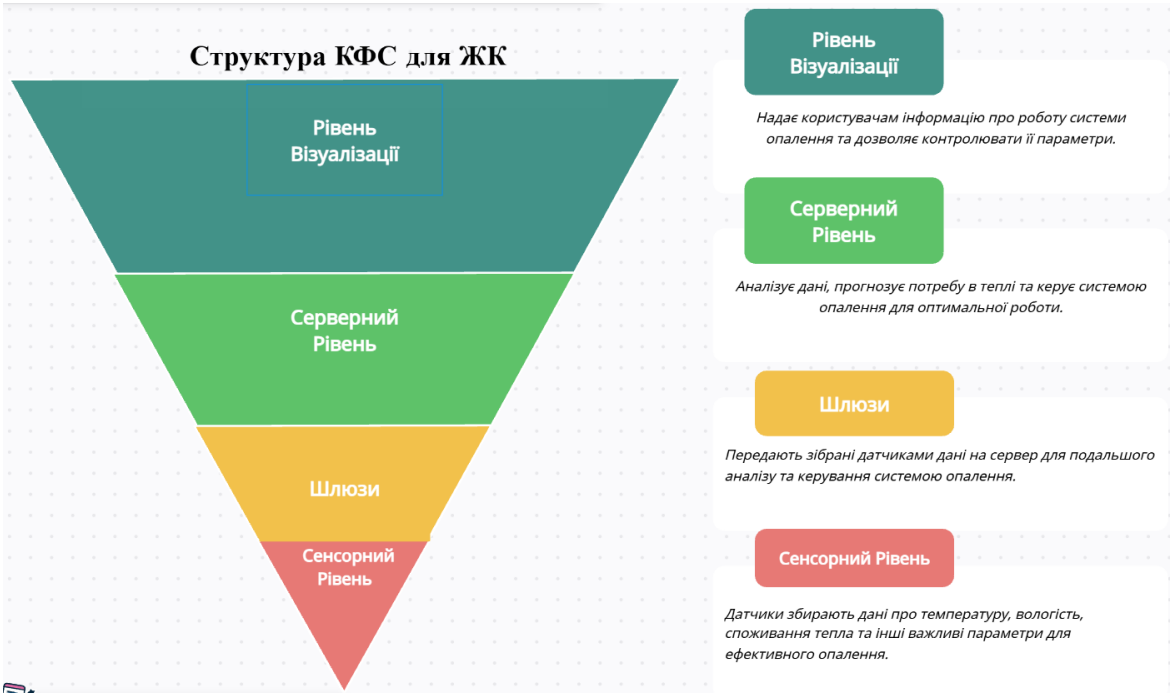


Рисунок 2.1 – Типова структура кіберфізичної системи для житлового комплексу

Перш за все, система повинна базуватись на сучасних технічних засобах, які забезпечують точність вимірювань, стабільність роботи та енергоефективність. До таких засобів належать датчики температури (наприклад, DS18B20 або DHT22), тиску, витрати теплоносія, контролери типу ESP32 або STM32, а також шлюзи для збору і передачі інформації. Вибрані пристрої повинні мати відповідні сертифікати якості, захист від пилу та вологи, та бути придатними для роботи в широкому діапазоні температур.

Програмне забезпечення має включати як вбудовані програми на мікроконтролерах, так і серверні компоненти – базу даних, модуль обробки та візуалізації інформації, веб-інтерфейс або мобільний додаток. Важливо, щоб система була гнучкою у конфігурації, підтримувала оновлення без втручання в апаратну частину та мала можливість інтеграції з іншими платформами або сервісами через API.

Організаційне забезпечення полягає у створенні умов для безперебійної експлуатації системи. Потрібно визначити порядок технічного обслуговування, відповідальних осіб, частоту перевірок обладнання, а також режим оновлення програмного забезпечення. Крім того, важливо забезпечити

навчання персоналу, що працює з системою, – для правильного користування інтерфейсами, інтерпретації отриманих даних та вчасного реагування на повідомлення.

Необхідно також враховувати вимоги до зберігання та захисту даних. Усі зібрані дані повинні архівуватися з можливістю резервного копіювання на окремий носій або хмарний сервер. Повинен бути реалізований захист від несанкціонованого доступу – як до системи, так і до самих даних. Це може включати авторизацію користувачів, шифрування трафіку та журналювання дій.

Крім того, система повинна підтримувати масштабованість. У разі розширення житлового комплексу або підключення додаткових будівель, повинна бути можливість легко додати нові вузли моніторингу без необхідності значної модифікації інфраструктури.

Таким чином, забезпечення системи має відповідати всім вимогам до сучасних кіберфізичних рішень – бути надійним, безпечним, простим в обслуговуванні та готовим до майбутнього розвитку.

2.1.5 Вимоги до експлуатації, обслуговування та безпеки

Ефективна експлуатація кіберфізичної системи моніторингу опалення передбачає наявність чітко визначених умов використання, регулярного технічного обслуговування та реалізації заходів безпеки на всіх рівнях функціонування. Ці вимоги мають бути враховані ще на етапі проєктування, щоб забезпечити довговічну та стабільну роботу системи в умовах реальної експлуатації.

Умови експлуатації повинні відповідати технічним характеристикам встановленого обладнання. Сенсорні пристрої мають бути захищені від вологи, пилу, перегрівання та механічних впливів. Для внутрішньобудинкової інфраструктури важливо забезпечити підтримку стабільної температури в приміщеннях з серверним обладнанням, резервне електроживлення (наприклад, через ДБЖ) і мінімізацію впливу електромагнітних завад.

Система має працювати в безперервному режимі, з мінімальним втручанням з боку персоналу. Водночас повинна бути передбачена періодична перевірка працездатності обладнання, зокрема – тестування сенсорів, оновлення прошивок контролерів та програмного забезпечення серверної частини. Регламент обслуговування може включати щомісячні перевірки вузлів, піврічне профілактичне обслуговування та екстрене реагування у випадку збоїв чи аварій.

Окрему увагу необхідно приділити інформаційній та фізичній безпеці системи. Оскільки система оперує потенційно чутливими даними (інформація про технічний стан будівель, режими теплопостачання тощо), має бути реалізований доступ лише для авторизованих користувачів. Рекомендується впровадити багаторівневу аутентифікацію, системи журналювання дій користувачів та шифрування переданих даних.

З технічного боку, захист передбачає використання фаєрволів, мережевої ізоляції (наприклад, VLAN для IoT-пристроїв), регулярне оновлення безпекових компонентів та застосування антивірусного/захисного ПЗ на серверній стороні. Для захисту від фізичних загроз важливо розміщувати ключові компоненти (сервери, маршрутизатори, комутатори) в окремих технічних приміщеннях з обмеженим доступом.

У випадку аварійної ситуації система повинна мати можливість сповістити персонал через попередньо налаштовані канали зв’язку, а також зберегти критичні дані до завершення інциденту. У цьому контексті важливим є також регулярне створення резервних копій – як даних моніторингу, так і конфігураційних файлів системи.

Таким чином, забезпечення належного рівня експлуатації та безпеки є не лише технічним, а й організаційним завданням, що має бути інтегроване у загальну концепцію системи моніторингу ще на етапі її проєктування.

2.2 Розробка апаратної частини та мережевої інфраструктури

2.2.1 Розробка топології розміщення пристроїв у будівлях комплексу

Для забезпечення надійної та ефективної роботи кіберфізичної системи моніторингу опалення в житловому комплексі було розроблено структуровану топологію розміщення мережевих пристроїв. Архітектура системи ґрунтується на принципах ієрархічної побудови локальних мереж з розділенням на підмережі (LAN) відповідно до функціонального призначення окремих будівель та підсистем.

Згідно з варіантом завдання, у системі реалізовано п’ять логічно розділених сегментів:

LAN1 – мережа офісів керуючої компанії та аналітичного центру;

LAN2 – підмережа окремого житлового приміщення (квартири), що включає сенсори та контролери для локального збору показників температури, вологості;

LAN3 – головна серверна та центр збору даних з теплолічильників і сенсорів;

LAN4 – мережа обслуговування та підтримки, що включає віддалений доступ для адміністраторів та інженерів;

LAN5 – мережа диспетчерської служби, що здійснює моніторинг та обробку сигналів від сенсорних систем.

Кожна підмережа реалізована за допомогою комутаторів Cisco 2960, об’єднаних у трикутну резервовану топологію для уникнення відмов у разі пошкодження одного з каналів. Для маршрутизації між сегментами використано маршрутизатори Cisco 2811 (див. рисунок 2.2).

Рисунок 2.2 – Cisco 2811

Усі підмережі мають VLAN-розділення для сервісного, адміністративного та користувацького трафіку. Центральним вузлом мережі є маршрутизатор Kostiuchenko_Router_5, через який здійснюється вихід в Інтернет, взаємодія з хмарними сервісами та резервне з'єднання із віддаленим сервером моніторингу.

Така топологія дозволяє забезпечити масштабованість, зручність, відмовостійкість та безпечний обмін даними між всіма елементами кіберфізичної системи.

2.2.2 Побудова загальної архітектури корпоративної мережі

Побудова корпоративної мережі житлового комплексу базується на сучасних принципах масштабованості, надійності та безпеки. Мережа слугує основою для функціонування кіберфізичної системи моніторингу роботи опалення, а також забезпечує передачу даних з усіх сенсорів у централізовану систему збору та обробки інформації.

Корпоративна мережа організована за ієрархічною структурою з трьома основними рівнями: доступу, агрегації та ядра. Така модель забезпечує зручне управління, гнучкість при розширенні та зменшує вплив можливих відмов окремих елементів на всю систему в цілому.

На рівні доступу розміщуються сенсори, мікроконтролери, а також комутатори (світчі), що з'єднують локальні сегменти мережі в межах кожного житлового будинку або технічного приміщення. Для організації цієї ланки використовуються гігабітні керовані комутатори з підтримкою VLAN, що дозволяє розділяти трафік сенсорів та службових систем.

На рівні агрегації передбачено встановлення центральних маршрутизаторів та мережевих серверів, які збирають трафік з усіх будинків комплексу. Пристрої агрегації відповідають за маршрутизацію, фільтрацію даних та балансування навантаження. Мережеві вузли цього рівня розміщуються у центрі обслуговування комплексу, або у спеціально виділеному приміщенні з резервним живленням.

На рівні ядра функціонує головний маршрутизатор або фаєрвол, що забезпечує з’єднання з Інтернетом, реалізує політики безпеки та контроль доступу до системи ззовні. Через цей вузол здійснюється віддалений моніторинг, адміністрування та оновлення системи. З метою забезпечення безперервної роботи використовуються технології резервування – як для з'єднання, так і для обладнання.

Дані з мікроконтролерів (наприклад, ESP32) передаються через локальні Wi-Fi мережі до комутаторів, а далі – маршрутизуються до сервера збору даних. Усі пристрої працюють у межах окремого підмережевого простору з обмеженим доступом до зовнішніх ресурсів, що підвищує рівень кіберзахисту.

Кожен сегмент мережі конфігурується з урахуванням специфіки розташування: в житлових будинках – акцент на безпровідні з'єднання та мінімальне втручання в інтер’єри; в технічних приміщеннях – переважно дротове з'єднання з кращими показниками надійності.

Для ефективного функціонування мережі використано такі технології:

- VLAN – для логічного розділення трафіку між службами;
- QoS (Quality of Service) – для пріоритетності трафіку моніторингу;
- NAT, DHCP та Firewall – для захисту мережі та зручного адміністрування;
- SNMP та Syslog – для моніторингу стану обладнання та ведення журналів подій.

Особлива увага приділяється відмовостійкості: критичне обладнання підключається до джерел безперебійного живлення, а також дублюється у критичних точках мережі. Це дозволяє забезпечити цілодобову роботу кіберфізичної системи навіть у разі часткових відмов.

Таким чином, побудована корпоративна мережа є гнучкою, безпечною та оптимізованою під завдання моніторингу опалення, відповідаючи сучасним вимогам до кіберфізичних систем в багатоквартирних житлових комплексах.

2.2.3 Обґрунтування вибору структурної схеми та технічних засобів системи моніторингу

Для реалізації кіберфізичної системи моніторингу роботи опалення у житловому комплексі було обрано структурну схему з багаторівневою ієрархією пристроїв. Такий підхід забезпечує надійність, гнучкість і масштабованість системи, дозволяючи ефективно здійснювати моніторинг та аналіз параметрів опалення в межах усієї мережі будівель комплексу.

На нижньому рівні системи, так би мовити польовому, розміщуються сенсори температури, вологості, а також пристрої для зчитування стану вузлів обліку тепла. Ці сенсори підключаються до мікроконтролерів типу ESP32, які здатні локально обробляти дані та передавати їх далі через Wi-Fi. ESP32 було обрано як універсальний і доступний пристрій, що має достатні обчислювальні можливості та бездротовий модуль зв’язку.

Передача даних між мікроконтролерами та центральними вузлами системи відбувається через мережу Wi-Fi або Ethernet. Враховуючи розмір комплексу та наявність кількох будинків, було вирішено встановити точки доступу для забезпечення стабільного покриття в технічних приміщеннях. У місцях зі значним навантаженням або потребою в надійному з'єднанні застосовуються керовані комутатори, які дозволяють сегментувати мережу, підвищити її безпеку та ефективність.

На середньому рівні системи розміщується мережеве обладнання – маршрутизатори та комутатори, які об’єднують окремі підсистеми будівель у загальну локальну мережу комплексу. Це дає змогу централізовано контролювати трафік, впроваджувати політики безпеки та забезпечувати баланс навантаження.

На верхньому рівні – серверному – розташовується головний вузол збору та обробки даних. Це може бути фізичний сервер або компактне, але потужне рішення, наприклад, Raspberry Pi або настільний ПК із серверним ПЗ. Сервер приймає та зберігає показники сенсорів, обробляє їх у реальному часі, візуалізує та формує звіти для подальшого аналізу. Саме на цьому рівні

реалізується взаємодія з користувачем, адміністрування системи, ведення архіву даних та підключення до хмарного середовища у разі потреби.

