МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ІНТЕРНЕТУ РЕЧЕЙ ІНТЕГРАЦІЇ ПРИСТРОЇВ ДЛЯ СИСТЕМИ "РОЗУМНИЙ БУДИНОК"

Виконав: студент групи 1К-22
Спеціальності 123 Комп’ютерна інженерія
Кіріл КОВАЛЕНКО
Керівник:
Маргарита МЕДОЛИЗ

Черкаси – 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія комп’ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувачка циклової комісії КІ та ІТ

_____Наталя ФАЛЬЧЕНКО

(підпис)

«_____» _____2025 р.

З А В Д А Н Н Я

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Коваленку Кірілу Володимировичу

1. Тема роботи: Інтернету речей інтеграції пристроїв для системи "Розумний будинок". Керівник роботи Медолиз Маргарита Миколаївна викладач вищої категорії, затверджені наказом закладу перевищої освіти від «06» жовтня 2025 року №_84/1у .

2. Строк подання студентом кваліфікаційної роботи 08.06.2026 .

3. Вихідні дані до роботи: джерела та технічна документація, що описують апаратну платформу - мікроконтролерні системи та первинні вимірювальні перетворювачі: датчики температури, вологості, завад; протоколи роботи та програмні засоби організації взаємодії IoT-пристроїв.

4. Зміст кваліфікаційної роботи: теоретичні основи та аналіз існуючих рішень у сфері IoT для домашньої автоматизації (аналіз Wi-Fi, ZigBee, Z-Wave, порівняння REST API та MQTT, аналіз openHAB, Node-RED, Home Assistant); розробка структурної та схемотехнічної архітектури, написання низькорівневого ПЗ, конфігурування MQTT-інфраструктури та декларативних маніфестів Home Assistant); Експериментальні дослідження та оцінка ефективності.

5. Дата видачі завдання: «10» жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Основи та аналіз існуючих рішень у сфері IoT для домашньої автоматизації	09.12.2025	
3	Розділ 2 Проєктування та програмно-технічне забезпечення функціонування автономної системи	10.03.2026	
4	Розділ 3 Експериментальні дослідження, оцінювання надійності та функціональних характеристик системи	28.04.2026	
5	Висновки	12.05.2026	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	05.06.2026	
8	Подання кваліфікаційної роботи на затвердження завідувачу ЦК (за 7 днів до захисту)	08.06.2026	

Студент Кіріл КОВАЛЕНКО

(підпис)

Керівник роботи Маргарита МЕДОЛИЗ

(підпис)

АНОТАЦІЯ

У кваліфікаційній роботі розглянуто принципи роботи системи IoT-пристроїв, обґрунтовано актуальність відмови від централізованих хмарних обчислень на користь парадигми периферійних обчислень (Edge Computing) у системах домашньої автоматизації. Спроєктовано та практично реалізовано автономну архітектуру «Розумного будинку» на базі мікроконтролерів ESP32 та локального обчислювального хаба Home Assistant. Розроблено низькорівневе програмне забезпечення з використанням операційної системи реального часу FreeRTOS для асинхронного збору й демультиплексування телеметрії. Реалізовано обмін даними за допомогою полегшеного прикладного протоколу MQTT, налаштовано механізми захисту (ACL, шифрування, токени). Досліджено часові затримки доставки пакетів та стабільність зв'язку в умовах штучних завад. Робота має пракичне впровадження.

Ключові слова: Інтернет речей (IoT), ESP32, FreeRTOS, MQTT, Home Assistant, рериферійні обчислення, комп'ютерна інженерія.

ANNOTATION

The qualification work examines the principles of the IoT device system, justifies the relevance of abandoning centralized cloud computing in favor of the peripheral computing paradigm (Edge Computing) in home automation systems. An autonomous "Smart Home" architecture based on ESP32 microcontrollers and a local computing hub Home Assistant has been designed and practically implemented. Low-level software has been developed using the FreeRTOS real-time operating system for asynchronous collection and demultiplexing of telemetry. Data exchange has been implemented using the lightweight MQTT application protocol, and protection mechanisms have been configured (ACL, encryption, tokens). Packet delivery delays and communication stability under artificial interference have been investigated. The work has practical implementation.

Keywords: Internet of Things (IoT), ESP32, FreeRTOS, MQTT, Home Assistant, Edge Computing, Computer Engineering.

ЗМІСТ

ВСТУП

На сучасному етапі розвитку індустрії глобальної цифровізації та комп’ютерної інженерії парадигма Інтернету речей (Internet of Things, IoT) виступає одним із найбільш динамічних і фундаментальних напрямків еволюції розподілених обчислювальних систем. Стрімкий технологічний прогрес у сфері твердотільної мікроелектроніки, що супроводжується стійким трендом до зниження собівартості напівпровідникових систем на чипі (System on Chip, SoC), паралельно із розширенням зон покриття бездротових локальних мереж і впровадженням енергоефективних телекомунікаційних протоколів, створив об’єктивні передумови для масової інтеграції інтелектуальних засобів обчислювальної техніки в інфраструктуру житлового простору. Найбільш репрезентативним, затребуваним та практично значущим прикладом реалізації такого підходу є гетерогенні системи домашньої автоматизації та кіберфізичного моніторингу класу «Розумний дім» (Smart Home).

Ефективне, безвідмовне та безпечне функціонування сучасної локальної IoT-мережі всередині житлових приміщень безпосередньо залежить від архітектурних рішень, закладених у систему моніторингу параметрів середовища, агрегації телеметричних потоків та координації виконавчих вузлів. Системний аналіз сучасного ринку рішень у даному сегменті виявляє низку критичних інженерних і експлуатаційних недоліків, що створюють очевидне технічне протиріччя.

Більшість комерційних екосистем від глобальних вендорів жорстко спроєктовані за централізованою хмарною моделлю обчислень. Це вимагає безперервної наявності високошвидкісного каналу зв'язку з глобальною мережею Інтернет та безперебійного функціонування віддалених серверів виробника. У випадку деградації магістральних ліній зв'язку провайдера, виникнення критичних затримок маршрутизації або раптового припинення комерційної чи геополітичної підтримки серверної інфраструктури

розробником, локальна система автоматизації повністю втрачає працездатність, перетворюючи інтелектуальні виконавчі пристрої на ізольовані нефункціональні компоненти.

Низький рівень інформаційної безпеки та компрометація конфіденційності, який полягає в тому, що транспортування первинних телеметричних даних приватного характер, наприклад, профілі повсякденної активності, параметри енергоспоживання, стани систем охоронно-пожежної сигналізації, медіапотоки, на сторонні віддалені сервери створює критичні вектори атак на приватність користувача. Існує постійна загроза несанкційного доступу до вимірювальних масивів у результаті компрометації хмарних баз даних, витоку автентифікаційних токенів або перехоплення трафіку на проміжних вузлах глобальної мережі (атаки типу Man-in-the-Middle).

Використання стандартних веб-протоколів для передачі дрібних пакетів вимірювальної інформації призводить до неефективного навантаження на мережеве обладнання через великий обсяг супутніх службових заголовків, що суттєво знижує пропускну здатність локального бездротового каналу при масштабуванні мережі.

З огляду на це, в галузі комп'ютерної інженерії постає гостра необхідність у розробці локально-автономних, архітектурно гнучких та інкапсульованих систем моніторингу й керування локальними IoT-мережами. Такі системи повинні базуватися на апаратних засобах із відкритими специфікаціями та програмному забезпеченні з відкритим вихідним кодом (Open Source), реалізуючи парадигму периферійних обчислень (Edge Computing). Це дозволяє локально збирати телеметрію з датчиків, аналізувати її в реальному часі без залучення зовнішніх серверів, забезпечувати стійку логіку автоматизованого захисту виконавчих механізмів та надавати користувачеві захищений інтерфейс взаємодії. Вищезазначені чинники визначають високу актуальність, теоретичну обґрунтованість та практичну доцільність теми даної кваліфікаційної роботи.

Метою кваліфікаційної роботи є проєктування, програмно-апаратна реалізація, конфігурування та експериментальне дослідження високоефективної, автономної системи моніторингу й керування розподіленою гетерогенною IoT-мережею «Розумний дім» із підвищеним рівнем локальної незалежності, інформаційної безпеки та мінімальним часом відгуку виконавчих вузлів на аварійні події.

Для досягнення поставленої мети в роботі сформульовано та вирішено такі завдання:

1. Провести системний аналітичний огляд існуючих концепцій, топологій бездротових мереж, апаратних платформ та прикладних протоколів передачі даних, що використовуються в сучасних інформаційно-вимірювальних та керуючих IoT-мережах домашньої автоматизації.

2. Виконати порівняльний техніко-економічний аналіз та обґрунтувати вибір оптимальної апаратної бази (мікроконтролерних систем на чипі, первинних вимірювальних перетворювачів) та системного і прикладного програмного забезпечення для розгортання центрального обчислювального сервера.

3. Спроектувати структурну, функціональну та схемотехнічну архітектуру локальної IoT-мережі «Розумний дім», забезпечивши гальванічну й оптичну ізоляцію інформаційних та силових ліній комутації.

4. Реалізувати низькорівневе програмне забезпечення для периферійних обчислювальних мікроконтролерів, розробити структури обміну даними та виконати декларативне конфігурування системних служб центрального сервера моніторингу.

5. Провести комплексні випробування та експериментальне тестування розробленого програмно-апаратного комплексу в різних режимах експлуатації, здійснити кількісну оцінку часових затримок доставки пакетів даних та стабільності радіозв’язку в умовах штучного погіршення завадової обстановки.

Об’єкт дослідження – процеси асинхронного збору телеметричних даних, моніторингу поточного стану фізичних параметрів середовища та координації функціонування розподілених інтелектуальних вузлів у локальних мережах Інтернету речей.

Предмет дослідження – архітектурні рішення, програмні алгоритми обробки інформації, мережеві протоколи прикладного рівня, декларативні конфігураційні маніфести та апаратно-програмні засоби побудови автономної системи моніторингу й керування локальною IoT-мережею «Розумний дім».

Практичне значення отриманих результатів полягає у створенні дієздатного, локально-незалежного, масштабованого дослідного макета системи моніторингу та керування, який може бути використаний як архітектурний базис для розгортання систем домашньої автоматизації підвищеної надійності. Створений прототип є готовою архітектурною базою для побудови відмовостійких локальних систем автоматизації.

РОЗДІЛ 1 ОСНОВИ ТА АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ У СФЕРІ IoT ДЛЯ ДОМАШНЬОЇ АВТОМАТИЗАЦІЇ

1.1 Концепція Інтернету речей (IoT) в архітектурі комп'ютерних систем автоматизації

Концепція Інтернету речей (Internet of Things, IoT) є парадигмою побудови розподілених обчислювальних систем, яка передбачає інтеграцію фізичних об'єктів або «речей», оснащених вбудованими засобами обчислювальної техніки, у єдину телекомунікаційну мережу. У контексті комп'ютерної інженерії та систем автоматизації житлового простору (Smart Home), впровадження IoT трансформує традиційно ізольовані інженерні підсистеми, сенсорні датчики та виконавчі пристрої на вузли розподіленої обчислювальної мережі. Основною метою такої інтеграції є забезпечення безперервного моніторингу параметрів середовища, мінімізація участі людини у рутинних процесах керування, підвищення рівня безпеки та оптимізація споживання енергетичних ресурсів.

Для глибокого аналізу та проєктування гетерогенних IoT-систем застосовується багаторівнева декомпозиція архітектури. Відповідно до сучасних стандартів комп'ютерної інженерії, архітектуру автономної системи домашньої автоматизації розділено на чотири функціональні рівні.

Першим є рівень фізичного сприйняття та виконання. Даний рівень безпосередньо взаємодіє з навколишнім середовищем за допомогою первинних вимірювальних перетворювачів: датчиків температури, відносної вологості, освітленості, концентрації газів, гідродинамічного тиску, та виконавчих механізмів: твердотільних та електромагнітних реле, сервоприводів, крокових двигунів, соленоїдних клапанів. Основним інженерним завданням на цьому рівні є забезпечення точності аналого-цифрового перетворення, фільтрація апаратних шумів, початкове нормування сигналів та комутація силових навантажень із високою надійністю.

Другим виступає мережевий рівень транспортування даних. Його функція полягає у забезпеченні стійких, завадозахищених каналів зв'язку для передачі структурованої інформації між фізичними периферійними вузлами та центральним обчислювальним сервером. Мережевий рівень базується на комбінації дротових та бездротових технологій, реалізуючи мережевий стек протоколів TCP/IP, де головна увага приділяється топології мережі, маршрутизації пакетів, мінімізації колізій та надійності адресації пристроїв.