Обрана структурна схема дозволяє масштабувати систему без істотних змін в архітектурі, що важливо для перспективного розширення комплексу або інтеграції з іншими інженерними мережами. Крім того, враховуючи реальні умови експлуатації, вибрані технічні засоби забезпечують достатній рівень захисту від зовнішніх факторів, економію електроенергії та зручність обслуговування.

Для реалізації проєкту було сформовано базовий список рекомендованої апаратури, що відповідає потребам кіберфізичної системи моніторингу опалення у житловому комплексі. Під час відбору враховувались такі фактори, як функціональність пристроїв, енергоефективність, підтримка сучасних протоколів зв’язку, сумісність із обраною архітектурою системи, а також вартість та доступність компонентів. Зведені дані про основні апаратні елементи, їх призначення та характеристики наведено у таблиці 2.1. Цей перелік не є вичерпним, однак охоплює ключові вузли системи, необхідні для її базової реалізації та подальшого розширення.

Таблиця 2.2 – Специфікація апаратних засобів кіберфізичної системи моніторингу опалення

№	Найменування	Тип	Одиниці виміру	Кі-сть	Технічні Характеристики
1	Cisco 2811 Router 2800 Series ISR	Маршру-тизатор	од.	7	2 порти Fast Ethernet, 4 слоти WIC для підключення серійних інтерфейсів, 1 слот NM та AIM для розширення функціональності. Підтримка VPN, QoS та VoIP. Програмне забезпечення Cisco IOS з різними рівнями ліцензій

Продовження таблиці 2.2

2	Cisco Catalyst 2960 Series	Комутатор	од.	9	48 портів Fast Ethernet, порти Uplink SFP та Gigabit Ethernet, підтримка IEEE 802.3af PoE. Програмне забезпечення LAN Base або LAN Lite. Технологія Cisco EnergyWise для контролю енергоспоживання підключених пристроїв.
3	HPE ProLiant MicroServer Gen10 Plus	Сервер	од.	3	Компактний сервер з процесором Intel Xeon E-2224 (4 ядра, 3.4 ГГц) або Pentium Gold G5420, підтримка до 32 ГБ ОЗУ DDR4 ECC. 4 слоти для жорстких дисків/SSD (підтримка SATA та NVMe), 1 порт Oculink для високошвидкісного підключення.
4	Acer Aspire C24 All-in-One (AIO)	Моноблок	од.	32	Екран: 23.8" Full HD (1920×1080) IPS, сенсорний (опція) Процесор: Intel Core i3/i5/i7 (10-11-го покоління) або AMD Ryzen 3/5/7 Оперативна пам'ять: До 16/32 ГБ DDR4 (залежно від конфігурації) Накопичувач: SSD (до 1 ТБ) або комбо SSD + HDD Графіка: Intel UHD / AMD Radeon / NVIDIA MX330 (опція)

Продовження таблиці 2.2

5	APC Smart-UPS 1500VA LCD	ДБЖ	од.	10	Потужність: 1500VA / 900Вт Тип: Лінійно-інтерактивний Автономність: ~30-60 хв (при 50% навантаженні) Розетки: 8 (4 резервні + 4 із захистом) Керування: LCD-дисплей, USB/SmartSlot Призначення: Захист серверів та мережевого обладнання

Для забезпечення безперебійної роботи ключових елементів КФС моніторингу, зокрема серверного обладнання, вузлів диспетчерської та офісних систем, передбачено використання автономних джерел живлення (UPS). Базова конфігурація включає 10 ДБЖ потужністю від 1000 до 1500 ВА, що дозволяє підтримувати роботу критичних елементів щонайменше 10–15 хвилин при повному навантаженні, або 30+ хвилин при частковому.

2.2.4 Аналіз потенційних ризиків і обмежень впровадження КФС

У процесі розробки та впровадження кіберфізичної системи важливо враховувати не лише технічні характеристики, а й низку супутніх факторів, які можуть вплинути на стабільність, безпеку та ефективність функціонування. Серед них особливу увагу слід приділити ризикам, пов’язаним із надійністю мережі, впливом зовнішнього середовища, людським фактором, а також інтеграційними чи організаційними обмеженнями (див. таблицю 2.3). Їх своєчасна ідентифікація дає змогу передбачити слабкі місця архітектури системи та заздалегідь спланувати заходи з їхньої нейтралізації.

Таблиця 2.3 – Основні ризики впровадження кіберфізичної системи моніторингу

№	Категорія ризику	Опис проблеми	Потенційні наслідки	Можливі заходи мінімізації
1	2	3	4	5
1	Технічні збої	Вихід з ладу сенсорів, збої шлюзів або серверного ПЗ	Втрата даних, некоректні показники	Резервне живлення, дублювання критичних вузлів
2	Якість мережевого сигналу	Слабке покриття в технічних приміщеннях, затримки передавання	Переривання зв'язку з сенсорами, затримка сигналів	Використання провідного зв'язку, підсилювачів сигналу
3	Кіберзагрози	Відсутність шифрування, слабка автентифікація, відкриті порти	Несанкціонований доступ, викрадення або модифікація даних	Впровадження VLAN, ACL, протоколів шифрування (HTTPS, SSH)
4	Енергетична залежність	Втрата живлення призводить до зупинки всієї системи	Повна недоступність моніторингу	Установлення ДБЖ або живлення від окремої лінії
5	Людський фактор	Помилки конфігурації, недостатня кваліфікація персоналу	Втрата працездатності системи, неправильні налаштування	Документація, навчання персоналу, чіткі процедури

Продовження таблиці 2.3

6	Несумісність з існуючими системами	Складність інтеграції з платформами ЖК або SCADA	Подвійний облік, дублювання інформації	Розробка проміжного API, шлюзів або адаптерів
7	Масштабова-ність	Складність додавання нових вузлів, перенавантаження мережі	Ручна IP-конфігурація, порушення топології	DHCP, автоматичне виявлення пристроїв, SNMP
8	Фінансові обмеження	Висока вартість мережевого обладнання, серверів	Відмова від впровадження або використання застарілих технологій	Гібридний підхід, часткове віртуальне розгортання

2.3 Перспективи розвитку та масштабування системи

Кіберфізична система моніторингу, як і будь-який сучасний цифровий інструмент, повинна мати потенціал для подальшого розвитку, розширення функціональних можливостей і адаптації до змін у структурі житлового комплексу або технологічному середовищі. Вже на етапі проєктування необхідно передбачити її масштабованість, щоб у майбутньому можна було безперешкодно додавати нові вузли, змінювати логіку обробки даних або інтегрувати систему з іншими цифровими платформами.

Один з основних напрямів розвитку – це розширення географії контролю. Якщо спочатку система впроваджується в окремих будинках чи під'їздах, надалі вона може охопити весь житловий квартал або навіть кілька об'єктів, об'єднаних у єдину енергетичну або інформаційну інфраструктуру. Завдяки модульній побудові, додавання нових точок збору даних можливе без критичних змін у загальній архітектурі.

Також передбачається можливість інтеграції з іншими системами управління – наприклад, із системою диспетчеризації, пожежної безпеки, вентиляції або освітлення. Це дозволить створити комплексне рішення для моніторингу та управління інженерними мережами на базі єдиної цифрової платформи. Така інтеграція відкриває шлях до реалізації концепції "розумного будинку" або навіть "розумного міста".

Функціональне масштабування також може включати впровадження елементів штучного інтелекту для прогнозування несправностей, оптимізації режимів опалення залежно від погодних умов або поведінки мешканців. Аналіз великих масивів даних, зібраних за тривалий час, дозволить будувати математичні моделі для виявлення закономірностей у споживанні тепла, що стане основою для зниження енерговитрат.

Ще одним перспективним напрямом є використання хмарних технологій. Перехід на зберігання та обробку даних у хмарному середовищі забезпечить доступ до інформації з будь-якої точки, спростить обслуговування та забезпечить додаткові рівні надійності через розподіленість даних.

З точки зору обслуговування, у майбутньому можлива автоматизація більшості процесів технічної підтримки – оновлення програмного забезпечення «по повітрю» (OTA), віддалена діагностика обладнання, попереджувальні повідомлення про зниження рівня сигналу або зношення елементів системи. Принцип оновлення «over-the-air» показано на рисунку 1.1.

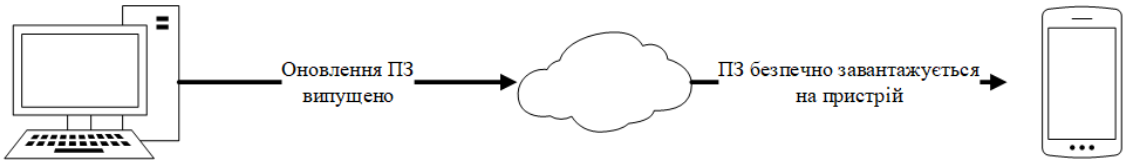


Рисунок 2.3 – Принцип оновлення «over-the-air»

Таким чином, проєктована система не є статичним рішенням – вона здатна еволюціонувати, реагувати на зміни зовнішнього середовища та зростаючі вимоги користувачів. Це забезпечує її актуальність, гнучкість і довготривалу ефективність експлуатації.

3 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ СИСТЕМИ

3.1 Розрахунок IP-адресації для підмереж житлового комплексу

Для забезпечення коректної роботи кіберфізичної системи моніторингу опалення у межах житлового комплексу необхідно попередньо здійснити поділ загального IP-адресного простору на логічні підмережі. Такий підхід дозволяє структурувати мережу, забезпечити ізоляцію трафіку між різними зонами, налаштувати маршрутизацію, підвищити рівень захисту та гнучко реагувати на зміни у конфігурації.

У мережі житлового комплексу реалізовано декілька функціональних підсистем, зокрема:

Офісна підмережа (LAN1) об'єднує офіси керуючої компанії та аналітичний центр. У цьому сегменті працюють клієнтські ПК, системи керування, робочі станції аналітиків та управлінців, які мають доступ до візуалізації показників та зведеної статистики роботи системи опалення.

Житлове приміщення – сенсорна підмережа (LAN2) представляє собою приклад реалізації локальної КФС у межах однієї квартири. Тут розміщено датчики температури, вологості, які фіксують параметри мікроклімату. Отримані дані надсилаються до центрального серверного вузла для зберігання, обробки та подальшого аналізу.

Головна підмережа (LAN3) об’єднує центр збору та обробки даних системи моніторингу. У цьому сегменті розміщено сервери, бази даних, шлюзи для прийому телеметричної інформації з підмереж (зокрема LAN2), а також інфраструктурні сервіси – DNS, HTTP. LAN3 є центральним вузлом, через який здійснюється обмін даними між усіма логічними сегментами системи – LAN1, LAN2, LAN4 та LAN5.

Сервісна підмережа (LAN4) використовується для обслуговування та технічного супроводу системи. У її межах функціонує TFTP-сервер, мережа резервного адміністрування та інженерні вузли. Доступ до цього сегмента

мають лише авторизовані адміністратори, а трафік ізольований від решти підмереж для забезпечення стабільної та безпечної роботи.

Диспетчерська підмережа (LAN5) відповідає за роботу диспетчерської служби, в якій персонал здійснює моніторинг показників у реальному часі, приймає рішення щодо регулювання теплового режиму, формує звіти та проводить діагностику на основі отриманих даних.

Згідно з варіантом завдання 12, виділено блок адрес 172.24.160.0/21, який включає 2048 IP-адрес, що підходить для організації структури з декількома незалежними підмережами. Початково необхідно визначити кількість вузлів у кожній з них. В облік беруться не лише основні робочі станції, а й допоміжні пристрої: шлюзи, точки доступу, системи захисту, мережеві принтери, трансляційні адреси, а також закладається резерв на розширення. Детальні дані представлені у таблиці 3.1.

Таблиця 3.1 – Список підмереж

Підмережа	Назва	Кі-сть вузлів
LAN1	офісна підмережа	84
LAN2	сенсорна підмережа	28
LAN3	головна підмережа	43
LAN4	сервісна підмережа	101
LAN5	диспетчерська підмережа	215

Після підрахунку кількості хостів постає питання вибору способу розподілу адресного простору. Статичне виділення фіксованої маски (наприклад, /24 для всіх сегментів) призвело б до суттєвої перевитрати адрес, особливо для малих підмереж, таких як диспетчерська або сенсорна. Тому було обрано метод VLSM (Variable Length Subnet Masking), який дозволяє гнучко задавати розмір кожної підмережі відповідно до фактичних потреб.

Методика VLSM передбачає послідовне виділення блоків з відповідною довжиною префіксу. Найбільшій підмережі (LAN5) присвоюється маска /24,

яка охоплює 254 вузли. Меншим сегментам виділяються блоки з масками /25, /26 та /27, що дозволяє значно зменшити кількість невикористаних адрес.

Такий підхід є гнучким, масштабованим та дозволяє зберігати адресний простір для майбутніх змін або резервних зон. Детальний розподіл IP-адрес із використанням VLSM наведено у таблиці 3.2.

Таблиця 3.2 – Виділення IP-адрес з використанням VLSM

Підмережа	Адреса мережі	IP-діапазон	Маска	Доступно хостів	Виділено фактично	Шлюз
LAN5	172.24.160.0	172.24.160.1 - 172.24.160.254	/24	254	215	172.24.160.1
LAN4	172.24.161.0	172.24.161.1 - 172.24.161.126	/25	126	101	172.24.161.1
LAN1	172.24.161.128	172.24.161.129 - 172.24.161.254	/25	126	84	172.24.161.129
LAN3	172.24.162.0	172.24.162.1 - 172.24.162.62	/26	62	43	172.24.162.1
LAN2	172.24.162.64	172.24.162.65 - 172.24.162.94	/27	30	28	172.24.162.65

Окремі IP-адреси у кожній підмережі зарезервовані для шлюзу. Після призначення усіх підмереж використано близько 512 адрес, що залишає значний вільний простір у межах виділеного блоку для розширення системи або створення WAN-лінків, DMZ-зони та інших додаткових компонентів.

Отже, застосування методу VLSM у межах роботи дозволило мінімізувати витрати IP-ресурсу, чітко розмежувати функціональні сегменти мережі, забезпечити резерв і спростити подальшу маршрутизацію. Такий підхід вважається найбільш доцільним у випадках, коли структура мережі складається з декількох різнорозмірних підмереж і потребує чіткої організації.

3.2 Побудова моделі кіберфізичної мережі в Cisco Packet Tracer

Логічна структура мережі житлового комплексу охоплює п’ять підмереж, кожна з яких відповідає окремим функціональним компонентам кіберфізичної системи моніторингу. Такий поділ забезпечує структурованість, безпеку та ефективну маршрутизацію трафіку між елементами системи.

Загальна архітектура мережі реалізована за принципом ієрархічної моделі, яка включає як основні локальні сегменти, так і віддалені вузли. Одна з підмереж – умовно віддалена – підключена через зовнішній маршрутизатор, що моделює доступ через телекомунікаційне обладнання провайдера. Це дозволяє врахувати сценарії реального розміщення підрозділів або технічних об'єктів поза межами основної будівлі.

На рівні ядра мережі функціонують чотири маршрутизатори, які забезпечують зв’язність між усіма сегментами. Вони з'єднані між собою у повнозв’язну топологію, що підвищує надійність роботи мережі, дозволяє ефективно маршрутизувати трафік і забезпечує швидке перемикання у разі часткової відмови. Така схема гарантує високу продуктивність системи та стійкість до збоїв, що особливо важливо для кіберфізичної інфраструктури житлового призначення.

Для візуалізації та перевірки працездатності моделі використано програмне середовище Cisco Packet Tracer, яке дозволяє детально змоделювати логіку роботи мережі, налаштування пристроїв, маршрутизацію та взаємодію між підмережами в умовах, наближених до реального середовища. Архітектура кіберфізичної системи представлена на рисунку 3.1.

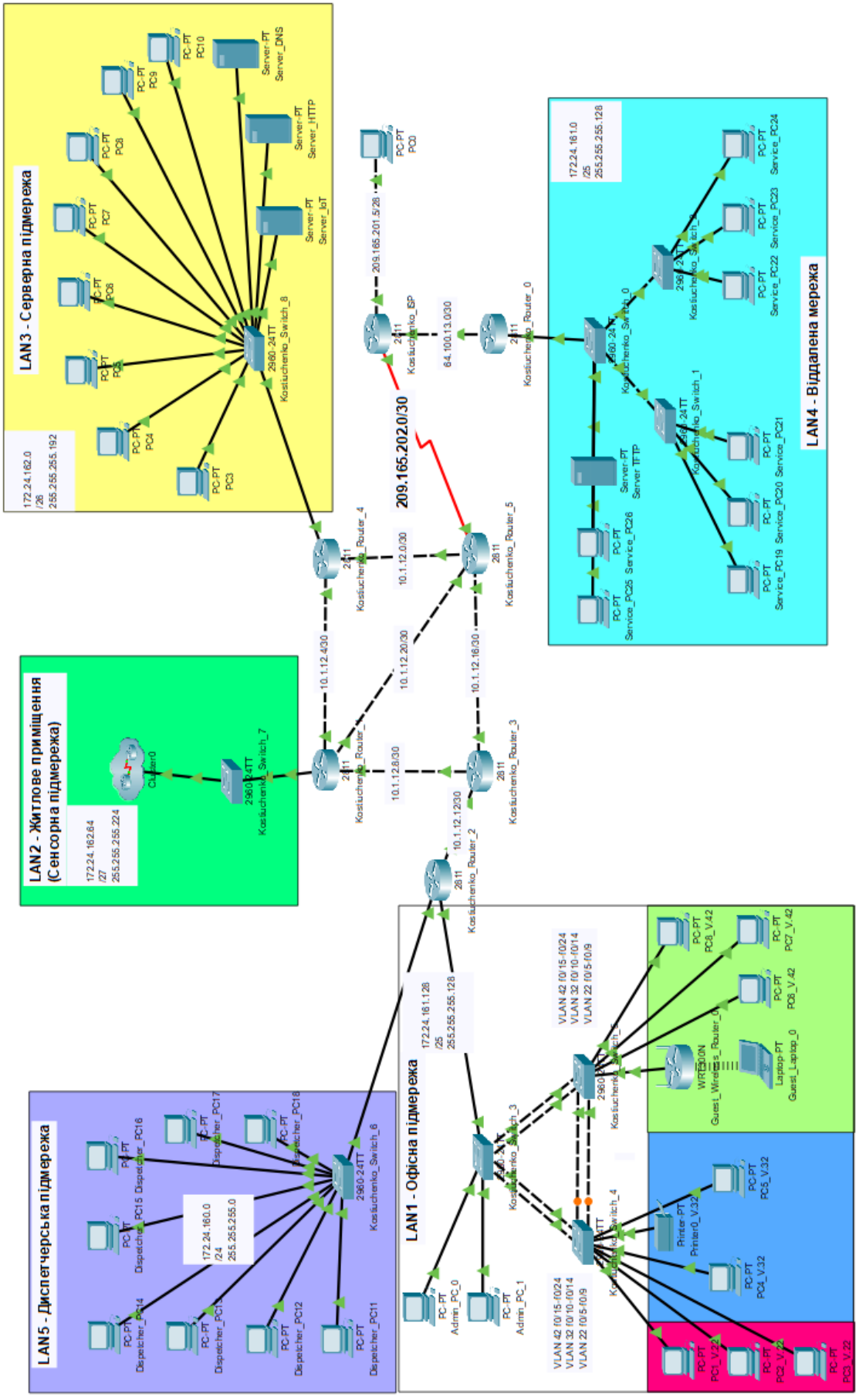


Рисунок 3.1 – Архітектура кіберфізичної системи

3.3 Налаштування пристроїв у моделі

3.3.1 Базове налаштування конфігурації пристроїв

Першим етапом проєктування корпоративної мережі кіберфізичної системи є формування схеми IP-адресації з урахуванням технічних вимог до мережевої інфраструктури. Згідно з варіантом завдання, організації надано IP-простір у межах мережі 172.24.160.0/21, що забезпечує до 2046 доступних IP-адрес. Цей обсяг дозволяє реалізувати необхідну кількість підмереж із резервом для майбутнього розширення.

Усього в системі передбачено п’ять локальних підмереж, кількість вузлів у кожній із яких визначено з урахуванням можливого масштабування:

LAN1 (офісна) – 84 пристрої;

LAN2 (житлове приміщення / сенсорна) – 28 пристроїв;

LAN3 (серверна) – 43 пристрої;

LAN4 (сервісна) – 101 пристрій;

LAN5 (диспетчерська) – 215 пристроїв.

Крім того, мережа передбачає кілька міжмаршрутизаторних з’єднань, які потребують створення окремих точок IP-зв’язку. Для цього зазвичай використовується допоміжний адресний блок, який ділиться на підмережі з префіксом /30, що ідеально підходить для з’єднання двох активних пристроїв у точці-точці.

Для ефективного використання адресного простору обрано метод VLSM (Variable Length Subnet Mask), що дозволяє задавати підмережі різної довжини маски залежно від потреби в кількості вузлів. Це забезпечує мінімальні втрати адрес та можливість залишити вільні діапазони для подальших змін у структурі мережі.

Під час розрахунку використовувалися округлені значення з урахуванням службових адрес та запасу. Таким чином було призначено такі маски:

- LAN1 – маска /25 (до 126 хостів);
- LAN2 – маска /27 (до 30 хостів);
- LAN3 – маска /26 (до 62 хостів);
- LAN4 – маска /25 (до 126 хостів);
- LAN5 – маска /24 (до 254 хостів).

Решта простору зарезервована під міжмаршрутизаторні зв’язки та потенційні службові підмережі. Зокрема, для кожного з’єднання між маршрутизаторами створено окрему підмережу з префіксом /30 (4 адреси, з яких 2 доступні), що дозволяє організувати стабільну маршрутизацію між сегментами мережі.

У результаті реалізовано логічну адресну структуру, що дозволяє гнучко керувати підмережами, гарантувати маршрутизованість та масштабованість архітектури кіберфізичної системи (див. таблицю 3.3).

Таблиця 3.3 – Схема адресації пристроїв

Пристрій	Інтер-фейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключе-ного пристрою
Kostiuchenko_ Router_0	Fa0/0	64.100.13.2	/30	-	1	Kostiuchenko_ ISP Fa0/0
	Fa0/1	172.24.161.1	/25	-	1	Kostiuchenko_ Switch_1 G0/1
Kostiuchenko_ Router_1	Fa0/0	10.1.12.9	/30	-	1	Kostiuchenko_ Router_3 Fa0/1
	Fa0/1	10.1.12.6	/30	-	1	Kostiuchenko_ Router_4 Fa0/0
	Fa1/0	10.1.12.22	/30	-	1	Kostiuchenko_ Router_5 Fa0/1
	Fa1/1	172.24.162.65	/27	-	1	Kostiuchenko_ Switch_7 G0/1
Kostiuchenko_ Router_2	Fa0/1	10.1.12.14	/30	-	1	Kostiuchenko_ Router_3 Fa0/0
	Fa1/0.22	172.24.161.129	/27	-	22	Kostiuchenko_ Switch_3 G0/1
	Fa1/0.32	172.24.161.161	/27	-	32	Kostiuchenko_ Switch_3 G0/1

Продовження таблиці 3.3

	Fa1/0.42	172.24.161.193	/27	-	42	Kostiuchenko_ Switch_3 G0/1
	Fa1/0.99	172.24.161.225	/27	-	99	Kostiuchenko_ Switch_3 G0/1
	Fa1/1	172.24.160.1	/24	-	1	Kostiuchenko_ Switch_6 G0/1
Kostiuchenko_ Router_3	Fa0/0	10.1.12.13	/30	-	1	Kostiuchenko_ Router_2 Fa0/1
	Fa0/1	10.1.12.10	/30	-	1	Kostiuchenko_ Router_1 Fa0/0
	Fa1/0	10.1.12.18	/30	-	1	Kostiuchenko_ Router_5 Fa1/0
Kostiuchenko_ Router_4	Fa0/0	10.1.12.5	/30	-	1	Kostiuchenko_ Router_1 Fa0/1
	Fa0/1	10.1.12.2	/30	-	1	Kostiuchenko_ Router_5 Fa0/0
	Fa1/1	172.24.162.1	/26	-	1	Kostiuchenko_ Switch_8 G0/1
Kostiuchenko_ Router_5	Se0/0/0	209.165.202.2	/30	-	1	Kostiuchenko_ ISP Se0/0/0
	Fa0/0	10.1.12.1	/30	-	1	Kostiuchenko_ Router_4 Fa0/1
	Fa0/1	10.1.12.21	/30	-	1	Kostiuchenko_ Router_1 Fa1/0
	Fa1/0	10.1.12.17	/30	-	1	Kostiuchenko_ Router_3 Fa1/0
Kostiuchenko_ ISP	Se0/0/0	209.165.202.1	/30	-	1	Kostiuchenko_ Router_5 Se0/0/0
	Fa0/0	64.100.13.1	/30	-	1	Kostiuchenko_ Router_0 Fa0/0
	Fa1/1	209.165.201.1	/28	-	1	PC-Internet Fa0
Kostiuchenko_ Switch_0	VLAN1	172.24.161.2	/25	172.24.161.1	1	-
Kostiuchenko_ Switch_1	VLAN1	172.24.161.3	/25	172.24.161.1	1	-
Kostiuchenko_ Switch_2	VLAN1	172.24.161.4	/25	172.24.161.1	1	-
Kostiuchenko_ Switch_3	VLAN99	172.24.161.226	/27	172.24.161.225	99	-
Kostiuchenko_ Switch_4	VLAN99	172.24.161.227	/27	172.24.161.225	99	-

Продовження таблиці 3.3

Kostiuchenko_ Switch_5	VLAN99	172.24.161.228	/27	172.24.161.225	99	-
Kostiuchenko_ Switch_6	VLAN1	172.24.160.2	/24	172.24.160.1	1	-
Kostiuchenko_ Switch_7	VLAN1	172.24.162.66	/27	172.24.162.65	1	-
Kostiuchenko_ Switch_8	VLAN1	172.24.162.2	/26	172.24.162.1	1	-
Server_DNS	Fa0	172.24.162.22	/26	172.24.162.1	1	Kostiuchenko_ Switch_8 Fa0/24
Server_HTTP	Fa0	172.24.162.23	/26	172.24.162.1	1	Kostiuchenko_ Switch_8 Fa0/23
Server_IoT	Fa0	172.24.162.24	/26	172.24.162.1	1	Kostiuchenko_ Switch_8 Fa0/22
Server_TFTP	Fa0	172.24.161.22	/25	172.24.161.1	1	Kostiuchenko_ Switch_1 G0/2
Guest_Wireless _Router	Internet	172.24.161.194	/27	172.24.161.193	42	Kostiuchenko_ Switch_5 Fa0/15
Home_Gatewa y	Internet	172.24.162.66	/27	172.24.162.65	1	Kostiuchenko_ Switch_7 Fa0/1

Початковим кроком у процесі налаштування створюваної мережевої інфраструктури є конфігурація базових параметрів пристроїв. Зокрема, це встановлення імені пристрою, конфігурація паролів доступу з їх шифруванням, створення банеру привітання, реєстрація локального користувача, а також активація захищеного віддаленого доступу за допомогою протоколу SSH.