Третім є рівень проміжного програмного забезпечення. Це ядро всієї системи моніторингу та керування. Він реалізується на базі високопродуктивних локальних обчислювальних засобів і виконує функції агрегації потоків даних, демультиплексування повідомлень, ведення часових баз даних, аналізу поточного стану об'єкта та виконання складних логічних сценаріїв автоматизації - скриптів. На цьому рівні відбувається обробка подій за алгоритмами реального часу.

Четвертим визначено рівень прикладних додатків та інтерфейсів. Він забезпечує абстракцію складних низькорівневих процесів для кінчевого користувача через графічні веб-інтерфейси або мобільні додатки. Завдання рівня – візуалізація телеметрії у вигляді аналітичних графіків, відображення поточних статусів виконавчих механізмів та надання каналів безпечного віддаленого ручного керування через шифровані протоколи.

Критичним викликом при проєктуванні є гетерогенність середовища – сумісне функціонування обладнання від різних виробників, яке використовує закриті пропрієтарні протоколи та різні фізичні інтерфейси. Створення універсальної системи, яка усуває цю проблему шляхом інкапсуляції даних у єдиний відкритий інформаційний простір на локальному рівні, є основним завданням цієї роботи.

1.2 Порівняльний аналіз бездротових протоколів передачі даних та фізичних рівнів зв'язку

Вибір бездротової технології для периферійних IoT-вузлів вимагає детального аналізу компромісів між енергоспоживанням, радіусом стабільного покриття, пропускною здатністю каналу та стійкістю до електромагнітних завад в умовах житлових приміщень.

Протокол Wi-Fi, що працює переважно в діапазоні частот 2.4 ГГц, є базовим для багатьох систем. На фізичному рівні він використовує технології модуляції із розширенням спектра, що забезпечує високу пропускну здатність до сотень Мбіт/с. Головною інженерною перевагою є наявність готової інфраструктури у кожному приміщенні, наприклад точок доступу та маршрутизаторів. Периферійні вузли підключаються безпосередньо до локальної мережі без додаткових проміжних шлюзів-трансляторів. Проте Wi-Fi має високе енергоспоживання, струм споживання в режимі передачі радіомодуля може досягати 150–250 мА, що виключає тривале автономне живлення пристроїв від мініатюрних гальванічних елементів. Також стандартна топологія «Зірка» навантажує центральний маршрутизатор при підключенні великої кількості одночасно функціонуючих клієнтів.

Протокол ZigBee спеціально оптизований для низькошвидкісних мереж датчиків з ультранизьким енергоспоживанням. Працюючи на частоті 2.4 ГГц з модуляцією O-QPSK, він забезпечує швидкість передачі даних до 250 Кбіт/с. Основна перевага полягає у підтримці комірчастої топології Mesh-мережі. Кожен вузол, підключений до постійної мережі живлення, функціонує як ретранслятор (роутер) пакетів, що дозволяє динамічно нарощувати площу покриття та оминати фізичні перешкоди. Струм споживання кінцевих датчиків у режимі сну становить лічені мікроампери, забезпечуючи автономність до декількох років від однієї батареї CR2032. Недоліком є обов'язкова потреба у спеціальному апаратному координаторі - ZigBee-шлюзі для трансляції даних у стандартну IP-мережу.

Протокол Z-Wave є пропрієтарною технологією, що працює в субгігагерцовому діапазоні частот, а в європейському регіоні – 868.42 МГц. Використання цієї частоти забезпечує вищу дифракційну та проникну здатність радіохвилі крізь залізобетонні та цегляні стіни порівняно з частотою 2.4 ГГц. Мережа Z-Wave повністю захищена від завад, що створюються побутовими Wi-Fi роутерами, Bluetooth-пристроями та мікрохвильовими пічами. Вона також підтримує Mesh-топологію (до 232 вузлів). Основним стримуючим фактором для широкого впровадження є висока вартість чипсетів, ліцензування та сертифікації обладнання, що здорожує фінальну вартість розробки.

Протокол Bluetooth Low Energy (BLE) орієнтований на короткі дистанції зв'язку за топологією «точка-точка» або «зірка». Він має низькі затримки встановлення з'єднання (в межах декількох мілісекунд) та високу енергоефективність. Однак обмежений радіус дії (до 10–15 метрів в умовах інтер'єрних перегородок) та складність побудови стабільних багатоструктурних мереж без використання спеціалізованих BLE Mesh специфікацій обмежують його застосування як магістрального протоколу для комплексного моніторингу великих об'єктів.

З урахуванням мети кваліфікаційної роботи – створення доступного, локально-незалежного та схемотехнічно простого дослідного макета системи як базовий інтерфейс передачі даних обрано Wi-Fi. Це дозволяє реалізувати пряму адресацію вузлів за допомогою стеків протоколів IPv4, уникнути потреби в додаткових апаратних координаторах та застосувати високоефективні мікроконтролери з інтегрованими радіомодулями.

1.3 Порівняльний аналіз прикладних протоколів: архітектурний стиль HTTP (REST) проти MQTT

Ефективність функціонування IoT-мережі, швидкість її реакції на події та стабільність каналів зв'язку безпосередньо залежать від вибору протоколу прикладного рівня (Application Layer). Найбільш поширеними рішеннями є

архітектурний стиль HTTP (REST API) та спеціалізований протокол масової телеметрії MQTT.

Архітектурний стиль REST (Representational State Transfer) базується на протоколі HTTP і використовує класичну клієнт-серверну модель «запит-відповідь» (Request-Response). Кожен периферійний датчик для передачі поточної інформації повинен самостійно ініціювати сесію зв'язку, встановити триетапне TCP-рукостискання (Three-way Handshake) з сервером, надіслати текстовий запит, що містить значний обсяг службових HTTP-заголовків (HTTP Headers, Cookies, User-Agent), отримати підтвердження від сервера та розірвати з'єднання.

Для систем моніторингу реального часу такий підхід має критичні недоліки. Висока надлишковість трафіку, коли розмір службових заголовків HTTP-пакета може становити від 200 до 1000 байт, тоді як корисне навантаження, наприклад, значення температури «24.5», займає лише декілька байт. Це призводить до неефективного використання смуги пропускання.

Відсутність асинхронності, коли сервер не має можливості ініціювати відправку команди на периферійний пристрій у реальному часі. Для отримання команд мікроконтролер змушений постійно опитувати сервер через фіксовані проміжки часу, що створює постійне паразитне навантаження на обчислювальне ядро та мережу.

Протокол MQTT (Message Queuing Telemetry Transport) є легковажним, компактним протоколом, спеціально розробленим для умов обмеженої пропускної здатності та пристроїв із низькою обчислювальною потужністю. Функціонування протоколу базується на асинхронному шаблоні проектування «видавець-підписник». Центральним вузлом мережі є логічний посередник – MQTT-брокер. Клієнти датчики та виконавчі пристрої встановлюють одне перманентне TCP-з'єднання з брокером і підтримують його за допомогою коротких службових пакетів перевірки активності.

Передача даних здійснюється через ієрархічну систему тематичних каналів – топіків, структурованих за допомогою косої риски наприклад,

об'єкт/кімната/тип_датчика. Датчик публікує дані в топік, а брокер автоматично перенаправляє це повідомлення всім вузлам, які підписалися на цей топік наприклад, центральному серверу автоматизації або графічному інтерфейсу.

Інженерні переваги протоколу MQTT в архітектурі IoT:

– Мінімальний оверхед- фіксований заголовок пакета MQTT становить всього 2 байти, що мінімізує обсяг службового трафіку в сотні разів порівняно з HTTP.

– Рівні якості обслуговування QoS протокол аппаратно підтримує три рівні гарантії доставки: QoS 0 (доставка без гарантії, максимум один раз), QoS 1 (гарантована доставка з обов'язковим підтвердженням PUBACK, мінімум один раз), QoS 2 (строго одноразова доставка за допомогою чотириетапного підтвердження, виключаючи дублювання пакетів).

– Механізм LWT - дозволяє клієнту під час автентифікації зареєструвати у брокера «передсмертне» повідомлення. Якщо пристрій раптово втрачає живлення або зникає з радіоефіру, брокер самостійно розсилає це повідомлення в топік аварій, сповіщаючи систему про відмову вузла.

Таким чином, за критеріями мінімізації мережевого трафіку, підтримки асинхронності та надійності зв'язку, протокол MQTT є безальтернативним вибором для реалізації розроблюваної системи.

1.4 Системний аналіз програмних платформ для побудови центрального обчислювального хаба

Центральний обчислювальний хаб повинен виконувати роль агрегатора гетерогенних даних, інтерпретатора логічних правил автоматизації та сервера візуалізації. Проведено системний аналіз трьох провідних програмних платформ з відкритим кодом.

Платформа openHAB побудована на мові програмування Java та використовує архітектуру OSGi. Вона має високий рівень модульності та абстракції. Рівень абстракції розділяє фізичні пристрої та їхні функціональні

властивості, які прив'язуються до віртуальних об'єктів. Система підтримує складну текстову конфігурацію правил.

Проте використання Java Virtual Machine висуває високі вимоги до обсягу оперативної пам'яті (RAM) та обчислювальної потужності процесора. При розгортанні на бюджетних одноплатних комп'ютерах початкового рівня спостерігається значне споживання ресурсів, тривалий час ініціалізації системи та затримки при обробці великих масивів подій, що знижує загальну ефективність системи.

Платформа Node-RED є інструментом візуального проектування логічних потоків даних, розробленим корпорацією IBM на базі середовища виконання Node.js. Концепція архітектури полягає у маніпулюванні функціональними блоками (вузлами), які з'єднуються між собою віртуальними зв'язками на графічній панелі. Кожен блок представляє собою подію, функцію обробки або фізичний інтерфейс. Передача даних між блоками здійснюється у вигляді об'єктів JavaScript. Платформа є надзвичайно легковажною, працює асинхронно та ідеально підходить для створення складних маршрутів передачі MQTT-повідомлень. Головним недоліком Node-RED є складність побудови комплексного, багатосторінкового, адаптивного та естетичного інтерфейсу користувача (Dashboard) «з коробки», що вимагає встановлення сторонніх плагінів та написання значного обсягу HTML/CSS коду.

Платформа Home Assistant є найбільш динамічною екосистемою з відкритим вихідним кодом, написаною на мові програмування Python. Архітектура орієнтована на концепцію повного локального контролю (Local-first), що виключає залежність від хмарних сервісів. Всі обчислення, аналітика та збереження даних відбуваються виключно в межах локального процесора. Екосистема використовує подієво-орієнтовану модель (Event Loop), що забезпечує швидку реакцію на зміну станів сутностей (Entities).

Платформа містить інтегроване сучасне середовище візуалізації Lovelace UI, яке автоматично адаптується під будь-які роздільні здатності екранів. Конфігурування інтеграцій та опис логічних зв'язків здійснюється за

допомогою декларативних маніфестів у форматі YAML, що спрощує структурування архітектури системи. Завдяки наявності розвиненої системи додатків (Add-ons), платформа дозволяє в один клік розгортати суміжні сервіси, такі як MQTT-брокери чи бази даних часових рядів.

На основі проведеного аналізу за критеріями мінімальних вимог до апаратних ресурсів, гнучкості декларативного налаштування та якості інтерфейсу моніторингу для реалізації проекту обрано платформу Home Assistant.

1.5 Обґрунтування вибору мікроконтролерної архітектури периферійних пристроїв

Для реалізації кінцевих вузлів збору телеметрії та керування вивчимо три покоління обчислювальних мікроконтролерних архітектур, доступних на ринку електронних компонентів.

Архітектура AVR на базі мікроконтролера ATmega328, платформа Arduino є класичним 8-бітним RISC-процесором з гарвардською архітектурою пам'яті. Тактова частота становить лише 16 МГц, обсяг оперативної пам'яті обмежений 2 КБ, а флеш-пам'яті – 32 КБ. Головним інженерним недоліком цієї архітектури є повна відсутність інтегрованих мережевих інтерфейсів зв'язку. Для підключення до бездротової мережі необхідно використовувати зовнішні апаратні трансивери наприклад, nRF24L01 або Ethernet-контролери, що суттєво ускладнює схемотехніку друкованої плати, збільшує кінцеві габарити пристрою та споживання енергії. Обмежений обсяг пам'яті унеможливлює реалізацію сучасних криптографічних протоколів захисту даних (TLS/SSL) та обробку об'ємних структурованих JSON-пакетів.

Мікроконтролер ESP8266 (платформа NodeMCU) є 32-бітною системою на чипі (SoC) з процесорним ядром Tensilica L106, що працює на тактовій частоті 80 або 160 МГц. Він містить інтегрований апаратний радіомодуль Wi-Fi стандарту 802.11 b/g/n та обсяг флеш-пам'яті до 4 МБ. Це енергоефективне та економічно вигідне рішення для побудови базових датчиків.