Такі початкові налаштування виконуються для кожного маршрутизатора в мережі, оскільки вони забезпечують базовий рівень безпеки та адміністрування. Усі конфігурації мають схожий характер, тому нижче наводиться приклад для одного з пристроїв – Kostiuchenko_Router_0.

```
enable
conf t
hostname Kostiuchenko_Router_0
```

banner motd 'Warning! Access restricted. Kostiuchenko only!'

line console 0

password cisco

login

line vty 0 15

password cisco

transport input ssh

login local

exit

enable secret class

service password-encryption

ip domain-name Kostiuchenko_Router_0

crypto key generate rsa

1024

username 123211_Kostiuchenko password admincisco

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Kostiuchenko_Router0
Kostiuchenko_Router0(config)#banner motd 'Warning! Access restricted. Kostiuchenko only!'
Kostiuchenko_Router0(config)#line console 0
Kostiuchenko_Router0(config-line)#password cisco
Kostiuchenko_Router0(config-line)#login
Kostiuchenko_Router0(config-line)#line vty 0 15
Kostiuchenko_Router0(config-line)#password cisco
Kostiuchenko_Router0(config-line)#login
Kostiuchenko_Router0(config-line)#enable secret class
Kostiuchenko_Router0(config)#service password-encryption
Kostiuchenko_Router0(config)#ip domain-name Kostiuchenko_Router
Kostiuchenko_Router0(config)#crypto key generate rsa
The name for the keys will be: Kostiuchenko_Router0.Kostiuchenko_Router
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Kostiuchenko_Router0(config)#username 123211_Kostiuchenko password admincisco
*Mar 1 1:27:55.409: %SSH-5-ENABLED: SSH 1.99 has been enabled
Kostiuchenko_Router0(config)#line vty 0 15
Kostiuchenko_Router0(config-line)#transport input ssh
Kostiuchenko_Router0(config-line)#login local
```

Рисунок 3.2 – Базові налаштування Kostiuchenko_Router_0

Для перевірки функціонування протоколу SSH, що забезпечує захищений віддалений доступ до мережевого обладнання, було виконано підключення з

командного рядка комп'ютера PC10, розміщеного в підмережі LAN3, до маршрутизатора Kostiuchenko_Router_0. Для доступу використовувався обліковий запис користувача 123211_Kostiuchenko із паролем admincisco.

Після виконання команди ssh -l система запитує пароль. Введення пароля admincisco завершує процес автентифікації, надаючи доступ до конфігурації маршрутизатора. Таким чином, була успішно перевірена працездатність SSH-підключення, що підтверджує коректність налаштувань та готовність обладнання до безпечного віддаленого адміністрування (див. рисунок 3.3).

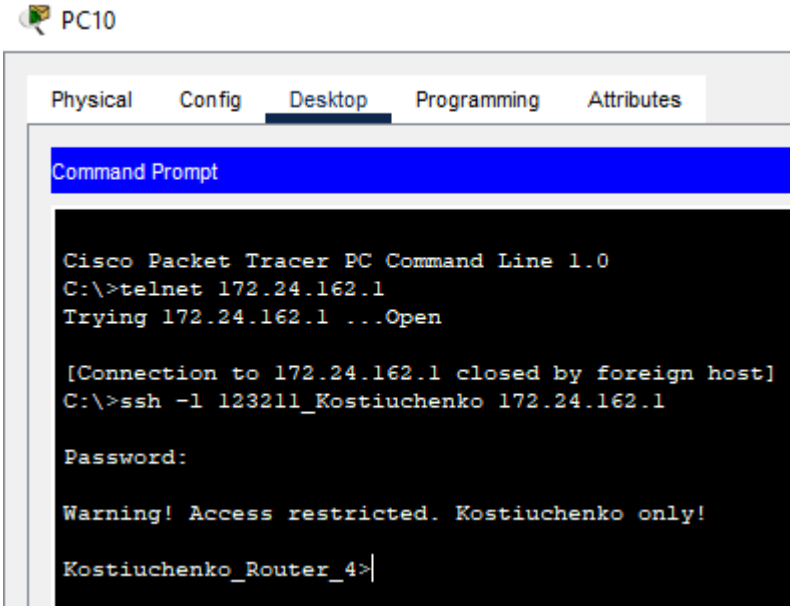


Рисунок 3.3 – Перевірка підключення до маршрутизатора Kostiuchenko_Router_0 за SSH

Як зображено на рисунку 3.4, згідно завдання необхідно на DCE-інтерфейсах маршрутизаторів призначити встановлення значення тактової частоти – 128000. Виконаємо налаштування на Kostiuchenko_ISP.

```
Kostiuchenko_ISP(config-if)#clock rate 128000
Kostiuchenko_ISP(config-if)#ip address 209.165.202.1 255.255.255.0
Kostiuchenko_ISP(config-if)#
```

Рисунок 3.4 – Налаштування пропускної здатності та метрики маршрутів

Також було виконано налаштування з'єднань між мережевими пристроями для забезпечення стабільного обміну даними. Задіяно

функціональні можливості для об’єднання каналів та оптимізації взаємодії між ключовими елементами мережі (див. рисунки 3.5, 3.6). Такі дії спрямовані на підвищення надійності та ефективності роботи інфраструктури.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range f0/1-4
Switch(config-if-range)#switchport mode trunk



Switch(config-if-range)#switchport nonegotiate
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
```

Рисунок 3.5 – Налаштування транкових каналів для агрегації на комутаторі

```
Kostiuchenko_Switch_3(config)#interface range f0/1-2
Kostiuchenko_Switch_3(config-if-range)#shutdown


Kostiuchenko_Switch_3(config-if-range)#channel-group 1 mode desirable
Kostiuchenko_Switch_3(config-if-range)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

Creating a port-channel interface Port-channel 1



Kostiuchenko_Switch_3(config-if-range)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```

Рисунок 3.6 – Налаштування агрегації каналів на комутаторі

3.3.2 Налаштування маршрутизаторів КФС (OSPF)

На цьому етапі виконано налаштування маршрутизаторів, які забезпечують зв'язок між підмережами кіберфізичної системи та відповідають за обробку й переспрямування трафіку згідно з конфігурацією. Основна мета налаштувань – забезпечити базову маршрутизацію, необхідну для міжмережевої комунікації, а також впровадити базову модель автентифікації користувачів для підвищення рівня безпеки доступу до пристроїв (див.

рисунок 3.7).

enable

configure terminal

route ospf 12

network 10.1.12.4 0.0.0.3 area 0

network 10.1.12.8 0.0.0.3 area 0

network 10.1.12.20 0.0.0.3 area 0

network 172.24.162.64 0.0.0.31 area 0

passive-interface f1/1

```
router ospf 12
 log-adjacency-changes
 passive-interface FastEthernet1/1
 network 10.1.12.4 0.0.0.3 area 0
 network 10.1.12.8 0.0.0.3 area 0
 network 10.1.12.20 0.0.0.3 area 0
 network 172.24.162.64 0.0.0.31 area 0
```

Рисунок 3.7 – Налаштування маршрутизації на Kostiuchenko_Router_1

На кожному маршрутизаторі виконано базову конфігурацію інтерфейсів, встановлено IP-адреси відповідно до підмереж, визначених у попередньому пункті. Для підтримки централізованої автентифікації та контролю доступу реалізовано налаштування елементів AAA (Authentication, Authorization, Accounting). Це дозволяє відслідковувати підключення до маршрутизаторів та управляти доступом до привілейованих режимів, що проілюстровано на рисунку 3.8, де показано налаштований сервіс на сервері DNS.

aaa new-model

aaa authentication login default group radius local

radius server Kostiuchenko_AAA

address ipv4 172.24.162.22

key radius123

exit

no radius server 172.24.162.22

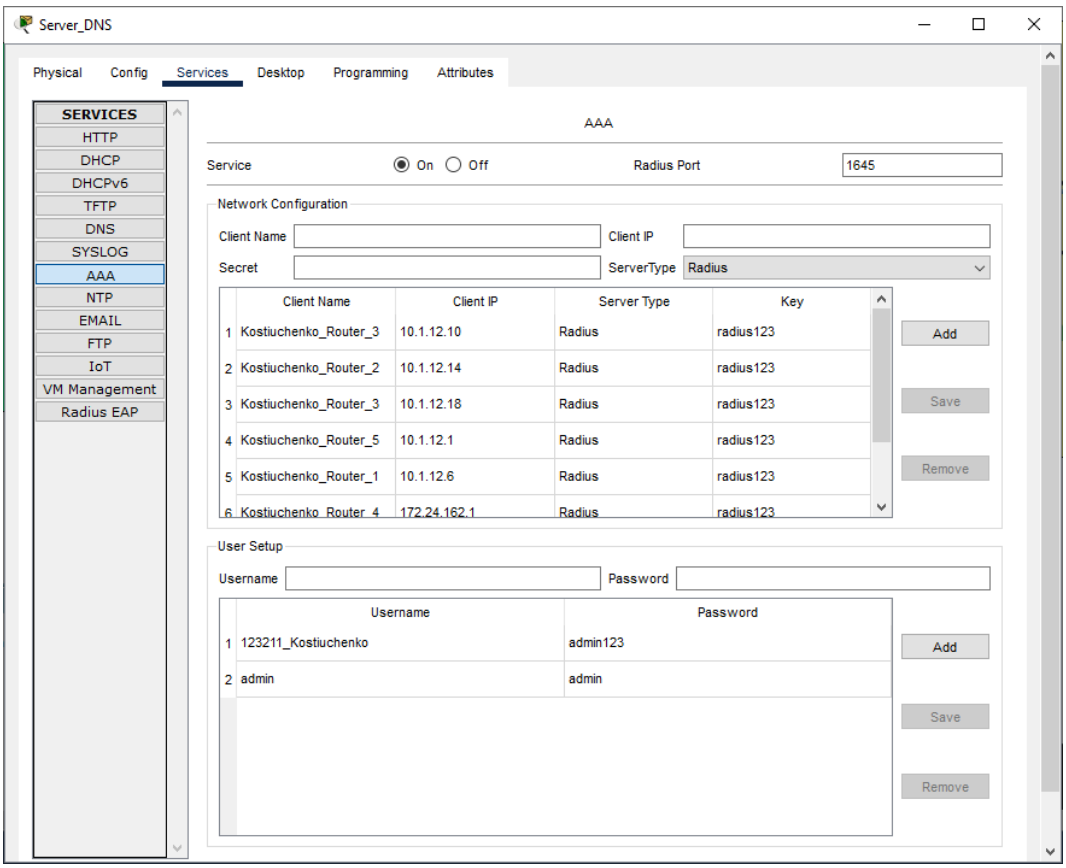


Рисунок 3.8 – Налаштований сервіс на сервері DNS

3.3.3 Розподіл пристроїв по VLAN та ізоляція трафіку

З метою підвищення безпеки, оптимізації трафіку та логічного структурування мережевої інфраструктури в моделі кіберфізичної системи реалізовано сегментацію мережі за допомогою віртуальних локальних мереж (VLAN). Такий підхід дозволяє розділити користувачів та пристрої за функціональним призначенням, що спрощує адміністрування та обмежує небажану взаємодію між підсистемами.

Всі пристрої локальної мережі LAN1 було розподілено між кількома VLAN відповідно до логіки організації: обліковий відділ, аналітичний підрозділ, гостьовий доступ, адміністративний сегмент тощо. Для кожної VLAN на комутаторах створено відповідні записи, налаштовано порти в режимі access, а для з'єднань між комутаторами – порти в режимі trunk, які забезпечують передачу трафіку кількох VLAN одночасно. Приклад налаштування VLAN показано на рисунку 3.9.

```
Kostiuchenko_Switch_3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Kostiuchenko_Switch_3(config)#vlan 22
Kostiuchenko_Switch_3(config-vlan)#name Accounting
Kostiuchenko_Switch_3(config-vlan)#vlan 32
Kostiuchenko_Switch_3(config-vlan)#name Resources_Department
Kostiuchenko_Switch_3(config-vlan)#vlan 42
Kostiuchenko_Switch_3(config-vlan)#name Guest
Kostiuchenko_Switch_3(config-vlan)#vlan 99
Kostiuchenko_Switch_3(config-vlan)#name Management
Kostiuchenko_Switch_3(config-vlan)#vlan 100
Kostiuchenko_Switch_3(config-vlan)#name Native
Kostiuchenko_Switch_3(config-vlan)#interface range f0/5-9
Kostiuchenko_Switch_3(config-if-range)#switchport mode access
Kostiuchenko_Switch_3(config-if-range)#switchport access vlan 22
Kostiuchenko_Switch_3(config-if-range)#interface range f0/15-24
Kostiuchenko_Switch_3(config-if-range)#switchport mode access
Kostiuchenko_Switch_3(config-if-range)#switchport access vlan 32
Kostiuchenko_Switch_3(config-if-range)#interface range f0/10-14
Kostiuchenko_Switch_3(config-if-range)#switchport mode access
Kostiuchenko_Switch_3(config-if-range)#switchport access vlan 42
Kostiuchenko_Switch_3(config-if-range)#
Kostiuchenko_Switch_3(config-if-range)#interface range f0/1-4, g0/1
Kostiuchenko_Switch_3(config-if-range)#switchport mode trunk

Kostiuchenko_Switch_3(config-if-range)#switchport trunk allowed vlan all
Kostiuchenko_Switch_3(config-if-range)#switchport trunk native vlan 100
Kostiuchenko_Switch_3(config-if-range)#no shutdown
%LINK-3-UPDOWN: Interface Port-channel1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to down

%LINK-3-UPDOWN: Interface Port-channel2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

Рисунок 3.9 – Приклад налаштування VLAN на комутаторі

Таким чином, впровадження VLAN у підмережі LAN1 дозволило ефективно розмежувати логічні сегменти мережі відповідно до функціонального призначення користувачів та пристроїв. Це підвищило рівень безпеки, спростило адміністрування та дало змогу реалізувати гнучке управління доступом до ресурсів мережі (див. рисунок 3.10).