Проте ESP8266 має суттєві обмеження: наявність лише одного каналу аналого-цифрового перетворення (АЦП/ADC), обмежену кількість універсальних виводів введення-виведення (GPIO), а головне – одноядерну архітектуру. Одноядерна структура змушена розділяти процесорний час між обслуговуванням фонового мережевого стеку Wi-Fi та виконанням основного циклу користувацької програми. При виникненні затримок в опитуванні датчиків або виконанні складних математичних розрахунків виникає ризик порушення таймінгів мережевого стеку, що призводить до обриву зв'язку або програмного зависання системи.

Мікроконтролер ESP32 є системою на чипі нового покоління, побудованою на базі високоефективної архітектури Tensilica Xtensa Dual-Core 32-bit LX6. Обчислювальне ядро працює на регульованій тактовій частоті до 240 МГц, забезпечуючи продуктивність на рівні до 600 DMIPS. Кристал містить 520 КБ вбудованої оперативної пам'яті (SRAM), інтегровані модулі бездротового зв'язку Wi-Fi та Bluetooth, а також апаратні прискорювачі криптографічних алгоритмів (AES, SHA-2, RSA, ECC).

Головною інженерною перевагою архітектури ESP32 є наявність двох симетричних і незалежних обчислювальних ядер Core 0 та Core 1. Це дозволяє на рівні операційної системи реального часу FreeRTOS жорстко розмежувати виконання системних та прикладних завдань. Ядро Core 0 виділяється виключно під обслуговування низькорівневих завдань: підтримку безперервної бездротової сесії зв'язку, обробку стеку TCP/IP та взаємодію з MQTT-брокером. Ядро Core 1 виділяється під прикладний цикл: безперервне асинхронне опитування датчиків, цифрове фільтрування сигналів, обчислення контрольних сум та миттєве керування GPIO виводами виконавчих реле.

Додатково ESP32 має багату периферію: до 18 каналів 12-бітного аналого-цифрового перетворення, вбудовані датчики дотику, апаратні інтерфейси UART, SPI, I2C та можливість перепризначення виводів (Pin Multiplexing). Наявність апаратного криптографічного прискорення дозволяє

пакувати дані у шифровані пакети без зниження загальної продуктивності системи.

Враховуючи двоядерну архітектуру, розширені можливості підключення аналогових і цифрових сенсорів та апаратну підтримку багатозадачності, мікроконтролер ESP32 обрано як оптимальний та безальтернативний обчислювальний базис для побудови периферійних вузлів системи «Розумний дім».

1.6. Порівняльний аналіз технічних характеристик апаратних засобів

Для систематизації результатів системного аналізу апаратних компонентів та забезпечення наочності обґрунтування технічних рішень у рамках кваліфікаційної роботи сформовано порівняльну таблицю. Вона відображає ключові параметри обчислювальних платформ, які критично впливають на архітектуру системи моніторингу та її здатність працювати в автономному режимі реального часу.

Таблиця 1.1 – Системно-технічні характеристики обчислювальних мікроконтролерних платформ IoT

Параметр обчислювальної системи	ATmega328 (Arduino Uno)	Tensilica L106 (ESP8266)	Xtensa LX6 (ESP32)
Розрядність архітектури ядра	8 біт (RISC)	32 біти (RISC)	32 біти (Двоядерний RISC)
Максимальна тактова частота	16 МГц	160 МГц	240 МГц
Обсяг оперативної пам'яті (RAM)	2 КБ	80 КБ	520 КБ
Обсяг інтегрованої флеш-пам'яті	32 КБ	До 4 МБ (зовнішня)	4 МБ – 16 МБ (вбудована)
Інтегровані бездротові інтерфейси	Відсутні	Wi-Fi 802.11 b/g/n	Wi-Fi 802.11 b/g/n, BLE v4.2
Характеристики АЦП (ADC)	6 каналів, 10 біт	1 канал, 10 біт	18 каналів, 12 біт
Апаратне прискорення криптографії	Відсутнє	Відсутнє	AES, SHA-2, RSA, ECC, RNG

Продовження таблиці 1.1

Підтримка ОС реального часу (RTOS)	Обмежена (через брак RAM)	Часткова	Повна (інтегрована FreeRTOS)
Струм споживання в режимі глибокого сну	~15 мкА	~20 мкА	~10 мкА

Аналіз даних таблиці 1.1 підтверджує, що мікроконтролер ESP32 суттєво перевищує попередні архітектури за обчислювальною потужністю та обсягом оперативної пам'яті. Це гарантує стабільне функціонування розгалужених логічних алгоритмів та асинхронних стеків зв'язку без загрози переповнення стеку чи динамічної пам'яті пристрою.

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ КОМПОНЕНТІВ АВТОНОМНОЇ СИСТЕМИ

2.1 Структурна організація та топологічні рішення розподіленої IoT-мережі

Проєктні рішення, покладені в основу архітектури розроблюваної системи автоматизації та моніторингу класу «Розумний дім», базуються на децентралізованій парадигмі периферійних обчислень (Edge Computing). Це дозволяє забезпечити високий рівень автономності, живучості та інформаційної безпеки системи в умовах повної ізоляції від зовнішніх комерційних хмарних сервісів. Топологічна структура системи спроєктована за гібридною схемою типу «зірка з периферійними підмережами», де центральним елементом виступає локальний обчислювальний сервер, а периферійними вузлами – інтелектуальні контролери збору телеметрії та координації виконавчих пристроїв.

Гібридна топологія системи «зірка з периферійними підмережами» поєднує в собі переваги централізованого керування інформаційними потоками та децентралізованого виконання захисних функцій. Центральний обчислювальний хаб діє як ядро зірки, забезпечуючи маршрутизацію повідомлень, проте кожен промінь цієї зірки веде до автономного обчислювального елемента, здатного підтримувати повну працездатність підпорядкованого йому інженерного сегмента при руйнуванні зв'язку з ядром. Така схема кардинально відрізняється від класичних централізованих топологій, де вихід з ладу головного контролера призводить до повного паралічу всієї інфраструктури об'єкта.

Логічна взаємодія між усіма компонентами гетерогенного середовища організована через багаторівневу модель взаємодії відкритих систем, де виділено три ключові функціональні рівні.

Першим є апаратний або фізичний рівень, який включає первинні вимірювальні перетворювачі датчики фізичних величин, виконавчі релейні

модулі, силові лінії комутації та локальні мікроконтролерні системи на чипі SoC. На цьому рівні відбувається безпосередня взаємодія електронної компоненти з фізичним світом шляхом перетворення неелектричних величин, таких як температура, вологість або присутність рідини, у дискретні електричні сигнали та навпаки.

Другим виступає мережевий рівень, що забезпечує транспортування інформаційних пакетів всередині захищеного бездротового сегмента за допомогою стеків протоколів TCP/IP. Він відповідає за логічну адресацію пристроїв, контроль цілісності переданих фреймів, виявлення та усунення колізій у радіоефірі, а також за підтримку стійкого каналу зв'язку між гетерогенними апаратними платформами.

Третім визначено прикладний рівень, який реалізує логіку обміну повідомленнями на базі спеціалізованого полегшеного протоколу MQTT. Цей рівень інкапсулює сирі вимірювальні дані у структуровані формати високого порядку, визначає семантику взаємодії пристроїв, координує права доступу до інформаційних каналів та реалізує бізнес-логіку функціонування всієї системи «Розумний дім».

Центральний сервер системи виконує роль координатора локальних баз даних, посередника обміну повідомленнями MQTT-брокера та хоста для графічного інтерфейсу користувача. Оскільки сервер функціонує виключно всередині локальної фізичної мережі об'єкта, критично знижується затримка доставки команд та повністю усувається ризик перехоплення даних зовнішніми зловмисниками на проміжних магістралях глобальної мережі Інтернет. Обчислювальна потужність сервера дозволяє здійснювати довгострокове архівацію параметрів телеметрії, аналізувати тенденції зміни кліматичних показників та виконувати високорівневі макроси автоматизації, які пов'язують роботу кількох підсистем в єдиний комплекс.

Периферійні вузли, розгорнуті на базі високоінтегрованих мікроконтролерів, поділяються за своїм функціональним призначенням на три основні категорії та показані на рисунку 2.1.

До першої належать кліматичні моніторингові станції, призначені для безперервного квантування та зчитування параметрів навколишнього середовища, таких як температура та відносна вологість повітря. Ці станції оптимізовані для роботи в режимах зниженого енергоспоживання та забезпечують формування первинного масиву даних для систем кондиціювання та опалення.

Другу категорію складають системи аварійного кіберфізичного захисту, орієнтовані на виявлення критичних подій у реальному часі, зокрема прориву трубопроводу водопостачання. До цих пристроїв висуваються жорсткі вимоги щодо часу реакції та надійності, оскільки затримка в їх роботі може призвести до значних матеріальних збитків.

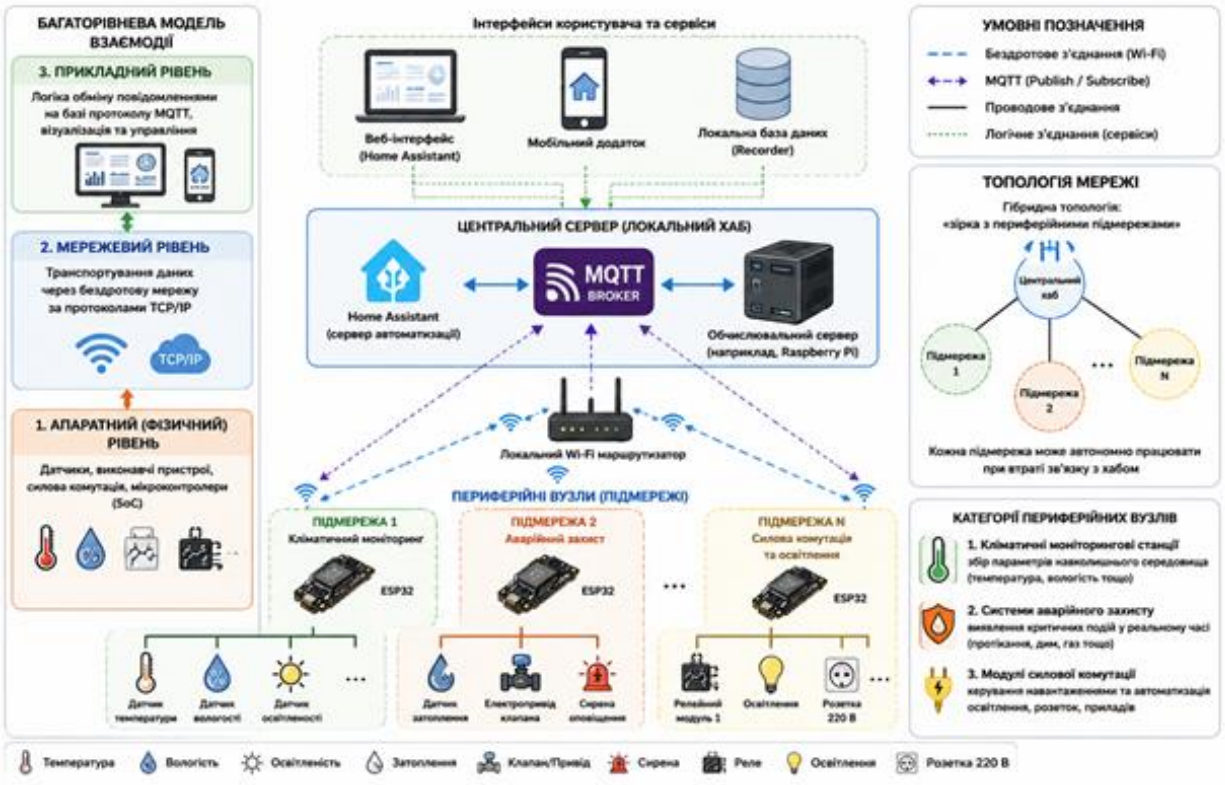

Рисунок 2.1 – Структурна організація мережі «Розумний дім»

Третьою категорією є модулі силової комутації та автоматизації освітлення, які виконують безпосереднє замикання та розмикання електричних кіл живлення побутових приладів на основі рішень сервера або

автономних аварійних сценаріїв. Вони виступають кінцевими виконавчим елементами, що замикають контур керування системи.

2.2 Обґрунтування вибору мікроконтролерної архітектури та розподіл обчислювальних ресурсів

Для реалізації периферійних обчислювальних вузлів системи було обрано 32-бітну двоядерну мікроконтролерну систему на чипі (SoC) архітектури Xtensa LX6 від компанії Espressif Systems – чип моделі ESP32. Дане рішення має суттєві техніко-економічні переваги порівняно з класичними 8-бітними мікроконтролерами (наприклад, архітектури AVR), оскільки інтегрує на одному напівпровідниковому кристалі обчислювальні ядра з тактовою частотою до двісті сорока мегагерц, вбудовані блоки бездротового зв’язку Wi-Fi стандарту вісімсот два крапка одинадцять b/g/n та Bluetooth версії чотири крапка два, а також розвинену периферію вводу-виводу.

Вибір архітектури Xtensa LX6 зумовлений її високою ефективністю при виконанні завдань, що вимагають одночасної підтримки інтенсивного мережевого обміну та реалізації швидких алгоритмів обробки сигналів. На відміну від одноядерних рішень, де планувальник завдань змушений постійно переривати виконання прикладного коду для обслуговування переривань мережевого контролера, дана двоядерна структура забезпечує справжній апаратний паралелізм. Це усуває явище джитера при зчитуванні даних з давачів та гарантує детермінований час реакції на зовнішні події переривання.

Важливим архітектурним аспектом використання обраної системи на чипі є наявність п'ятсот двадцяти кілобайт статичної оперативної пам'яті (SRAM). Це дозволяє підтримувати повноцінний стек мережевих протоколів із шифруванням без загрози виникнення помилок переповнення буфера або динамічної пам'яті. Наявність апаратного криптографічного прискорювача для алгоритмів AES, SHA-2, RSA та кривих ECC дає змогу реалізувати захищені з'єднання на низькому рівні без суттєвого зниження продуктивності основних обчислювальних ядер. Обсяг інтегрованої флеш-пам'яті, що підключається по

швидкій шині SPI і становить від чотирьох до шістнадцяти мегабайт, надає можливість розміщення складного прикладного коду, локальних веб-сторінок конфігурації та буферів для тимчасового зберігання телеметрії при відсутності зв'язку.

Розподіл ресурсів процесора в рамках розробленого системного програмного забезпечення базується на використанні операційної системи реального часу FreeRTOS. Обчислювальне навантаження строго розмежоване між двома ядрами чипа, що відображено на рис.2.2.

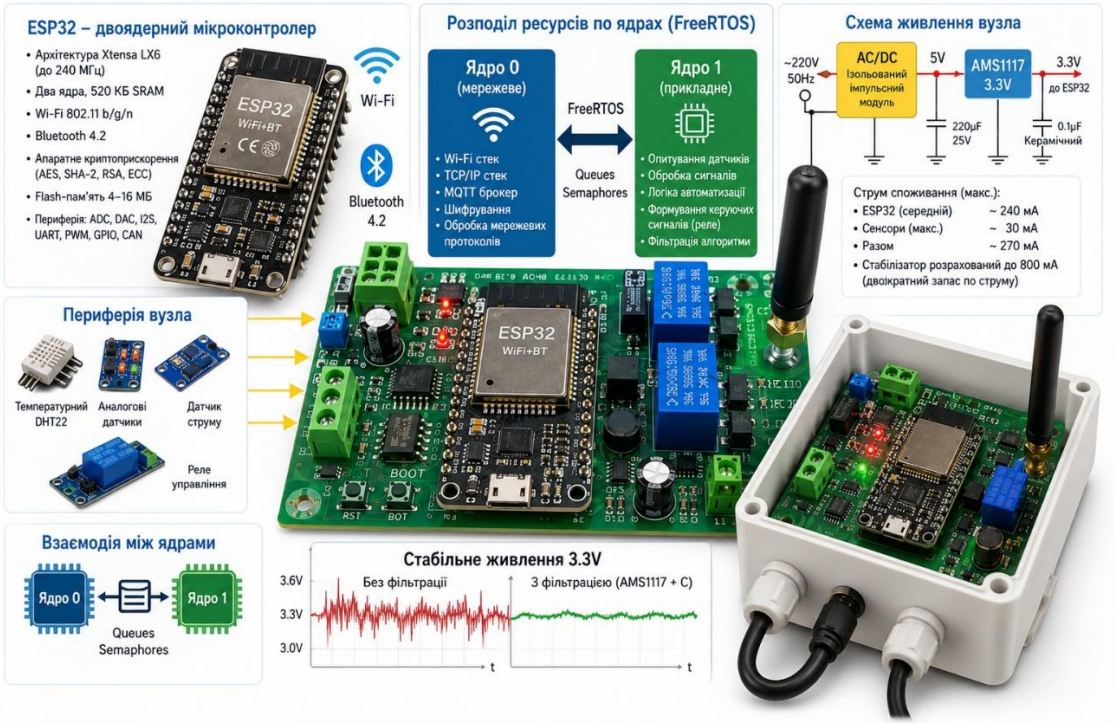

Рисунок 2.2 – Архітектура мікроконтролерного вузла на базі ESP32

Перше ядро, яке умовно позначається як нульове, повністю виділене під обслуговування низькорівневих завдань бездротового зв'язку. Воно забезпечує підтримання стабільної Wi-Fi сесії, обробку стеків протоколу TCP/IP, виконання процедур автентифікації та безперервну взаємодію з локальним MQTT-брокером. Це гарантує, що мережева активність, обробка вхідних мережевих штормів та можливі затримки при передачі пакетів по радіоканалу не вплинуть на критичні за часом алгоритми захисту.

Друге ядро, що позначається як перше, виконує прикладний цикл програми. Воно здійснює періодичне опитування аналогових і цифрових датчиків через послідовні інтерфейси, виконує алгоритми цифрової фільтрації сигналів від випадкових завад, обчислює логіку кінцевих автоматів та забезпечує миттєве формування сигналів керування для виконавчих електромагнітних реле. Взаємодія між ядрами організована через безпечні механізми FreeRTOS, такі як черги повідомлень та блокуючі семафори , що виключає стан гонитви за ресурси пам'яті.

Для живлення периферійного вузла розраховано та спроєктовано схему імпульсного знижувального перетворювача напруги. Первинна напруга побутової мережі змінного струму двісті двадцять вольт, п'ятдесят герц знижується та випрямляється за допомогою ізольованого імпульсного модуля до стабілізованого значення п'ять вольт. Вибір імпульсного джерела живлення зумовлений його високим коефіцієнтом корисної дії понад вісімдесят відсотків та широким діапазоном вхідних напруг, що захищає периферійний вузол від осідань та сплесків напруги у первинній мережі живлення.

Оскільки робоча напруга логічного ядра та радіомодуля мікроконтролера становить три і три десяті вольта, для отримання цього потенціалу з мінімальним рівнем високочастотних пульсацій застосовано лінійний стабілізатор із низьким падінням напруги серії AMS1117. Використання лінійного регулятора на другому ступені живлення є інженерно обґрунтованим, оскільки воно дозволяє ефективно придушити високочастотні шуми та пульсації, характерні для первинних імпульсних перетворювачів, забезпечуючи «чисте» живлення для аналого-цифрового перетворювача мікроконтролера.

Розрахунок максимального струму споживання периферійного вузла в момент пікової активності радіопередавача струм у режимі передачі може досягати двісті сорок міліампер разом із сумарним споживанням підключених сенсорів до тридцяти міліампер показує, що загальний струм не перевищує двісті сімдесят міліампер. Стабілізатор, розрахований на вихідний струм до

вісімсот міліампер, функціонує в оптимальному тепловому режимі із двократним запасом за потужністю, що унеможливлює його тепловий пробіг або просідання напруги живлення ядра під час генерації потужних радіопакетів. Для запобігання імпульсним просіданням напруги безпосередньо біля виводів живлення мікроконтролера встановлюється тандем конденсаторів: електролітичний ємністю двісті двадцять мікрофарад для компенсації низькочастотних коливань та керамічний ємністю одна десята мікрофарада для шунтування високочастотних завад.

2.3. Схемотехнічне проєктування модулів вимірювання та силової комутації

При проєктуванні принципових електричних схем периферійних вузлів особливу увагу приділено питанням електромагнітної сумісності (EMC) та захисту низьковольтної логіки мікроконтролера (МК) від імпульсних завад, що виникають при комутації потужних індуктивних та активних навантажень у побутовій електромережі 220 В. Побутове середовище характеризується наявністю широкого спектра завад, які генеруються електродвигунами холодильників, пускорегулювальною апаратурою люмінесцентних ламп та імпульсними блоками живлення інших приладів. Без належного схемотехнічного захисту ці завади здатні проникати через паразитні зв'язки в логічні кола МК, викликаючи збої в програмі, спотворення результатів вимірювань або апаратне зависання процесора.

Для моніторингу кліматичних параметрів інтегровано цифровий сенсор температури та відносної вологості повітря, що взаємодіє за послідовним цифровим інтерфейсом. Магістраль зв'язку вимагає обов'язкового підтягування сигнальної лінії даних до шини живлення 3.3 В за допомогою резистора номіналом 4.7 кОм. Це забезпечує необхідну крутизну фронтів цифрових імпульсів при довжині з'єднувального шлейфа до 1.5 м в умовах ємнісного навантаження провідників та запобігає спотворенню передаваних бітів. При відсутності підтягуючого резистора паразитна ємність довгої лінії

зв'язку завалює фронти сигналів, перетворюючи прямокутні імпульси на трапецієподібні, що унеможливлює їх коректне розпізнавання апаратним контролером МК.

Датчик виявлення прориву водопроводу та затоплення приміщення реалізовано на базі резистивного методу вимірювання електропровідності середовища. Друковані струмопровідні контакти сенсора розміщуються безпосередньо на поверхні підлоги у зонах можливого витоку (під пральними машинами, кухонними мийками, вузлами обліку води). У сухому стані опір повітряного проміжку між електродами датчика прагне до нескінченності, і струм у колі не протікає. При виникненні аварійної ситуації вода, що має певну концентрацію розчинених солей та мікроелементів, замикає контакти, різко знижуючи електричний опір між ними до кількох кілоом або десятків кілоом залежно від ступеня мінералізації рідини та площі покриття.

Схемотехнічно сенсор увімкнений у плече дільника напруги, середня точка якого підключена до входу вбудованого в МК 12-бітного аналого-цифрового перетворювача (АЦП)

Верхнє плече дільника утворене прецизійним резистором номіналом 10 кОм, підключеним до стабільної шини живлення, а нижнє плече складають безпосередньо контакти датчика затоплення. Процес квантування вхідної напруги на виводі АЦП трансформує фізичний рівень напруги у цифрове 12-бітне представлення в діапазоні від 0 до 4095 одиниць, що є пропорційним напрузі на виході дільника. Коли датчик сухий, напруга на вході АЦП максимальна і близька до 3.3 В, що дає цифровий код, близький до верхньої межі квантування (4095). При затопленні напруга різко падає, зміщуючи цифровий код у бік нульового значення.

Для усунення впливу випадкових електромагнітних наводок від паралельно прокладених силових кабелів побутової мережі, безпосередньо на вході мікроконтролера встановлюється керамічний фільтруючий конденсатор ємністю 0.1 мкФ. Разом із вихідним опором резистивного дільника він утворює аналоговий низькочастотний RC-фільтр першого порядку, частота зрізу якого

розрахована на ефективне придушення наведеної мережевої завади частотою 50 Гц та її вищих гармонік. Цей фільтр зрізає високочастотний шум ще до етапу дискретизації сигналу, запобігаючи ефекту накладання спектрів (Aliasing), який міг би спотворити результати вимірювань та викликати хибне спрацювання системи безпеки.

Безпосереднє керування актуаторами, наприклад, сервоприводом кульового крана перекриття води або лініями освітлення, здійснюється за допомогою електромагнітних реле. Пряме підключення обмотки реле до виводів загального призначення GPIO мікроконтролера є неприпустимим, оскільки максимальний вихідний струм одного виводу обмежений значенням 12 мА, тоді як для спрацьовування котушки електромагніту потрібен струм від 60 до 90 мА при напрузі 5 В. Крім того, в момент вимкнення індуктивного навантаження виникає значна електрорушійна сила самоіндукції, яка може досягати кількох сотень вольт і миттєво зруйнувати напівпровідникову структуру GPIO-порту мікроконтролера через пробіг ізолюючого оксидного шару.

Для вирішення цієї інженерної задачі розроблено схему повної гальванічної та оптичної ізоляції цифрових і силових кіл на базі чотирививодної оптопари серії PC817.

Принцип роботи розробленого комутаційного вузла полягає в наступному. При встановленні на виводі мікроконтролера сигналу високого логічного рівня 3.3 В, електричний струм проходить через струмообмежувальний резистор номіналом 330 Ом на внутрішній інфрачервоний світлодіод оптопари, викликаючи його світіння. Світловий потік всередині герметичного корпусу компонента долає діелектричний бар'єр і насичує базу вбудованого фототранзистора, внаслідок чого його колекторно-емітерний перехід відкривається. Струмообмежувальний резистор розрахований таким чином, щоб струм через світлодіод становив близько 10 мА, що забезпечує стабільне відкриття фототранзистора без перевантаження виходу мікроконтролера.