Завдяки налаштуванню режимів access і trunk на портах комутаторів забезпечено стабільну передачу трафіку між сегментами, що позитивно впливає на продуктивність та надійність роботи кіберфізичної системи.

```
Kostiuchenko_Router_2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Kostiuchenko_Router_2(config)#ip dhcp excluded-address 172.24.161.129 172.24.161.134
Kostiuchenko_Router_2(config)#ip dhcp excluded-address 172.24.161.161 172.24.161.166
Kostiuchenko_Router_2(config)#ip dhcp excluded-address 172.24.161.193 172.24.161.198
Kostiuchenko_Router_2(config)#ip dhcp excluded-address 172.24.161.225 172.24.161.230
Kostiuchenko_Router_2(config)#
Kostiuchenko_Router_2(config)#interface f1/0.22
Kostiuchenko_Router_2(config-subif)#encapsulation dot1Q 22
Kostiuchenko_Router_2(config-subif)#ip address 172.24.161.129 255.255.255.224
Kostiuchenko_Router_2(config-subif)#interface f1/0.32
Kostiuchenko_Router_2(config-subif)#encapsulation dot1Q 32
Kostiuchenko_Router_2(config-subif)#ip address 172.24.161.161 255.255.255.224
Kostiuchenko_Router_2(config-subif)#interface f1/0.42
Kostiuchenko_Router_2(config-subif)#encapsulation dot1Q 42
Kostiuchenko_Router_2(config-subif)#ip address 172.24.161.193 255.255.255.224
Kostiuchenko_Router_2(config-subif)#interface f1/0.99
Kostiuchenko_Router_2(config-subif)#encapsulation dot1Q 99
Kostiuchenko_Router_2(config-subif)#ip address 172.24.161.225 255.255.255.224
%LINK-5-CHANGED: Interface FastEthernet1/0.22, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0.22, changed state to up

%LINK-5-CHANGED: Interface FastEthernet1/0.32, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0.32, changed state to up

%LINK-5-CHANGED: Interface FastEthernet1/0.42, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0.42, changed state to up

%LINK-5-CHANGED: Interface FastEthernet1/0.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0.99, changed state to up
```

Рисунок 3.10 – Налаштування маршрутизації між VLAN

Виконано налаштування міжвіртуальної маршрутизації для кількох VLAN на маршрутизаторі за допомогою підінтерфейсів. Для кожного з них задано відповідний ідентифікатор VLAN через команду encapsulation dot1Q, а також IP-адресу для взаємодії з пристроями в межах відповідного сегмента. Крім того, зарезервовано певні діапазони IP-адрес для виключення з DHCP-пула, щоб уникнути конфліктів з адресами, призначеними підінтерфейсам.

На рисунку нижче наведено перевірку за допомогою echo-запитів між VLAN.

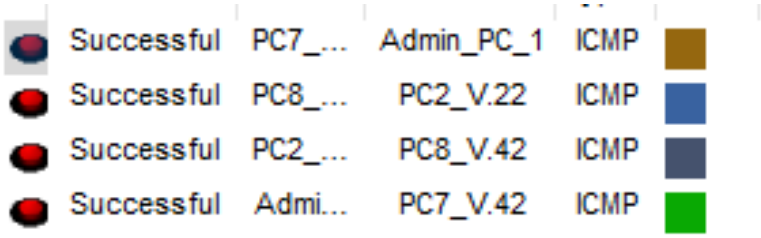


Рисунок 3.11 – Перевірка досяжності між ПК в VLAN

3.3.4 Забезпечення доступу до зовнішньої мережі (Інтернет)

Одним із ключових етапів під час налаштування мережевої інфраструктури є організація стабільного доступу до зовнішньої мережі. Такий доступ необхідний для функціонування службових ресурсів, взаємодії з адміністративними платформами та для забезпечення можливостей віддаленого керування мережею.

У моделі кіберфізичної системи було передбачено підключення до Інтернету через прикордонний маршрутизатор, який виконує роль шлюзу для всієї внутрішньої мережі. Вихідний інтерфейс цього маршрутизатора з’єднано з мережею провайдера, що моделює зовнішнє середовище.

З метою безпечного адміністрування та забезпечення захищеного віддаленого доступу, у роботі передбачається реалізація VPN-з'єднання (рисунок 3.12). Такий підхід дозволяє адміністраторам та сервісним працівникам здійснювати доступ до внутрішніх вузлів із зовнішньої мережі без ризику перехоплення трафіку. VPN-тунель створює зашифроване з'єднання між віддаленим клієнтом та маршрутизатором, унеможливлюючи несанкціоноване втручання ззовні.

```
Kostiuchenko_Router_0(config)#no access-list 112
Kostiuchenko_Router_0(config)#access-list 112 permit ip 172.24.161.0 0.0.0.127 10.1.12.0 0.0.0.255
Kostiuchenko_Router_0(config)#access-list 112 permit ip 172.24.161.0 0.0.0.127 172.24.160.0 0.0.0.255
Kostiuchenko_Router_0(config)#access-list 112 permit ip 172.24.161.0 0.0.0.127 172.24.161.128 0.0.0.127
Kostiuchenko_Router_0(config)#access-list 112 permit ip 172.24.161.0 0.0.0.127 172.24.162.0 0.0.0.127
Kostiuchenko_Router_0(config)#access-list 112 permit ip 172.24.161.0 0.0.0.127 host 209.165.202.2
Kostiuchenko_Router_0(config)#
Kostiuchenko_Router_0(config)#crypto isakmp policy 10
Kostiuchenko_Router_0(config-isakmp)#authentication pre-share
Kostiuchenko_Router_0(config-isakmp)#encryption aes 256
Kostiuchenko_Router_0(config-isakmp)#group 5
Kostiuchenko_Router_0(config-isakmp)#exit
Kostiuchenko_Router_0(config)#crypto isakmp key Kostiuchenko123211 address 209.165.202.2
Kostiuchenko_Router_0(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
Kostiuchenko_Router_0(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Kostiuchenko_Router_0(config-crypto-map)#desc VPN Connect
Kostiuchenko_Router_0(config-crypto-map)#set peer 209.165.202.2
Kostiuchenko_Router_0(config-crypto-map)#set pfs group5
Kostiuchenko_Router_0(config-crypto-map)#set security-association lifetime seconds 86400
Kostiuchenko_Router_0(config-crypto-map)#set transform-set VPN-SET
Kostiuchenko_Router_0(config-crypto-map)#match address 112
Kostiuchenko_Router_0(config-crypto-map)#exit
Kostiuchenko_Router_0(config)#int f0/0
Kostiuchenko_Router_0(config-if)#crypto map VPN-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Рисунок 3.12 – Налаштування VPN на роутері Kostiuchenko_Router_0

Для забезпечення доступу до Інтернету був налаштований сервіс DNS на

сервері. Налаштування включало активацію DNS-сервісу та додавання необхідних записів ресурсів для коректної роботи.

Був доданий запис для доменного імені "123.dnipro.ua", який вказує на IP-адресу 172.24.162.23, яка відноситься до HTTP-серверу (див. рисунок 3.13).

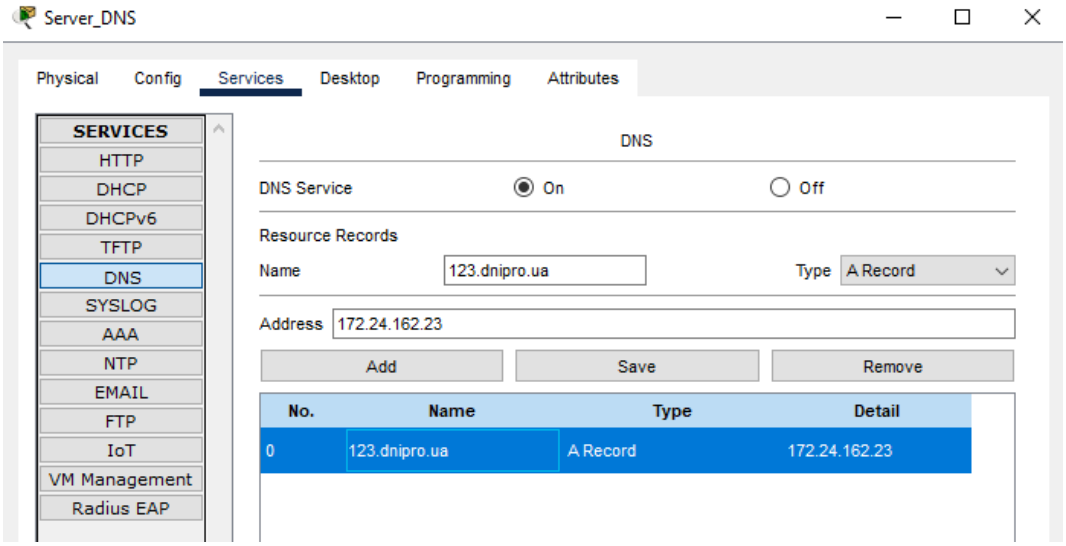


Рисунок 3.13 – Налаштований сервіс DNS

Як зображено на рисунку 3.14, для забезпечення безпечного з’єднання на сервері HTTP був залишений лише протокол HTTPS, який є більш безпечним відносно протоколу HTTP.

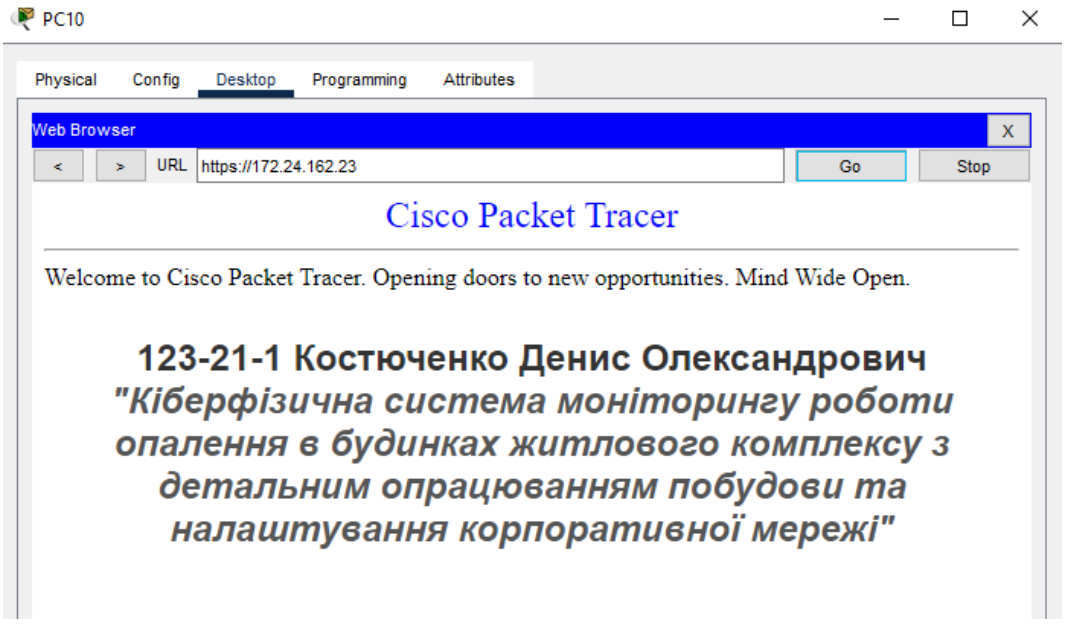


Рисунок 3.14 – Робота HTTP та DNS серверів

Як видно на рисунку 3.15, налаштування HTTP-серверу працюють

корректно.

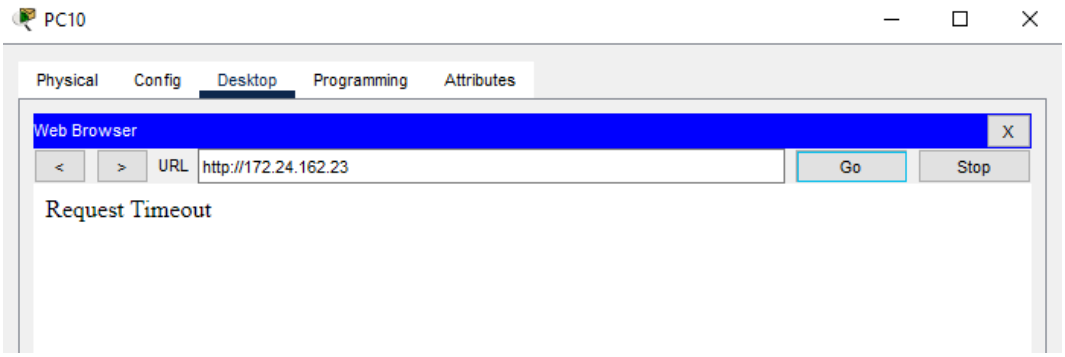


Рисунок 3.15 – Невдала спроба з’єднання через протокол HTTP

3.3.5 Організація безпеки мережі (ACL,NAT, DHCP захист)

На прикордонному маршрутизаторі Kostiuchenko_Router_5 було налаштовано протокол NAT відповідно до вимог роботи. Основна мета – забезпечити трансляцію внутрішніх IP-адрес житлового комплексу, що належать до діапазону 172.24.160.0/21, у зовнішні глобальні адреси з виділеного пулу 209.165.202.5 – 209.165.202.30.

Для реалізації трансляції було створено пул з іменем Internet, до якого включено глобальні адреси з зазначеного діапазону. Окрім динамічного NAT для клієнтів внутрішньої мережі, також передбачено статичну трансляцію для критичних служб:

HTTP-сервер: 172.24.162.23/26

DNS-сервер: 172.24.162.22/26

Доступ до трансляції контролюється за допомогою списку доступу №12, який визначає допустимі джерела трафіку для NAT-перетворення. Налаштування NAT, детальне представлення якого можна побачити на рисунку 3.16, забезпечує як зовнішній доступ клієнтам внутрішньої мережі, так і можливість підключення до публічно доступних серверів, при цьому зберігаючи структурованість та безпеку адресного простору.

```
Warning! Access restricted. Kostiuchenko only!