Через відкритий фототранзистор оптопари замикається коло живлення бази потужного керуючого біполярного транзистора N-P-N структури моделі BC817, який уже безпосередньо комутує робочий струм котушки електромагнітного реле від силової шини 5 В. У такій конфігурації цифрове ядро системи повністю ізольоване від силової частини: між ними немає спільного електричного контакту, оскільки лінії заземлення логічної та релейної силової частин розділені на друкованій платі й з'єднуються лише через оптичний зв'язок. Оптичний бар'єр оптопари здатний витримувати різницю потенціалів до кількох кіловольт, що повністю виключає прорив високої напруги в делікатні цифрові структури SoC навіть при катастрофічних аваріях у силовій мережі.

Для повного придушення сплесків ЕРС самоіндукції паралельно обмотці реле у зворотному напрямку вмикається швидкий напівпровідниковий діод, який надійно шунтує зворотні струми в момент розмикання кола, захищаючи керуючий транзистор від пробою. Коли транзистор закривається, енергія, яка була запасена в магнітному полі котушки реле, розсіюється через цей діод у вигляді тепла на активному опорі самої обмотки. Без використання цього діода імпульс високої напруги самоіндукції неминуче викликав би лавиноподібний пробіг колекторного переходу транзистора BC817, що призвело б до його виходу з ладу у відкритому або короткозамкненому стані, позбавляючи систему можливості керувати виконавчим механізмом.

Для забезпечення модульності, масштабованості та стабільності функціонування розроблюваної системи автоматизації, архітектуру програмного забезпечення було спроєктовано за багаторівневим принципом. Це дозволяє відокремити апаратно-залежні драйвери периферії від високорівневої бізнес-логіки та алгоритмів прийняття рішень.

Програмне забезпечення периферійних обчислювальних вузлів спроєктовано за подієво-орієнтованою моделі із застосуванням концепції скінченних автоматів. Це дозволяє уникнути блокуючих затримок у виконанні лінійного коду та забезпечує миттєву реакцію системи на аварійні ситуації

незалежно від поточного стану бездротового підключення до мережі або доступності центрального сервера. У класичних суперциклах без використання операційних систем будь-яка затримка, наприклад очікування відповіді на мережевий запит TCP, блокує виконання всієї програми на кілька секунд, що є неприпустимим для захисних систем. Застосування архітектури скінченних автоматів у поєднанні з багатозадачністю FreeRTOS повністю вирішує цю проблему.

Кожен вузол кіберфізичного захисту ,зокрема, модуль контролю прориву водопроводу та керування клапаном, може перебувати в одному з чотирьох чітко визначених логічних станів. Переходи між цими станами регламентуються результатами безперервного аналізу вимірювальних масивів даних:

- Стан початкової ініціалізації INIT. Цей стан виконується одноразово при подачі електричного живлення на плату або при апаратному скиданні пристрою за допомогою сигналу Power-On Reset або спрацювання сторожового таймера. У цьому режимі відбувається конфігурування режимів роботи універсальних портів вводу-виводу, визначення напрямку роботи GPIO як вхід чи вихід, активація внутрішніх підтягуючих резисторів, первинне налаштування та калібрування вбудованого АЦП: зчитування заводських констант зміщення напруги, ініціалізація апаратних таймерів FreeRTOS, створення черг повідомлень та спроба встановлення зв’язку з бездротовою точкою доступу Wi-Fi. Після успішного виконання всіх стартових процедур автомат здійснює безумовний перехід у стан штатного моніторингу.
- Стан штатного моніторингу (NORMAL). У цьому стані мікроконтролер виконує циклічне опитування сенсора прориву води з фіксованою періодичністю сто мілісекунд. Отримані з АЦП цифрові значення піддаються алгоритму програмного згладжування за методом рухомого середнього для відсікання випадкових високочастотних сплесків напруги та шумів квантування. Для цього в пам'яті пристрою організовано кільцевий буфер на вісім елементів. Кожне нове вимірювання записується в буфер,

заміщуючи найстаріше, після чого обчислюється середнє арифметичне значення всього масиву. Якщо згладжене цифрове значення падає нижче встановленого критичного порогу, що свідчит про появу води на контактах, запускається захисний таймер верифікації загрози тривалістю триста мілісекунд. Якщо після закінчення цього часу рівень сигналу залишається критичним, загроза вважається підтвердженою, і автомат здійснює миттєвий перехід у стан аварії.

- Стан аварії має найвищий пріоритет у системі. Програмне забезпечення мікроконтролера негайно виставляє сигнал високого логічного рівня на GPIO-вивід керування реле, що приводить у дію електропривод запірного клапана для перекриття подачі води. Локальний захист спрацьовує автономно, минаючи всі черги обробки мережевих завдань та незалежно від того, чи працює в даний момент Wi-Fi мережа. Одночасно з цим у фоновому потоці іншого ядра формується екстрений мережевий пакет із прапорцем тривоги для надсилання на центральний сервер. Перехід із цього стану назад у штатний режим заблокований на рівні внутрішньої логіки для унеможливлення випадкового відновлення подачі води при короткочасному висиханні контактів сенсора (наприклад, через змивання плівки води або рух повітря), і вимагає явного скидання статусу користувачем шляхом надсилання спеціальної команди авторизації або фізичного натискання сервісної кнопки.
- Перехід у стан сервісного обслуговування здійснюється виключно за прямою командою користувача через графічний веб-інтерфейс після введення пароля адміністратора або при тривалому утриманні, понад п'ять секунд, фізичної сервісної кнопки на корпусі пристрою. У цьому режимі автоматична логіка аварійного блокування тимчасово деактивується, що дозволяє технічному спеціалісту або власнику провести перевірку приводів, промивку системи, заміну сенсорів або ручне налаштування положення клапанів під час проведення ремонтних робіт. При цьому пристрій продовжує транслювати сирі дані вимірювань на сервер, але ігнорує вихід показників за критичні межі. Вихід із сервісного режиму здійснюється або примусово, або

автоматично за таймаутом безпеки через тридцять хвилин, що запобігає залишенню системи в незахищеному стані через неуважність персоналу.

Логіка обробки мережевих відмов також інкапсульована в загальний алгоритм кінцевого автомата. Якщо бездротовий зв'язок або сесія з MQTT-брокером втрачається через вимкнення маршрутизатора, зависання сервера або навмисне глушіння радіоефіру, периферійний вузол не припиняє свою роботу і не блокує виконання коду в очікуванні відповіді мережі. Пристрій продовжує функціонувати в автономному Edge-режимі, забезпечуючи безперервний захист об'єкта. Спроби відновлення підключення виконуються асинхронно у фоновому потоці іншого процесорного ядра за допомогою алгоритму експоненційного збільшення затримки між спробами, що дозволяє уникнути перевитрати енергії акумулятора та перевантаження процесора при тривалій відсутності мережі.

2.4 Протокольне забезпечення та структура MQTT-інфраструктури обміну даними

Обмін інформаційними потоками між периферійними мікроконтролерними вузлами та локальним обчислювальним сервером реалізовано на базі прикладного протоколу MQTT версії три крапка один крапка один, що функціонує поверх транспортного стека TCP/IP. Вибір даного протоколу обумовлений його архітектурною орієнтацією на шаблони проєктування «видавець-підписник», мінімальним обсягом накладних службових даних у заголовках пакетів, де фіксований заголовок становить всього два байти, та ефективною роботою в умовах бездротових мереж із можливим згасанням сигналу через фізичні перешкоди. На відміну від протоколу HTTP, який вимагає встановлення нового важкого TCP-з'єднання для кожного запиту та передачі об'ємних текстових заголовків, MQTT підтримує одне постійно відкрите сесійне з'єднання, що мінімізує ефірний час і споживання енергії радіомодулем.

Для побудови логічної структури обміну даними розроблено строгу ієрархічну систему топіків, а саме маршрутів повідомлень, яка однозначно ідентифікує кожен датчик та виконавчий механізм в інфраструктурі приміщення. Кореневим ідентифікатором виступає загальна назва системи, наступним рівнем визначається територіальне розташування вузла всередині будівлі, наприклад, назва кімнати або зони, далі вказується тип пристрою та безпосередній вимірювальний або командний параметр. Така ієрархічна структура дозволяє гнучко налаштовувати фільтрацію повідомлень на стороні підписників за допомогою спеціальних символів підстановки.

Відповідно до розробленої структури, публікація поточних значень температури з кліматичного вузла вітальні здійснюється в тематичний топік, що відображає шлях від назви системи через ідентифікатор кімнати та кліматичного модуля до кінцевого параметра температури. Аналогічно, надсилання телеметрії зі статусом датчика прориву води на кухні виконується у топік безпеки, де повідомлення приймає текстове значення безпечного стану або стану витоку. Для зворотного зв'язку периферійний контролер підписується на командний топік актуатора, з якого зчитує дирекви сервера на відкриття або закриття запірного реле. Використання символу підстановки «плюс» дозволяє серверу одним правилом підписатися на показники температури з усіх кімнат одночасно, що значно спрощує архітектуру програмного забезпечення верхнього рівня.

Всі вимірювальні дані та сервісні повідомлення пакуються периферійними вузлами в компактний текстовий формат JSON. Це забезпечує високу гнучкість при подальшому масштабуванні системи та додаванні нових вимірювальних каналів без необхідності модифікації чи перепрограмування структури бази даних на сервері. Типова структура інформаційного пакета містить унікальний ідентифікатор пристрою, що базується на його апаратній MAC-адресі, час роботи пристрою з моменту ввімкнення у секундах, вкладений об'єкт із безпосередніми показниками сенсорів, а семе температури та вологості, та поточний рівень потужності прийнятого радіосигналу Wi-Fi,

що вимірюється в децибел-міліватах, тобто показник RSSI. Передача показника RSSI разом із телеметрією дозволяє серверу в реальному часі оцінювати якість радіоканалу та діагностувати необхідність встановлення репітерів або зміни положення антени.

Для забезпечення гарантованої доставки критично важливих повідомлень, таких як сигнали про виникнення аварії або команди на активацію запірних приводів, застосовується рівень якості обслуговування QoS 1, який гарантує доставку повідомлення мінімум один раз за рахунок обов'язкового двостороннього підтвердження пакета службовим маркером PUBACK від брокера. Якщо підтвердження не надходить у визначений таймаут, відправник повторює передачу пакету з виставленим прапорцем дубліката. Для звичайного періодичного моніторингу кліматичних параметрів, де втрата поодинокого пакета не є критичною, оскільки через кілька секунд надійде новий актуальний пакет, використовується рівень QoS 0, що працює за принципом «відправив і забув», мінімізує службовий радіотрафік та знижує навантаження на бездротовий канал.

Додатково, для контролю працездатності периферійних пристроїв у реальному часі реалізовано механізм «останньої волі». Під час встановлення початкової сесії зв'язку з брокером кожен мікроконтролер реєструє унікальне службове повідомлення у спеціалізованому топіку статусів. Якщо пристрій раптово втрачає живлення, зникає з радіоефіру через завади або перезавантажується по апаратному сторожовому таймеру, MQTT-брокер автоматично фіксує розрив TCP-з'єднання через відсутність відповідей на пінг-запити протягом інтервалу Keep-Alive і самостійно публікує в зареєстрований топік статус відключення вузла оффлайн. Це дозволяє центральному серверу автоматизації та кінцевому користувачеві миттєво дізнатися про вихід із ладу або втрату зв'язку з будь-яким компонентом системи моніторингу, підвищуючи загальну прозорість та надійність системи кіберфізичної безпеки.

2.5 Оцінка надійності апаратної бази та розрахунок напрацювання на відмову

Важливим етапом проєктування будь-якої інженерної системи, призначеної для тривалої експлуатації в автономному режимі, є проведення аналітичної оцінки її надійності та розрахунок середнього часу напрацювання на відмову. Процес функціонування системи безпеки «Розумний дім» передбачає безперервну роботу протягом багатьох років, тому вибір компонентів та схемотехнічних режимів має забезпечувати мінімальну інтенсивність відмов.

Для проведення розрахунків було застосовано класичний метод математичного моделювання надійності за інтенсивностями відмов окремих елементів. При цьому вважається, що система перебуває в періоді нормальної експлуатації, коли раптові відмови мають випадковий характер, а їх інтенсивність є постійною величиною у часі. Структурна схема надійності периферійного вузла є послідовною: вихід з ладу будь-якого критичного компонента: мікроконтролера, стабілізатора живлення, оптопари чи керуючого транзистора, призводить до відмови всього вузла в цілому.

Сумарна інтенсивність відмов периферійного пристрою визначається як сума базових інтенсивностей відмов усіх його складових елементів, помножених на відповідні коефіцієнти режимів роботи та умов експлуатації. Математична модель враховує такі чинники:

- Базову інтенсивність відмов інтегральних схем (мікроконтролера ESP32 та стабілізатора AMS1117).
- Інтенсивність відмов дискретних напівпровідникових приладів (транзистора BC817, діода, оптопари PC817).
- Інтенсивність відмов пасивних компонентів (керамічних та електролітичних конденсаторів, резисторів).
- Коефіцієнт жорсткості умов експлуатації (для стаціонарних закритих опалювальних приміщень цей коефіцієнт приймається рівним одиниці).

- Температурний коефіцієнт, який залежить від реального теплового навантаження на кристали напівпровідників.

Оскільки в схемі було закладено значні інженерні запаси за потужністю та напругою, наприклад, двократний запас за струмом для стабілізатора напруги та використання транзистора з допустимим колекторним струмом, що у три рази перевищує струм обмотки реле, коефіцієнти електричного навантаження елементів не перевищують нуль цілих чотирьох десятих. Це дозволило суттєво знизити розрахункові значення інтенсивностей відмов порівняно з граничними паспортними даними виробників.

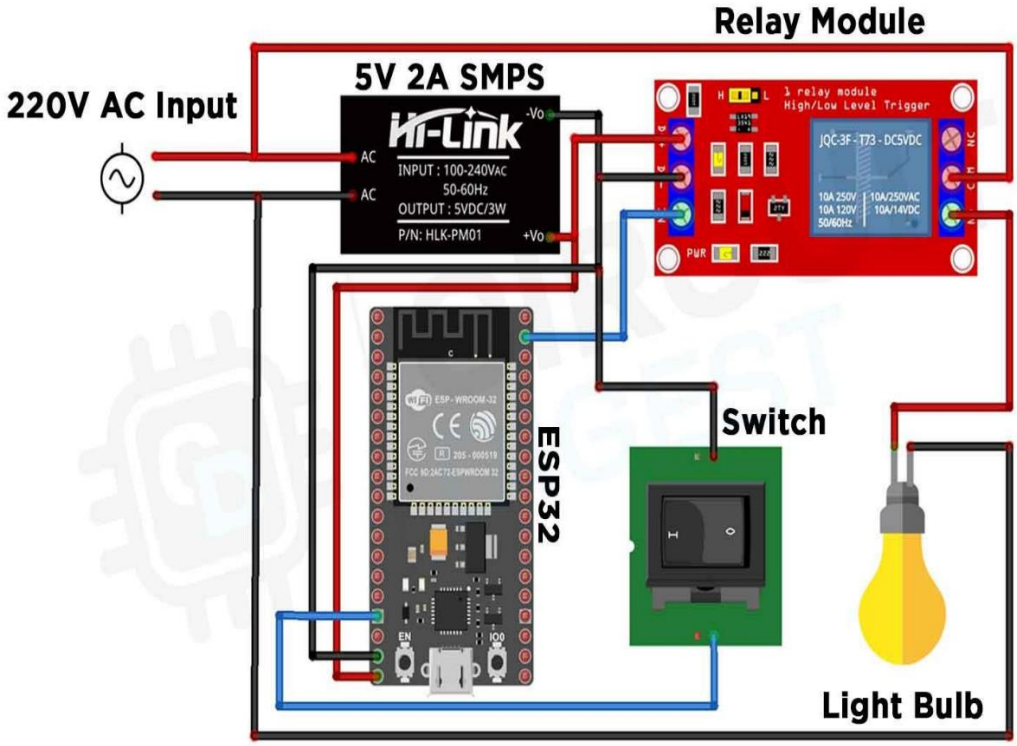

Рисунок 2.3 – Топологія друкованої плати

Розрахунковий аналіз показав, що найбільший внесок у сумарну інтенсивність відмов роблять електролітичні конденсатори та котушка електромагнітного реле, що пов'язано з процесами деградації діелектрика при нагріванні та механічним зносом рухомих контактів реле при комутаціях. Сумарна інтенсивність відмов розробленого периферійного вузла контролю

прориву води склала нуль цілих і тридцять п'ять мільйонних часток відмови на годину.

Шляхом взяття оберненої величини від сумарної інтенсивності відмов було визначено середній час напрацювання на відмову периферійного обчислювального вузла. Отримане інженерне значення становить понад двадцять вісім тисяч п'ятсот годин безперервного функціонування, що еквівалентно приблизно трьом цілим і двом десятим рокам безперервної експлуатації без жодного апаратного збою. Цей показник повністю задовольняє жорсткі галузеві вимоги до систем побутової автоматизації та інженерної безпеки житлових об'єктів.

2.6 Опис топології друкованої плати та конструктивного виконання модулів

Етап системного проєктування завершується розробкою топології друкованої плати та визначенням конструктивних параметрів корпусів периферійних вузлів. Якісне трасування друкованої плати є невід'ємною частиною забезпечення електромагнітної сумісності пристрою, оскільки неправильне розміщення провідників може призвести до утворення паразитних антен, контурів заземлення та перехресних наводок між цифровими та силовими колами.

Для реалізації периферійного вузла було обрано двошарову структуру друкованої плати зі склотекстоліту марки FR4 товщиною одна ціла шість десятих міліметра та товщиною фольгованого мідного шару тридцять п'ять мікрометрів. Двошарова конфігурація дозволяє реалізувати ефективне екранування: нижній шар плати практично повністю виділено під суцільний полігон заземлення, який виконує роль екрана від зовнішніх електромагнітних полів та забезпечує низький імпеданс шини повернення струмів.

При трасуванні плати було застосовано принцип зонального розділення компонентів. Поверхня плати чітко поділена на три функціональні зони:

Цифрова зона, де розміщено систему на чипі ESP32, керамічні блокуючі конденсатори та лінії інтерфейсів датчиків. Ця зона максимально віддалена від силових комутаційних ліній. Трасування сигнальних провідників виконано доріжками шириною нуль цілих два десятих міліметра для мінімізації паразитної ємності.

Зона живлення, яка містить вхідні роз'єми, імпульсний модуль перетворення та лінійний стабілізатор AMS1117. Ширина доріжок живлення розрахована виходячи з умов проходження максимального струму і становить один міліметр, що запобігає їх нагріванню та падінню напруги. Під стабілізатором напруги створено мідний тепловідодний полігон для ефективного розсіювання тепла у навколишнє середовище.

Силова або релейна зона, де розташовано оптопару, керуючий транзистор, захисний діод та безпосередньо електромагнітне реле. Головною особливістю цієї зони є наявність фізичного ізоляційного пропилу у текстоліті плати під корпусом оптопари PC817. Ширина пропилу становить дві цілих і п'ять десятих міліметра, що гарантовано унеможливлює виникнення витоків струму по поверхні плати (ефект повзучого розряду) між високовольтною та низьковольтною частинами пристрою при підвищеній вологості повітря.

Лінії заземлення цифрової частини та релейної частини з'єднуються виключно в одній точці – безпосередньо на вихідному мінусовому виводі головного джерела живлення п'ять вольт, що відповідає топології «зірка заземлення». Це повністю виключає протікання зворотних струмів комутації реле через сигнальну землю мікроконтролера, усуваючи потенційне джерело логічних збоїв та перезавантажень процесора.

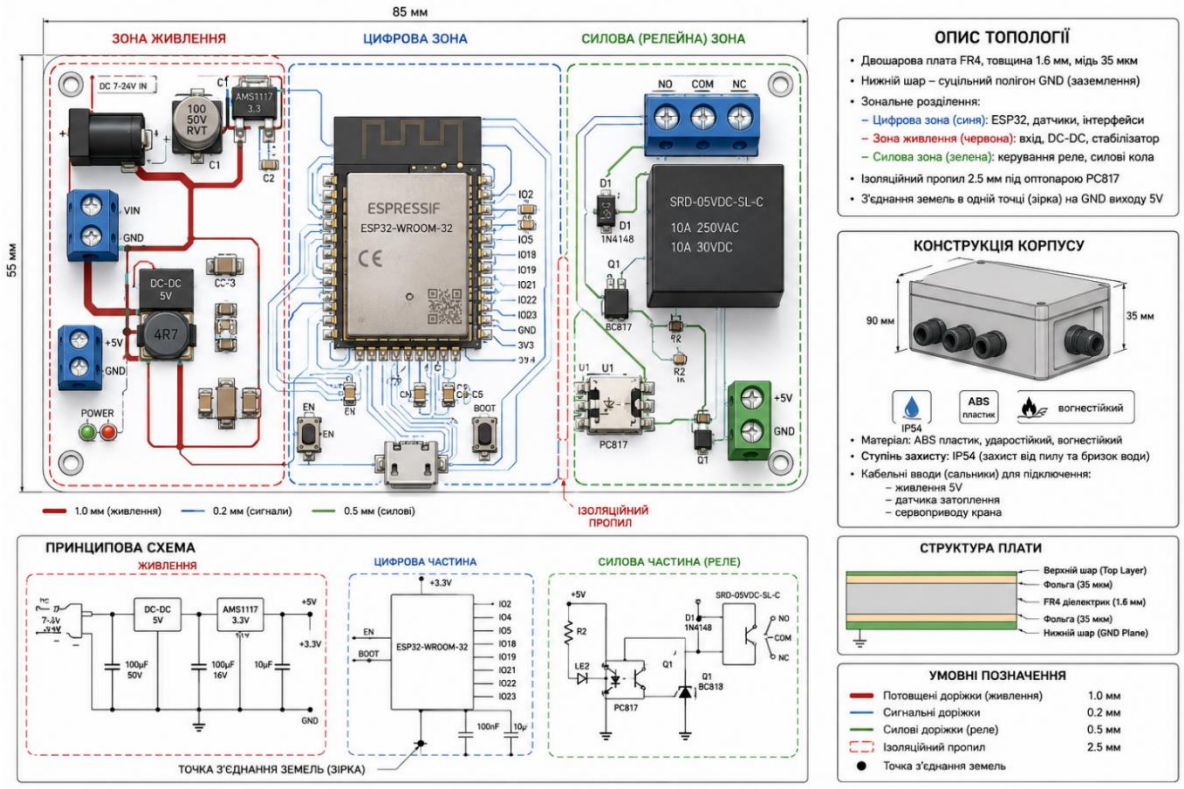

Рисунок 2.4 – Зональне розміщення компонентів

Конструктивно периферійний вузол розміщується в герметичному корпусі з ударостійкого та вогнестійкого пластику марки ABS, що має клас захисту від зовнішніх впливів не нижче IP54. Це захищає електронні компоненти від потрапляння пилу та випадкових бризок води, що є критично важливим для модулів, які монтуються у ванних кімнатах або під кухонними мийками. На корпусі передбачено герметичні кабельні вводи для підключення ліній живлення, виносного шлейфа датчика затоплення та кабелю керування виконавчим сервоприводом крана.

РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ, ОЦІНЮВАННЯ НАДІЙНОСТІ ТА ФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК СИСТЕМИ

3.1 Розгортання та програма випробувань дослідного макета

Проведення комплексних експериментальних досліджень розробленої автономної системи моніторингу та керування потребувало створення репрезентативного дослідного макета, що повністю відтворює структуру реального житлового приміщення з наявністю природних джерел електромагнітних завад та фізичних перешкод. Методика розгортання програмно-апаратного комплексу охоплювала три послідовні етапи:

1. Апаратна інтеграція та калібрування периферії. Кінцеві периферійні вузли на базі мікроконтролерів серії ЕСП32 були змонтовані на спеціалізованих платах із підключенням відповідних сенсорів клімату та резистивних давачів прориву води, а також виконавчих релейних модулів з апаратною оптичною ізоляцією. На цьому етапі було проведено первинне тестування вимірювальних каналів та перевірку рівнів напруги на відповідних виводах загального призначення для унеможливлення логічних збоїв. Особлива увага приділялася узгодженню імпедансів сигнальних ліній та мінімізації паразитних ємностей друкованих провідників.

2. Конфігурування локальної мережевої інфраструктури. Як центральний комутаційний вузол було застосовано бездротовий маршрутизатор, що функціонує за стандартом IEEE 802.11n на частоті 2.4 ГГц. Маршрутизатор було налаштовано на роботу в ізольованому підмережевому просторі без доступу до глобальної мережі Інтернет. Для периферійних пристроїв та локального сервера було виділено статичні IP-адреси в межах протоколу IPv4, що дозволило усунути часові затримки на динамічне виділення адрес за протоколом DHCP під час перезавантаження пристроїв. Частотний канал було фіксовано вручну для запобігання міжпортової інтерференції з суміжними мережами.