User Access Verification

Username: admin
Password:

Kostiuchenko_Router_5>en
Password:
Kostiuchenko_Router_5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Kostiuchenko_Router_5(config)#int f0/0
Kostiuchenko_Router_5(config-if)#ip nat inside
Kostiuchenko_Router_5(config-if)#int f0/1
Kostiuchenko_Router_5(config-if)#ip nat inside
Kostiuchenko_Router_5(config-if)#int f1/0
Kostiuchenko_Router_5(config-if)#ip nat inside
Kostiuchenko_Router_5(config-if)#int s0/0/0
Kostiuchenko_Router_5(config-if)#ip nat outside
Kostiuchenko_Router_5(config-if)#
```

Рисунок 3.16 – Налаштування NAT на роутері Kostiuchenko_Router_5

Нижче наведено команди для налаштування динамічного NAT.

access-list 12 permit 172.24.160.0 0.0.7.255

ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224

ip nat inside source list 12 pool Internet

ip nat inside source static 172.24.162.23 209.165.200.4

ip nat inside source static 172.24.162.22 209.165.200.3

Після конфігурації мережевої адресної трансляції (NAT) була проведена перевірка для підтвердження її коректної роботи та забезпечення доступу внутрішніх пристроїв до зовнішньої мережі.

Були зафіксовані активні трансляції, що демонструють успішне відображення внутрішніх приватних IP-адрес (наприклад, з 172.24.160.x та 172.24.162.x) на зовнішні публічні адреси з пулу (зокрема, з 209.165.200.x). Спостерігалися як динамічні трансляції для загального трафіку, так і статичні відображення для конкретних пристроїв (наприклад, 172.24.162.22 на 209.165.200.3 та 172.24.162.23 на 209.165.200.4). Це підтвердило правильність налаштувань NAT та його ефективну роботу (рисунок 3.17).

```
Kostiuchenko_Router_5#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.10:1  172.24.160.249:1   209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.11:1  172.24.160.254:1   209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.12:1  172.24.160.252:1   209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.6:3   172.24.162.60:3    209.165.201.5:3    209.165.201.5:3
icmp 209.165.200.7:4   172.24.162.61:4    209.165.201.5:4    209.165.201.5:4
icmp 209.165.200.8:1   172.24.162.62:1    209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.9:3   172.24.160.247:3   209.165.201.5:3    209.165.201.5:3
---  209.165.200.3     172.24.162.22      ---                ---
---  209.165.200.4     172.24.162.23      ---                ---
```

Рисунок 3.17 – Перевірка налаштувань NAT на роутері Kostiuchenko_Router_5

Для ефективного розподілу трафіку в межах підмережі LAN1 (офісна мережа) реалізовано логічну сегментацію на основі віртуальних локальних мереж (VLAN) (див. таблиця 3.4), що дозволяє ізолювати дані між різними групами користувачів. Налаштування виконано на трьох комутаторах: Kostiuchenko_Switch_3, Kostiuchenko_Switch_4 та Kostiuchenko_Switch_5.

Комутатори Switch4 та Switch5 працюють у режимі access, тобто до них підключаються кінцеві пристрої, які належать до певних VLAN:

Таблиця 3.4 – Назви VLAN в підмережі

№ VLAN	Назва VLAN	Примітка
1	default	Не використовується
22	Accounting	Бухгалтерія
32	Resources Department	Відділ кадрів
42	Guest	Гостьовий доступ
99	Management	Керування пристроями
100	Native	Власна

Комутатор Kostiuchenko_Switch_3 виконує функцію магістрального (trunk) пристрою, через який передається трафік усіх VLAN до маршрутизатора Kostiuchenko_Router_2 для подальшої маршрутизації між сегментами.

У підмережах житлового комплексу DHCP-сервіс реалізовано на маршрутизаторі Kostiuchenko_Router_2, який автоматично роздає мережеві

налаштування TCP/IP клієнтським пристроям у сегменті LAN1. Це значно спрощує адміністрування мережі та дозволяє уникнути ручного налаштування параметрів на кожному вузлі та зменшує ризик конфігураційних помилок.

Для підмережі LAN1 додатково передбачено логічний поділ на кілька віртуальних мереж (VLAN), відповідно до функціональних груп користувачів. Кожен VLAN має власний пул IP-адрес, що дозволяє не лише ізолювати трафік між підрозділами, а також забезпечує гнучке управління доступом до ресурсів. DHCP-пул конфігурується з урахуванням специфіки кожної групи, забезпечуючи оптимальне використання адресного простору та підвищення рівня безпеки в межах підмережі.

На рисунку 3.18 зображено приклад налаштування DHCP на роутері Kostiuchenko_Router_2.

```
Kostiuchenko_Router_2(config)#ip dhcp pool VLAN22
Kostiuchenko_Router_2(dhcp-config)#net 172.24.161.128 255.255.255.224
Kostiuchenko_Router_2(dhcp-config)#def 172.24.161.129
Kostiuchenko_Router_2(dhcp-config)#dns 172.24.162.22
Kostiuchenko_Router_2(dhcp-config)#ip dhcp pool VLAN32
Kostiuchenko_Router_2(dhcp-config)#net 172.24.161.160 255.255.255.224
Kostiuchenko_Router_2(dhcp-config)#def 172.24.161.161
Kostiuchenko_Router_2(dhcp-config)#dns 172.24.162.22
Kostiuchenko_Router_2(dhcp-config)#ip dhcp pool VLAN42
Kostiuchenko_Router_2(dhcp-config)#net 172.24.161.192 255.255.255.224
Kostiuchenko_Router_2(dhcp-config)#def 172.24.161.193
Kostiuchenko_Router_2(dhcp-config)#dns 172.24.162.22
Kostiuchenko_Router_2(dhcp-config)#ip dhcp pool VLAN99
Kostiuchenko_Router_2(dhcp-config)#net 172.24.161.224 255.255.255.224
Kostiuchenko_Router_2(dhcp-config)#def 172.24.161.225
Kostiuchenko_Router_2(dhcp-config)#dns 172.24.162.22
```

Рисунок 3.18 – Налаштування DHCP

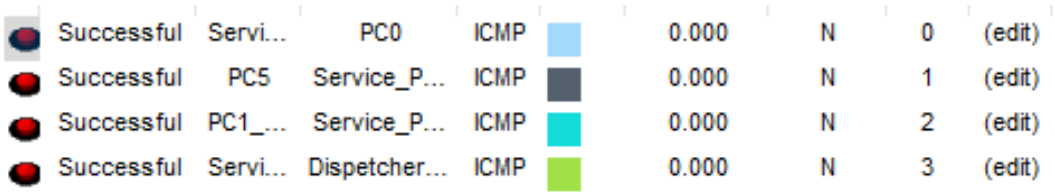
Кожній VLAN було призначено окремий діапазон IP-адрес, а також реалізовано маршрутизацію між ними за допомогою підінтерфейсів на відповідному маршрутизаторі. Це дозволяє забезпечити контрольовану взаємодію між логічними сегментами без потреби у фізичному розділенні обладнання.

Ізоляція трафіку між VLAN реалізована шляхом обмеження маршрутизації або за допомогою списків контролю доступу (ACL), що дозволяє запобігти несанкціонованому обміну даними між окремими

підрозділами. Це особливо важливо в середовищах, де одночасно функціонують користувацькі ПК, сервери, службове обладнання та IoT-пристрої.

3.4 Перевірка працездатності комп'ютерної мережі

Виконання команди ping між пристроями з різних підмереж комп'ютерної системи підтверджує коректну взаємодію всередині мережі, як показано на рис. 3.19. Також успішно проведено перевірку доступу до зовнішніх ресурсів з боку хостів корпоративної мережі. Це свідчить про правильність налаштування маршрутизації та наявність стабільного з'єднання з Інтернетом.



Successful	Servi...	PC0	ICMP	0.000	N	0	(edit)
Successful	PC5	Service_P...	ICMP	0.000	N	1	(edit)
Successful	PC1_...	Service_P...	ICMP	0.000	N	2	(edit)
Successful	Servi...	Dispetcher...	ICMP	0.000	N	3	(edit)

Рисунок 3.19 – Результат команди «ping»

```
Kostiuchenko_Router_5(config-ext-nacl)#do 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 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C       10.1.12.0/30 is directly connected, FastEthernet0/0
L       10.1.12.1/32 is directly connected, FastEthernet0/0
O       10.1.12.4/30 [110/2] via 10.1.12.2, 00:38:27, FastEthernet0/0
                     [110/2] via 10.1.12.22, 00:38:27, FastEthernet0/1
O       10.1.12.8/30 [110/2] via 10.1.12.22, 00:38:27, FastEthernet0/1
                     [110/2] via 10.1.12.18, 00:38:27, FastEthernet1/0
O       10.1.12.12/30 [110/2] via 10.1.12.18, 00:38:27, FastEthernet1/0
C       10.1.12.16/30 is directly connected, FastEthernet1/0
L       10.1.12.17/32 is directly connected, FastEthernet1/0
C       10.1.12.20/30 is directly connected, FastEthernet0/1
L       10.1.12.21/32 is directly connected, FastEthernet0/1
 --More--
```

Рисунок 3.20 – Перевірка налаштувань OSPF

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Структура та компоненти IoT-системи кіберфізичної системи

Ключовою частиною реалізованої кіберфізичної системи моніторингу опалення є підсистема Інтернету речей (IoT), що виконує функції локального збору даних, первинної обробки та передачі до серверної інфраструктури. Її структура базується на моделі розміщення пристроїв у межах окремого житлового приміщення, яке представляє один з вузлів розподіленої архітектури КФС.

Фізичний рівень підсистеми складається з кількох сенсорів температури та вологості, встановлених у функціональних зонах квартири (наприклад, кухня, спальня, вітальня). Один із сенсорів температури розташований зовні приміщення, що дозволяє враховувати зовнішній тепловий вплив у процесах керування опаленням. Сенсори з’єднані з мікроконтролером MCU типу ESP32, який виступає центральним вузлом збору та попередньої обробки даних. До нього також підключені виконавчі пристрої – обігрівачі (Furnace IoT), які активуються на основі встановлених сценаріїв.

Усі дані зчитуються в аналоговому вигляді, перетворюються в реальні фізичні показники та одразу аналізуються на рівні MCU. Після кожного циклу збору інформації мікроконтролер передає зведені дані до шлюзу за допомогою внутрішньої мережі. Шлюз забезпечує інтеграцію локального сегмента з серверною частиною КФС, передаючи інформацію на IoT-сервер.

Загальна схема реалізації представлена на рисунку 4.1. На ній відображено логічні зв’язки між сенсорами, мікроконтролером, виконавчими пристроями, шлюзом та сервером, а також умовну взаємодію з хмарною інфраструктурою.

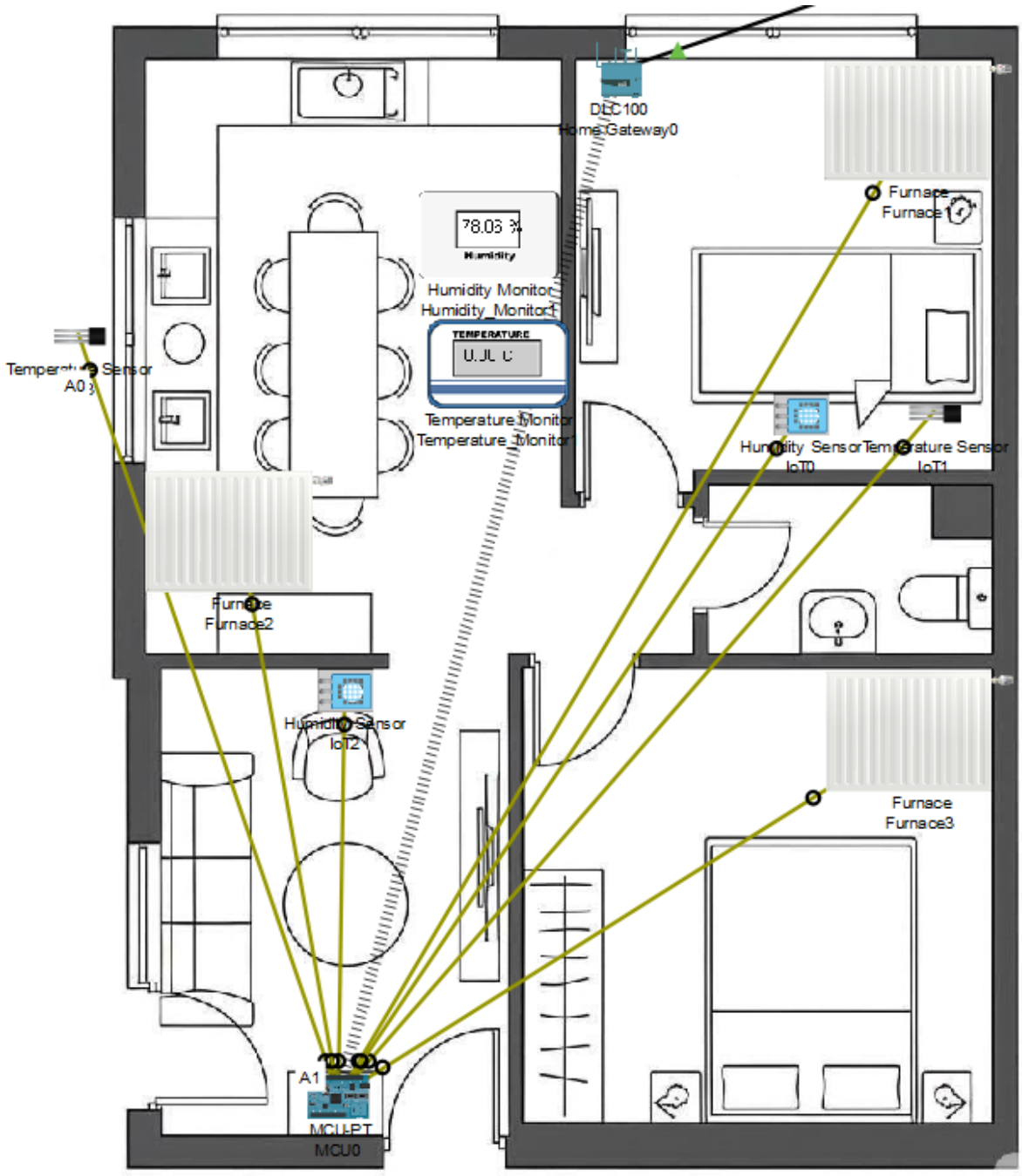


Рисунок 4.1 – План розміщення пристроїв у житловому приміщенні

Така побудова дозволяє масштабувати архітектуру на інші квартири та приміщення без істотної зміни логіки. Кожен житловий вузол працює як автономний агент з власним MCU, який виконує функції локального збору та контролю, забезпечуючи гнучкість і адаптивність всієї кіберфізичної системи

4.2 Функції кіберфізичної системи житлового комплексу

У цьому розділі розглянуто типові сценарії взаємодії елементів кіберфізичної системи у повсякденній роботі. Це дозволяє не лише підтвердити функціональність КФС, але й продемонструвати реальні переваги її використання для мешканців та адміністрації житлового комплексу.

– Сценарій 1: Автоматичне регулювання опалення

У разі зниження температури в житловому приміщенні нижче порогового значення, мікроконтролер активує відповідні обігрівачі. Якщо температура зростає – пристрої вимикаються, щоб зекономити енергію.

– Сценарій 2: Критичне перевищення температури

Коли одна з батарей увімкнена, але температура повітря перевищує 35 °C, система розпізнає аномальну ситуацію та примусово вимикає всі обігрівачі. Це запобігає перегріву, підвищує безпеку та комфорт.

– Сценарій 3: Зовнішній моніторинг та аварійні сповіщення

MCU передає дані про температуру, вологість і стан обладнання на IoT-сервер. У разі виявлення відхилень система надсилає сповіщення диспетчерам або мешканцям через панель візуалізації.

– Сценарій 4: Інтеграція з хмарними сервісами

Сервер обробки може перенаправляти отримані від MCU дані до хмарної платформи, де вони архівуються, аналізуються та можуть бути використані для довгострокової статистики або оптимізації теплових алгоритмів.

Послідовність логіки реагування системи проілюстровано на рисунку 4.2.

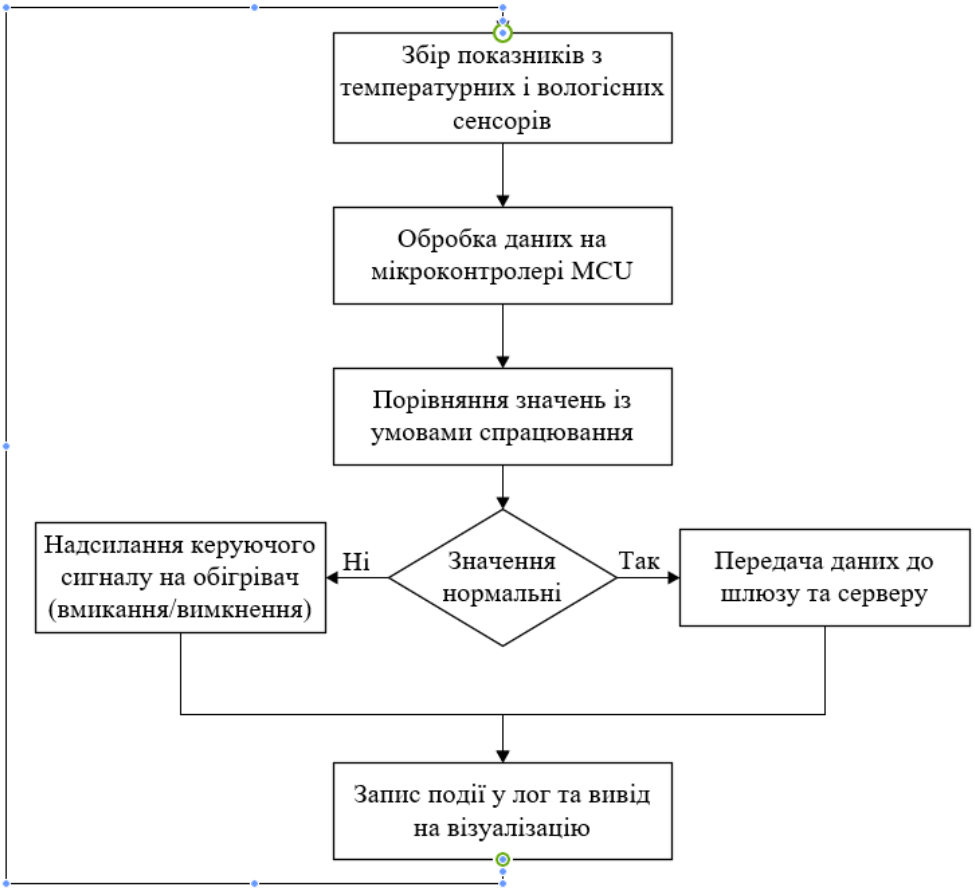


Рисунок 4.2 – Послідовність логіки реагування

4.3 Реалізація хмарних та туманних обчислень у кіберфізичній системі

У межах кіберфізичної системи житлового комплексу впроваджено комбіновану архітектуру, що поєднує туманні обчислення на рівні житлових приміщень із хмарною логікою на серверному рівні. Такий підхід забезпечує як локальну автономність, так і централізований моніторинг із можливістю віддаленого втручання у разі потреби.

Для реалізації хмарних обчислень у даній КФС спочатку необхідно додати запис DNS, що вказує на ваш налаштований IoT-сервер (рисунок 4.3). Це дозволить пристроям у мережі знаходити та взаємодіяти з IoT-сервером, забезпечуючи централізоване керування та збір даних.

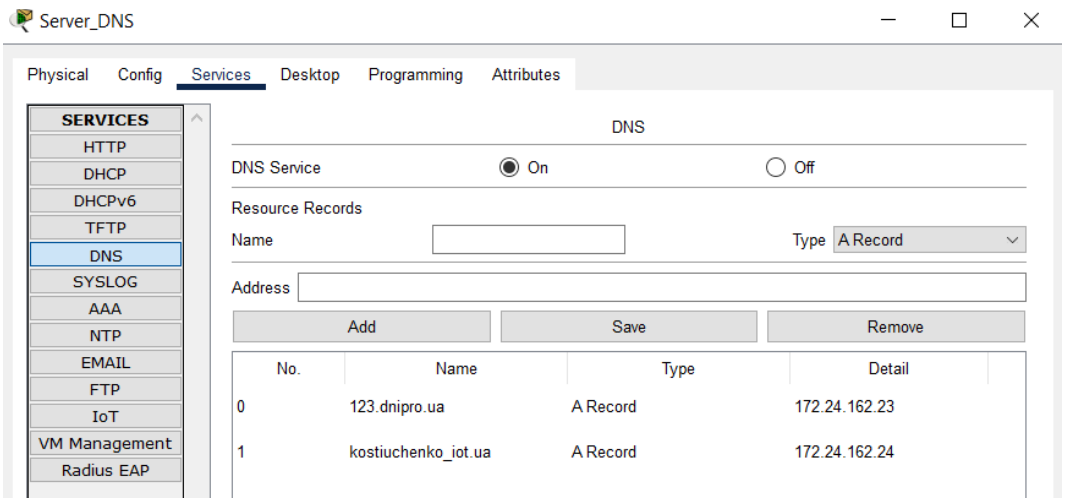


Рисунок 4.3 – Додавання налаштованого IoT серверу до DNS – серверу

Наступним кроком реєструємо нового користувача через Web-інтерфейс з будь-якого кінцевого пристрою. Приклад створення наведено на рисунку 4.4

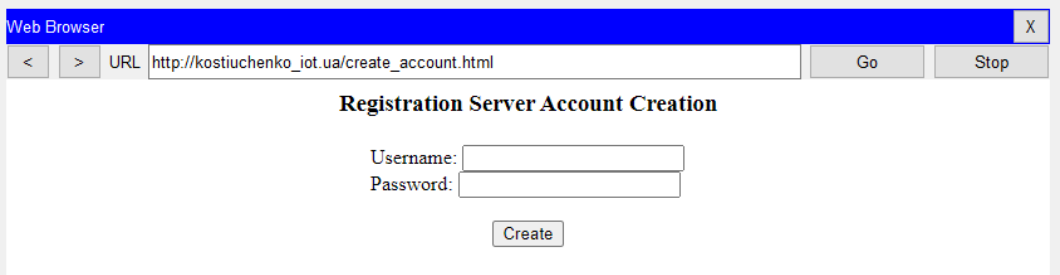


Рисунок 4.4 – Створення аккаунту на сервері

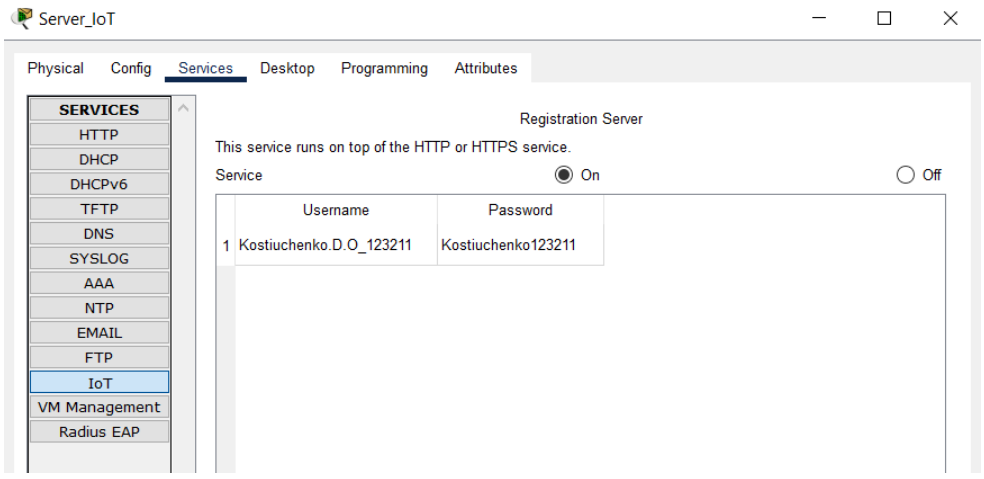


Рисунок 4.5 – Створений аккаунт на сервері IoT

У мережеву топологію було інтегровано пристрої Інтернету речей, після чого виконано налаштування маршрутизації для забезпечення їх взаємодії з іншими підсистемами. У ролі IoT-сервера виступає віддалений сервер,

підключений до відповідної підмережі.

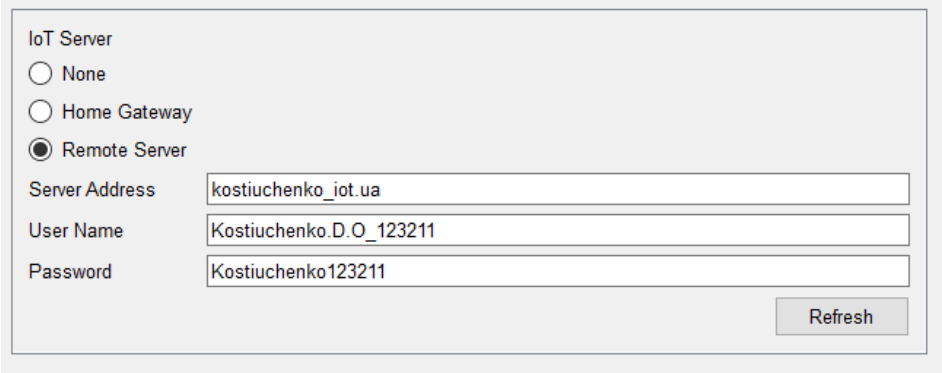


Рисунок 4.6 – Додавання пристрою до IoT-серверу

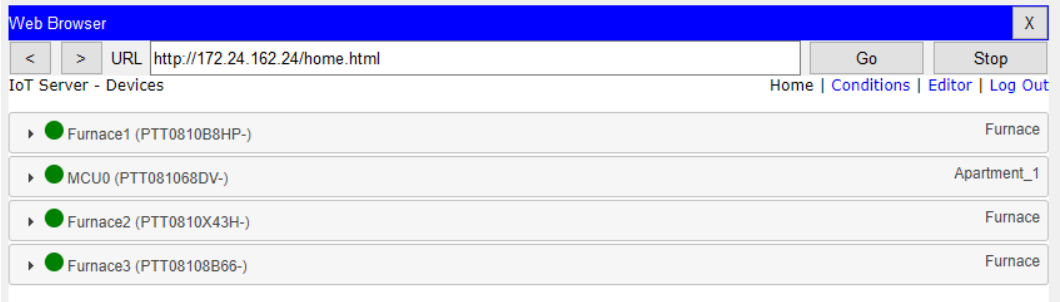


Рисунок 4.7 – Список підключених IoT-пристроїв

На рівні житлової підмережі LAN2 встановлений мікроконтролер MCU, який зчитує значення температури та вологості з сенсорів, розміщених у різних зонах квартири. Один із сенсорів температури (Temperature1) встановлено у внутрішньому приміщенні, а другий (Temperature2) – за межами житла, що дозволяє враховувати вплив зовнішніх кліматичних умов на роботу системи опалення. Усі значення зчитуються з аналогових входів, перетворюються у фізичні одиниці вимірювання, такі як градуси Цельсія, відсотки вологості та аналізуються безпосередньо на MCU.

Локальна логіка роботи реалізована у вигляді туманної обробки: при зниженні температури в приміщенні нижче 20 °C автоматично вмикаються два обігрівачі, а якщо температура зовні (за показником Temperature2) опускається нижче 18 °C при одночасному внутрішньому охолодженні – активується третій обігрівач. Якщо температурні значення повертаються в межі комфортного діапазону, опалення вимикається. Це дозволяє досягти

оперативної реакції без затримок, навіть у разі обмеженого доступу до зовнішньої мережі.

Після кожного циклу зчитування та реагування MCU передає актуальні значення температури, вологості та станів пристроїв на IoT-сервер, розміщений у віддаленій мережевій зоні.

На рівні хмарної логіки реалізовано сценарій централізованого захисту від перегріву (див. рисунок 4.8). Якщо температура в приміщенні досягає або перевищує 30 °C, а хоча б один із обігрівачів залишається увімкненим, IoT-сервер автоматично формує команду на вимкнення всіх обігрівачів, незалежно від локального сценарію. Такий захід підвищує надійність та безпеку роботи системи в умовах високого теплового навантаження.

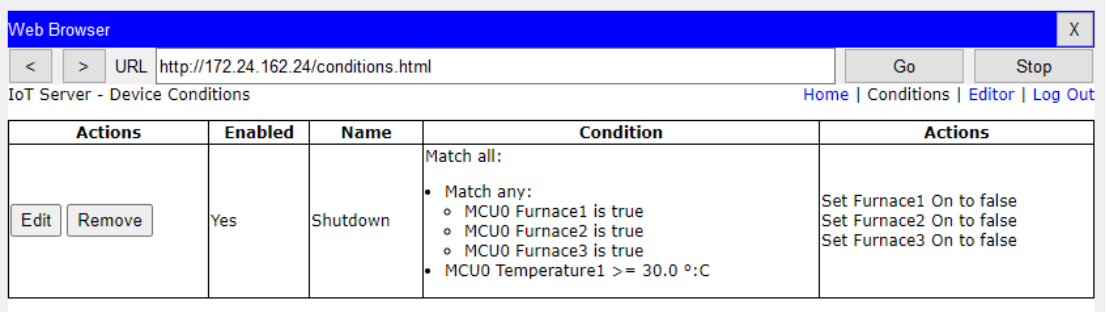


Рисунок 4.8 – Створений сценарій

ВИСНОВКИ

Результатом виконання кваліфікаційної роботи було розроблено функціональну модель кіберфізичної системи моніторингу та часткового управління опаленням у житловому комплексі. Проєкт охопив не лише створення структурної та логічної мережевої архітектури, а й інтеграцію інтелектуального блоку на основі IoT-технологій, що дозволяє забезпечити контроль параметрів мікроклімату та реагування на зміни у режимі реального часу. Реалізована система демонструє гнучку побудову з розподіленою логікою: дані зчитуються, аналізуються та обробляються безпосередньо на рівні MCU (туманний рівень), а у разі критичних ситуацій – рішення приймаються централізовано через IoT-сервер і хмарну логіку.

Мережева інфраструктура комплексу побудована із застосуванням сучасних засобів маршрутизації, сегментації трафіку через VLAN, а також захисту та автоматичної конфігурації (NAT, DHCP, SSH). Завдяки використанню протоколів динамічної маршрутизації та впровадженню хмарних служб забезпечено масштабованість, безперебійність і керованість усіх рівнів системи.

Перспективним напрямком розвитку даної кіберфізичної системи є впровадження додаткових сенсорів для моніторингу інших інженерних мереж (водопостачання, вентиляція, електропостачання), а також розширення функціональності серверного програмного забезпечення для аналітики та прогнозування. Також доцільно інтегрувати механізми автоматичного аварійного реагування та сповіщення, а в майбутньому – реалізувати мобільний або веб-інтерфейс для мешканців житлового комплексу, що дозволить зробити систему частиною більшої концепції "розумного дому". Залишаючись гнучкою, модульною та масштабованою, розроблена архітектура може бути легко адаптована до інших об’єктів з подібною інфраструктурою.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Cisco Systems. Cisco Catalyst 2960 Series Switches Datasheet [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/switches/catalyst-2960-series-switches/index.html

2. Espressif Systems. ESP32 Technical Reference Manual [Електронний ресурс]. – Версія 4.7. – 2023. – Режим доступу: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf

3. Schneider Electric. EcoStruxure Building Operation [Електронний ресурс]. – Режим доступу: https://www.se.com/ww/en/work/solutions/system/building/ecostruxure-for-building.jsp

4. IEEE Standards Association. *IEEE 802.3af-2003 (PoE Standard)* [Електронний ресурс]. – Режим доступу: https://standards.ieee.org/standard/802_3af-2003.html

5. MQTT.org. MQTT Version 5.0 Specification [Електронний ресурс]. – OASIS Standard. – 2019. – Режим доступу: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

6. National Institute of Standards and Technology (NIST). Framework for Cyber-Physical Systems [Електронний ресурс]. – Special Publication 1500-201. – 2017. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

7. European Committee for Standardization. *EN 15232:2017 Energy performance of buildings - Impact of Building Automation, Controls and Building Management* [Електронний ресурс]. – 2017. – Режим доступу: https://standards.cen.eu

8. OpenVPN. OpenVPN Cryptographic Layer [Електронний ресурс]. – Режим доступу: https://openvpn.net/community-resources/openvpn-cryptographic-layer/

9. OWASP Foundation. IoT Security Verification Standard (ISVS) [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-internet-of-things/

10. InfluxData. InfluxDB Documentation [Електронний ресурс]. – Режим доступу: https://docs.influxdata.com/influxdb/

11. Grafana Labs. Grafana Documentation [Електронний ресурс]. – Режим доступу: https://grafana.com/docs/grafana/latest/

ДОДАТОК А

Текст команд налаштування корпоративної мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРФІЗИЧНОЇ СИСТЕМИ ОПАЛЕННЯ У ЖИТЛОВОМУ КОМПЛЕКСІ

Текст програми

804.02070743.25012-01 12 01

Листів 9

2025

АНОТАЦІЯ

Дана програма містить більшу частину програмного коду, щовикористовувався при налаштування компонентів корпоративної мережікомп’ютерної системи.

Програма призначена для забезпеченняналаштування IP, DHCP, AAA, інтерфейсів, протоколу маршрутизації, NAT, консольних і vty ліній и ssh комп’ютерної системи.

ЗМІСТ

#Базові налаштування

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

#Налаштування імені

hostname Kostiuchenko_Router_5

#Пароль привілейованого доступу

enable secret 5 1mERr$9cTjUIEqNGurQiFU.ZeCi1

#Налаштування DHCP для Віртуальних мереж

ip dhcp excluded-address 172.24.161.129 172.24.161.134

ip dhcp excluded-address 172.24.161.161 172.24.161.166

ip dhcp excluded-address 172.24.161.193 172.24.161.198

ip dhcp excluded-address 172.24.161.225 172.24.161.230

!

ip dhcp pool VLAN22

 network 172.24.161.128 255.255.255.224

 default-router 172.24.161.129

 dns-server 172.24.162.22

ip dhcp pool VLAN32

 network 172.24.161.160 255.255.255.224

 default-router 172.24.161.161

 dns-server 172.24.162.22

ip dhcp pool VLAN42

 network 172.24.161.192 255.255.255.224

 default-router 172.24.161.193

 dns-server 172.24.162.22