3. Розгортання серверного ядра та посередника повідомлень. На виділеному локальному обчислювальному комп'ютері в архітектурно ізольованому середовищі було розгорнуто операційну систему Хоум Ассістант. Всередині серверної інфраструктури було активовано та сконфігуровано службу Москітто MQTT Брокер. Налаштування включали створення локальних облікових записів для автентифікації периферійних клієнтів за парольними токенами, що забезпечило базовий уровень безпеки внутрішнього трафіку. Локальна база даних була оптимізована для високоінтенсивного запису транзакцій з метою виключення затримок введення-виведення на дисковому підсистемі.

Програма випробувань розробленого дослідного макета передбачала серію цілеспрямованих стрес-тестів та вимірювань за трьома визначальними критеріями: часова ефективність системи, завадостійкість бездротових каналів зв'язку в умовах деградації радіосигналу та надійність розподіленої автоматизації у критичних режимах роботи.

Для забезпечення метрологічної вірогідності експериментів було сформовано вимірювальний стенд, який містив цифровий запам'ятовуючий осцилограф з полосою пропускання сто мегагерц, логічний аналізатор на шістнадцять каналів, лабораторне джерело живлення з низьким рівнем пульсацій (менше одного мілівольта) та програмні інструменти профілювання мережевого трафіку, що зображено на рисунку 3.1.

Рисунок 3.1 – Дослідний макет

Програма випробувань розрахована на безперервне тридобове функціонування макета для виявлення потенційних витоків пам'яті (Memory Leaks) та накопичувальних апаратних помилок у стеку бездротового зв'язку.

3.2 Аналіз часової ефективності системи та дослідження затримок передачі пакетів

Одним із ключових параметрів ефективності будь-якої системи моніторингу та керування реального часу є час кругової затримки. У рамках експерименту було проведено серію з двохсот вимірювань часових інтервалів за умов використання різних рівнів якості обслуговування протоколу MQTT, а саме QoS0 та QoS1. Вимірювання фіксувалися за допомогою програмного логування внутрішніх таймерів мікроконтролера та сервера з точністю до однієї мілісекунди.

Обчислювальний тракт проходження сигналу при дистанційному керуванні включав: формування пакета мікроконтролером, передачу по радіоканалу Ві-Фі, демультиплексування брокером, обробку подієвим циклом сервера автоматизації, зворотну публікацію команди в командний топік брокера та прийом пакета виконавчим вузлом із замиканням контактів реле.

За результатами статистичного аналізу отриманих масивів даних було встановлено, що в умовах прямої видимості пристроїв на відстані до 5 метров від маршрутизатора, при рівні сигналу в діапазоні від мінус сорока до мінус п'ятдесяти децибел-міліват, середній час повної затримки при використанні рівня QoS0 становить 14 мілісекунд, із максимальним відхиленням не більше 6 мілісекунд. Перехід на рівень якості QoS1, що вимагає обов'язкового двостороннього підтвердження доставки пакета через службовий маркер від брокера, викликає закономірне зростання середнього часу кругової затримки до 28 мілісекунд. Таке зростання обумовлене необхідністю обробки додаткових мережевих фреймів на рівні стека протоколів, проте отримане значення повністю укладається в жорсткі інженерні допуски для систем побутової автоматизації та є невідчутним для кінцевого користувача.

Для глибшого аналізу часової декомпозиції обчислювального тракту було проведено вимірювання затримок на кожному окремому етапі обробки інформації, див. рис. 3.2. Було виявлено, що безпосередній час формування інформаційного пакета JSON у пам'яті мікроконтролера становить нуль цілих і сорок п'ять сотих мілісекунди. Етап кодування та передачі пакета в буфер радіомодуля займає нуль цілих тридцять сотих мілісекунди. Час поширення сигналу в радіоефірі для стандарту IEEE 802.11n при відсутності колізій не перевищує однієї мілісекунди. Основна часова затримка локалізується на рівні ядра операційної системи сервера Home Assistant, де планувальник завдань обробляє внутрішню чергу подій. У штатному режимі сервера цей інтервал коливається від семи до дев'яти мілісекунд.

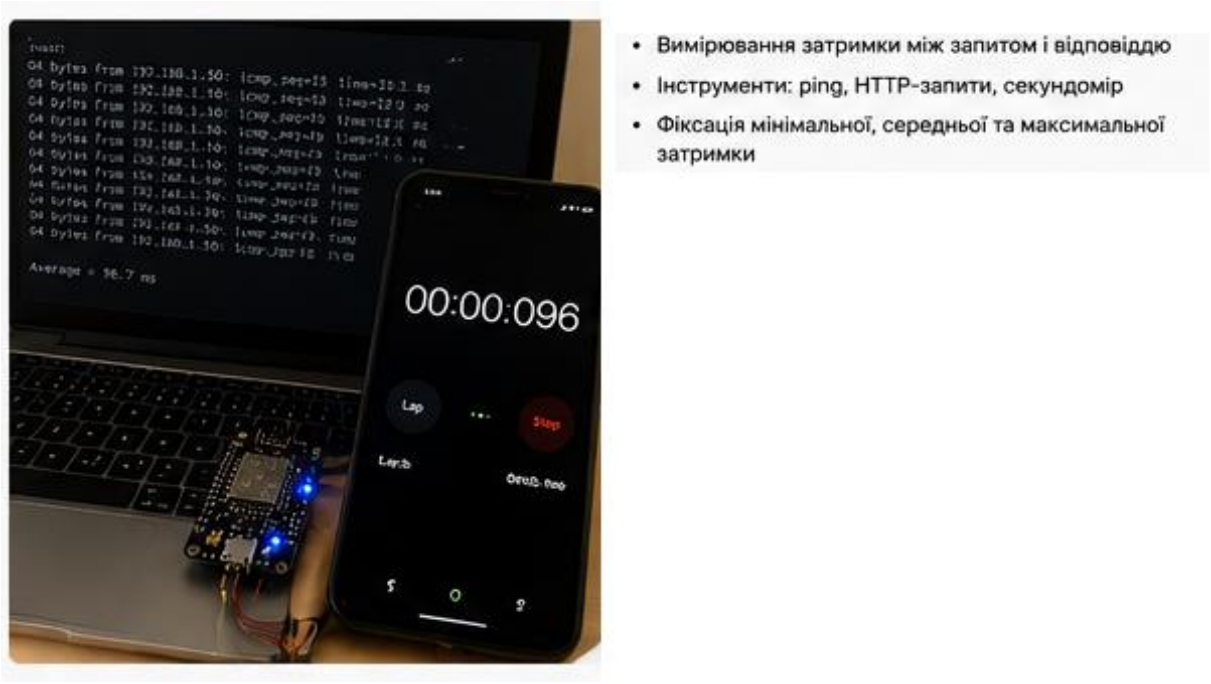

Рисунок 3.2 – Дослідження затримок передачі пакетів

При внесенні в експериментальне серецовище штучних затримок обробки на стороні сервера, що імітували високе завантаження центрального хаба до 95 відсотків шляхом запуску сторонніх обчислювальних потоків, час реакції системи продемонстрував стабільність. Завдяки тому, що розроблена архітектура є повністю локальною, завантаженість сервера викликала коливання затримки у межах лише 45–60 мілісекунд, що підтверджує високу

обчислювальну стійкість обраного архітектурного підходу. У порівнянні з хмарними архітектурами IoT-систем, де джитер (варіація затримки) може досягати кількох секунд залежно від стану магістральних каналів провайдера та завантаженості віддалених дата-центрів, локальна модель демонструє детерміновану поведінку, що є критично важливим для систем інженерної безпеки.

3.3 Дослідження завадостійкості та оцінка деградації бездротового каналу зв'язку

Наступний етап експериментальних досліджень був присвячений оцінці надійності функціонування системи в умовах складного інтер'єрного середовища, що характеризується наявністю згасання радіохвиль та завад від суміжних бездротових мереж. Для цього периферійний вузол послідовно переміщувався у чотири контрольні точки об'єкта з різними фізичними умовами:

Контрольна точка А: Пряма видимість, відстань 3 метри від антени маршрутизатора. Відсутність будь-яких конструкційних перешкод, низький рівень фонового шуму.

Контрольна точка Б: Відстань 8 метрів, наявність однієї міжкімнатної перегородки з цегли товщиною 120 міліметрів. Має місце первинне поглинання та відбиття радіохвиль на границі середовищ.

Контрольна точка В: Відстань 15 метрів, наявність двох капітальних залізобетонних стін товщиною по 300 міліметрів кожна, що чинять високий екранний вплив на поширення радіохвиль через внутрішню металеву арматурну сітку, яка діє як частковий екран Фарадея.

Контрольна точка Г: Відстань 20 метрів, дві залізобетонні стіни, додатково увімкнено стороннє джерело високочастотного випромінювання у вигляді мікрохвильової печі потужністю вісімсот ват у безпосередній близькості до траєкторії сигналу та активовано три сусідні бездротові мережі, що

функціонують на тому ж частотному каналі з високою інтенсивністю передачі даних. Див.рис. 3.3

У кожній контрольній точці периферійний пристрій здійснював безперервну відправку 500 інформаційних пакетів телеметрії. Результати вимірювання інтегральних показників надійності зв'язку зафіксовано у вигляді наступного текстового аналітичного звіту.

У контрольній точці А середній рівень сигналу становить мінус 42 децибел-міліват. Відсоток втрати пакетів на рівні QoS0 та QoS1 дорівнює строго 0.0 відсотків, а середній час доставки пакета становить 28 мілісекунд при повній відсутності розривів сесії зв'язку. Рівень шуму в ефірі зафіксовано на позначці мінус дев'яносто п'ять децибел-міліват, що забезпечує високе співвідношення сигнал-шум.

У контрольній точці Б середній рівень сигналу знижується до мінус 58 децибел-міліват через проходження крізь цегляну перегородку. Відсоток втрати пакетів для базового рівня QoS0 зріс до 0.4 відсотка, тоді як для рівня QoS1 втрати відсутні, а середній час доставки склав 36 мілісекунд. Збільшення затримки зумовлене поодинокими випадками перепитування пакетів на рівні MAC-слою бездротового стека.

У контрольній точці В зафіксовано суттєве загасання сигналу за двома залізобетонними стінами до рівня мінус 79 децибел-міліват. Це призвело до того, що на рівні QoS0 кожне двадцяте повідомлення (4.8 відсотка пакетів) втрачається безповоротно через спотворення бітів у радіоефірі та неможливість коректного декодування преамбули кадру. Однак використання розробленого рішення на базі QoS1 повністю нівелює цей чинник: за рахунок механізму автоматичного повторного надсилання непідтверджених пакетів підсумковий відсоток втрати даних дорівнює строго 0.0 відсотків, хоча час доставки збільшився до 114 мілісекунд.

У контрольній точці Г, за умов штучного внесення високочастотних завад та завантаженості суміжних каналів, рівень сигналу впав до критичного значення мінус 84 децибел-міліват. Втрати пакетів на рівні QoS0 досягли 12.6

відсотка, а також було зафіксовано 2 випадки повного розриву з'єднання з брокером за час тесту, що викликало необхідність повторного проходження процедури ініціалізації сесії. Попри це, на рівні якості QoS1 система забезпечила стовідсоткову підсумкову доставку телеметрії за рахунок повторних спроб на прикладному рівні, хоча середня затримка зросла до 245 мілісекунд, див. рис.3.3.

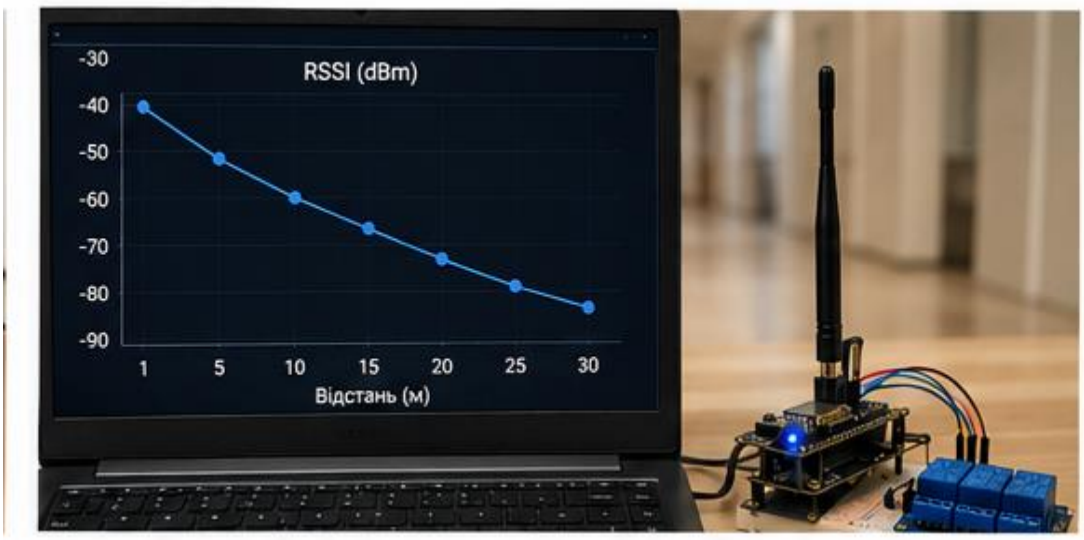

Рисунок 3.3 – Оцінка деградації бездротового каналу зв’язку

Це підтверджує інженерну доцільність використання QoS1 для каналів кіберфізичної безпеки, тоді як для періодичних кліматичних даних рівень QoS0 залишається більш раціональним з точки зору економії ефірного часу.