```
ip dhcp pool VLAN99
 network 172.24.161.224 255.255.255.224
 default-router 172.24.161.225
 dns-server 172.24.162.22
```

#Налаштування AAA за протоколом Радіус

```
aaa new-model
!
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
```

#Створення локального користувача

```
username 123211_Kostiuchenko password 7 082048430017061E010803
license udi pid CISCO2811/K9 sn FTX1017UI0S-
ip domain-name Kostiuchenko_Router_2
!
spanning-tree mode pvst
!
```

#Налаштування адрес для фізичних інтерфейсів та VLAN

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 10.1.12.14 255.255.255.252
 duplex auto
 speed auto
```

```
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet1/0.22
 encapsulation dot1Q 22
 ip address 172.24.161.129 255.255.255.224
!
interface FastEthernet1/0.32
 encapsulation dot1Q 32
 ip address 172.24.161.161 255.255.255.224
!
interface FastEthernet1/0.42
 encapsulation dot1Q 42
 ip address 172.24.161.193 255.255.255.224
!
interface FastEthernet1/0.99
 encapsulation dot1Q 99
 ip address 172.24.161.225 255.255.255.224
!
interface FastEthernet1/1
 ip address 172.24.160.1 255.255.255.0
 duplex auto
 speed auto
```

#Налаштування OSPF

```
router ospf 12
 log-adjacency-changes
```

```
 passive-interface FastEthernet1/0
 passive-interface FastEthernet1/1
 network 10.1.12.12 0.0.0.3 area 0
 network 172.24.161.128 0.0.0.127 area 0
 network 172.24.160.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
```

#Налаштування MOTD банеру

```
banner motd ^CWarning! Access restricted. Kostiuchenko only!^C
```

#Налаштування RADIUS

```
radius server Kostiuchenko_AAA
 address ipv4 172.24.162.22 auth-port 1645
 key radius123
radius server 172.24.162.22
 address ipv4 172.24.162.22 auth-port 1645
 key radius123
```

#Налаштування LINE VTY

```
radius server Kostiuchenko_AAA
 address ipv4 172.24.162.22 auth-port 1645
 key radius123
radius server 172.24.162.22
 address ipv4 172.24.162.22 auth-port 1645
 key radius123
```

#Налаштування VPN

```
crypto isakmp policy 12
 encr aes 256
 authentication pre-share
```

```
 group 5
!
crypto isakmp key Kostiuchenko123211 address 64.100.13.2
!
crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
!
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN Connect
 set peer 64.100.13.2
 set pfs group5
 set security-association lifetime seconds 86400
 set transform-set VPN-SET
 match address 112
!
interface Serial0/0/0
 ip address 209.165.202.2 255.255.255.252
 ip nat outside
 crypto map VPN-MAP
!
access-list 112 permit ip 10.1.12.0 0.0.0.255 172.24.161.0 0.0.0.127
access-list 112 permit ip 172.24.160.0 0.0.0.255 172.24.161.0 0.0.0.127
access-list 112 permit ip 172.24.161.128 0.0.0.127 172.24.161.0 0.0.0.127
access-list 112 permit ip 172.24.162.0 0.0.0.127 172.24.161.0 0.0.0.127
access-list 112 permit ip host 209.165.202.2 172.24.161.0 0.0.0.127
access-list 112 permit ip host 172.24.162.22 host 64.100.13.2
!
```

#Налаштування NAT

```
interface FastEthernet0/0
 ip address 10.1.12.1 255.255.255.252
```

```
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.1.12.21 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 209.165.202.2 255.255.255.252
 ip nat outside
 crypto map VPN-MAP
!
interface FastEthernet1/0
 ip address 10.1.12.17 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT pool Internet
ip nat inside source static 172.24.162.23 209.165.200.4
ip nat inside source static 172.24.162.22 209.165.200.3
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```

ДОДАТОК Б

Текст програми налаштування IoT-системи

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ IOT СИСТЕМИ

Текст програми

804.02070743.25012-01 12 01

Листів 8

2025

АНОТАЦІЯ

Дана програма містить програмний код, розроблений для реалізації алгоритму роботи системи моніторингу опалення в житловому приміщенні. Код написано мовою Python для мікроконтролера, що виконує локальне зчитування, обробку та передачу даних сенсорів у межах кіберфізичної системи.

ЗМІСТ

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

Furnace1Pin = 0
Furnace2Pin = 1
Furnace3Pin = 2
HumiditySensor1Pin = 6
TemperatureSensor1Pin = 8
TemperatureSensor2Pin = 7
HumiditySensor2Pin = 9

IoEClient.setup ({
  "type": "Apartment_1",
  "states":
        [
              {
                    "name": "Furnace1",
                    "type": "bool"
              },
              {
                    "name": "Furnace2",
                    "type": "bool"
              },
              {
                    "name": "Furnace3",
                    "type": "bool"
              },
              {
                    "name": "Humidity1",
```

```
                "type": "number",
                "unit": "%"
            },
            {
                "name": "Humidity2",
                "type": "number",
                "unit": "%"
            },
            {
                "name": "Temperature1",
                "type": "number",
                "unit": "&deg:C",
                "decimalDigits": 1
            },
            {
                "name": "Temperature2",
                "type": "number",
                "unit": "&deg:C",
                "decimalDigits": 1
            }
        ]
    })

def main():
    pinMode(Furnace1Pin, OUT)
    pinMode(Furnace2Pin, OUT)
    pinMode(Furnace3Pin, OUT)

    print("Starting apartment monitoring system...")
```

```
while True:
    # Зчитування показників з датчиків
    humidity1 = analogRead(HumiditySensor1Pin)
    humidity2 = analogRead(HumiditySensor2Pin)
    temp1 = analogRead(TemperatureSensor1Pin)
    temp2 = analogRead(TemperatureSensor2Pin)

    # Конвертація аналогових значень у реальні величини
    humidity1_percent = humidity1 * 100 / 1023
    humidity2_percent = humidity2 * 100 / 1023
    temp1_celsius = (temp1 * 200 / 1023) - 100
    temp2_celsius = (temp2 * 200 / 1023) - 100

    # Керування батареями основуючись на температурі
    if temp1_celsius < 20:
        digitalWrite(Furnace1Pin, HIGH)
        Furnace1State = 1
        digitalWrite(Furnace2Pin, HIGH)
        Furnace2State = 1
    elif temp1_celsius > 25:
        digitalWrite(Furnace1Pin, LOW)
        Furnace1State = 0
        digitalWrite(Furnace2Pin, LOW)
        Furnace2State = 0
    if temp2_celsius < 18 and temp1_celsius <20:
        digitalWrite(Furnace3Pin, HIGH)
        Furnace3State = 1
    else:
        digitalWrite(Furnace3Pin, LOW)
        Furnace3State = 0
```

```
            # Оновлення станів IoT-клієнту
            IoEClient.reportStates([Furnace1State, Furnace2State, Furnace3State,
humidity1_percent, humidity2_percent, temp1_celsius, temp2_celsius])
            sleep(0.5)

    if __name__ == "__main__":
      main()
```