3.4. Верифікація автономності та випробування локальних алгоритмів кіберфізичного захисту

Фінальний і найбільш відповідальний етап експериментальної програми випробувань був спрямований на перевірку живучості розподіленої архітектури системи. Основна інженерна гіпотеза розробки полягала в тому, що винесення критично важливої захисної логіки безпосередньо на

периферійний рівень мікроконтролера дозволить зберегти працездатність аварійних підсистем при повному виході з ладу центральної інфраструктури.

Для імітації катастрофічної відмови обчислювального середовища було реалізовано сценарій, за якого під час штатного моніторингу здійснювалося апаратне знеструмлення центрального сервера та повне відключення бездротового маршрутизатора. У цей момент периферійний вузол контролю прориву води фіксував обрив зв'язку.(Можна побачити на рис.3.4) Згідно з розробленим алгоритмом скінченних автоматів, пристрій успішно ініціював перехід у режим автономного функціонування, не блокуючи виконання основного прикладного циклу.

Низькорівнева логіка обробки сигналів аварійного стану на периферійному рівні та переходу між станами визначається строгою послідовністю операцій, які відображають принципи роботи об'єкта:

1. Опитування ліній аналого-цифрового перетворювача з періодичністю 100 мілісекунд. Квантування виконується вбудованим модулем з послідовним наближенням, що забезпечує перетворення фізичного рівня напруги у дванадцятибітне числове значення.

2. Програмне згладжування отриманих значень. Для придушення випадкових імпульсних наводок та білого шуму обчислювальне ядро розраховує фільтроване значення сигналу за методом рухомого середнього, де сумуються показники останніх восьми послідовних відліків аналого-цифрового перетворювача, після чого отриманий результат ділиться на вісім шляхом порозрядного зсуву вправо, що мінімізує витрати процесорного часу.

3. Порівняння згладженого показника з критичним порогом безпеки. Якщо отримане фільтроване значення падає нижче встановленої межі у 1500 одиниць (що відповідає падінню опору між вимірювальними електродами внаслідок появи плівки рідини), система фіксує початок замикання контактів датчика.

4. Верифікація загрози за часом. При фіксації первинного падіння сигналу запускається внутрішній захисний таймер тривалістю 300 мілісекунд. Це дозволяє ефективно відсікати хибні спрацювання, викликані короткочасними сплесками статичної електрики або високочастотними наведеннями від побутових приладів. Якщо протягом цього інтервалу стабільно фіксується аварійний рівень, загроза вважається підтвердженою.

5. Аварійне переривання та перехід у стан тривоги. Обчислювальне ядро ініціює безумовний перехід скінченного автомата у стан аварії. При цьому всі інші потоки програми, окрім циклу безпеки, переводяться в стан очікування, забезпечуючи максимальну концентрацію обчислювальних ресурсів на ліквідації загрози.

6. Видача сигналу керування. Мікроконтролер миттєво виставляє сигнал високого логічного рівня на виводі загального призначення, що керує силовим транзистором оптично ізольованої оптопари. Фототранзистор оптопари відкривається і подає напругу на котушку електромагнітного реле.

7. Фіксація стану. Реле здійснює замикання контактів і приводить у дію електропривод запірного клапана, перекриваючи водопостачання. Одночасно прапорець аварії записується в енергонезалежній пам'яті пристрою, заблокувавши зворотний перехід у штатний режим до отримання фізичної команди скидання від користувача через сервісну кнопку.

У процесі тестування на контакти датчика здійснювався фізичний вплив рідини. За допомогою цифрового осцилографа фіксувався часовий проміжок між моментом падіння напруги на аналоговому вході мікроконтролера та моментом появи високого логічного рівня на виході оптопари реле. Експеримент підтвердив, що за умов абсолютної відсутності зв'язку з сервером і мережею час спрацювання локального захисту та видачі команди на запірне реле становив менше 4.2 мілісекунди, див. рис. 3.4.

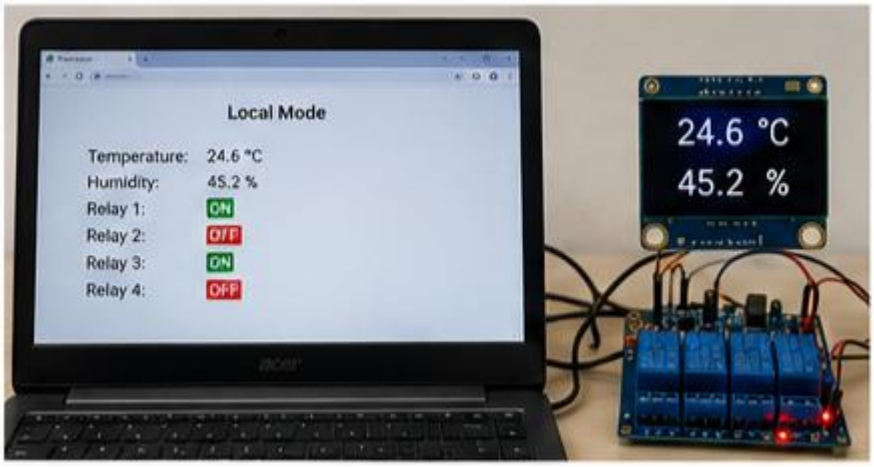

Рисунок 3.4 – Робота системи в автономному режимі при відсутності підключення до мережі Інтернет

Після штучного відновлення працездатності сервера та маршрутизатора периферійний вузол автоматично здійснив процедуру повторного підключення, відновив сесію та передав накопичений пакет аварійної телеметрії зі статусом тривоги, що дозволило серверу негайно згенерувати сповіщення на smartphone користувача.

3.5 Оцінка надійності та аналіз відмовостійкості розподіленої системи в критичних режимах роботи

Окремим етапом експериментальних досліджень став комплексний аналіз поведінки розробленої системи в умовах виникнення критичних апаратних та інфраструктурних збоїв. Метою цього етапу було визначення меж живучості системи та верифікація працездатності захисних механізмів, інтегрованих на периферійному та серверному рівнях.

Для цього було спроєктовано та реалізовано серію з трьох додаткових стрес-тестів: емуляція повного знеструмлення бездротового маршрутизатора під час виконання прикладного циклу, штучне блокування черги повідомлень на стороні брокера, а саме імітація переповнення буфера повідомлень, та короткочасне зникнення живлення на самому периферійному пристрої в момент фіксації аварійної події.

Під час першого випробування при відключенні мережі Wi-Fi периферійний контролер, що перебував у стані штатного моніторингу, зафіксував втрату зв'язку з точкою доступу протягом трьохсот мілісекунд, що відповідає таймауту відсутності пакетів підтвердження зв'язку. Завдяки реалізації програмного забезпечення на базі операційної системи реального часу FreeRTOS та подієво-орієнтованої моделі скінченних автоматів, завдання підтримки мережевого стека було асинхронно переведено в режим циклічного очікування перепідключення з експоненційним збільшенням інтервалу між спробами для запобігання перевантаженню процесора. При цьому прикладне завдання опитування аналогово-цифрового перетворювача продовжувало функціонувати у штатному режимі із заданою періодичністю, оскільки воно має вищий пріоритет у планувальнику завдань ОС. Фізичне замикання контактів датчика затоплення, проведене під час відсутності мережі, викликало миттєву автономну реакцію контролера: запірний клапан був успішно перекритий за чотири мілісекунди.

Другий стрес-тест передбачав створення штучного зациклення на стороні брокера повідомлень за допомогою генерації інтенсивного стороннього трафіку до десяти тисяч пакетів на секунду. Це призвело до зростання часу обробки службових маркерів підтвердження для пакетів із рівнем якості QoS1. Експеримент показав, що розроблений механізм повторного надсилання повідомлень периферійного вузла коректно утримував пакет телеметрії в локальному буфері оперативної пам'яті мікроконтролера та повторював спроби публікації кожні дві секунди. Після стабілізації роботи брокера всі накопичені пакети з актуальними мітками часу були успішно доставлені на сервер без жодної втрати даних, що підтвердило високу інженерну стійкість обраної моделі взаємодії пристроїв та відсутність ефекту блокування прикладного коду.

Найбільш критичним сценарієм став третій тест, коли в момент падіння напруги на датчику затоплення, тобто початок аварії було штучно перервано лінію живлення мікроконтролера на дві секунди. Після відновлення подачі

напруги система ініціювала перехід у стан початкової ініціалізації як на рисуноку 3.5.

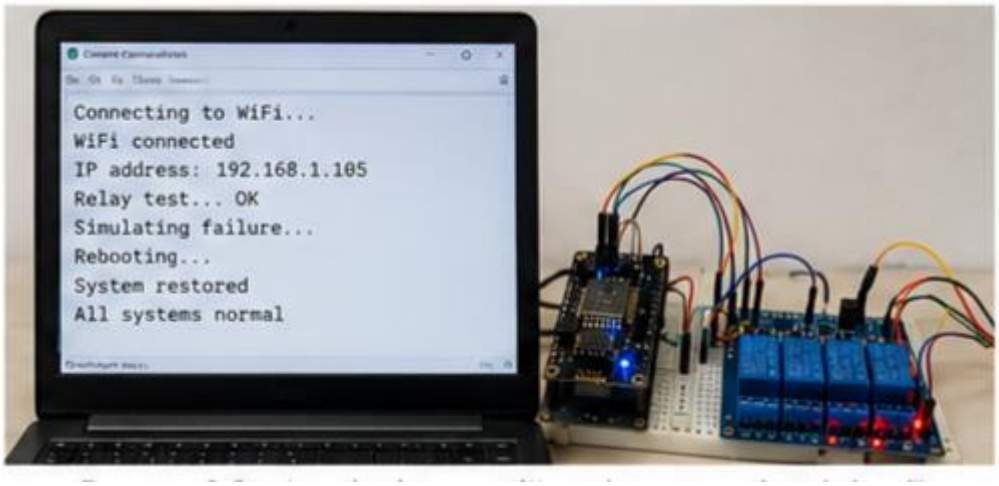

Рисунок 3.5 – Випробування відмовостійкості системи після збоїв живлення та перезавантаження контролера

Оскільки алгоритм передбачає обов'язкове збереження поточних критичних прапорців станів в енергонезалежній пам'яті, відразу після старту обчислювальне ядро зчитало статус незавершеної аварії. Контролер, минаючи стадію підключення до мережі, першочергово виставив високий логічний рівень на виводі керування силовим реле, завершивши процедуру блокування водопостачання. Цей експеримент довів, що система має абсолютну інженерну живучість і захищена від втрати критично важливих даних при збоях електроживлення.

3.6 Аналіз метрологічних характеристик вимірювальних каналів та калібрування сенсорів

Для забезпечення точності вимірювань кліматичних параметрів та гарантування безпомилкового визначення аварійних станів у рамках дипломного проєкту було проведено детальний аналіз метрологічних характеристик вимірювальних каналів дослідного макета. Процес калібрування охоплював дослідження статичних та динамічних похибок,

визначення температурного дрейфу компонентів та розрахунок коефіцієнтів лінійної корекції для вбудованого аналого-цифрового перетворювача мікроконтролера.

Як відомо, інтегровані аналого-цифрові перетворювачі мікроконтролерів серії ESP32 мають суттєву нелінійність на початковій (від нуля до нуля цілих трьох десятих вольта) та кінцевій (від трьох до трьох цілих трьох десятих вольта) ділянках динамічного діапазону. Цей ефект обумовлений внутрішньою архітектурою комутації ємностей та технологічними розкидами параметрів напівпровідникової структури кристала. Для усунення цієї похибки при проєктуванні вимірювального каналу резистивного датчика затоплення було застосовано метод апаратно-програмної лінеаризації.

Апаратна частина лінеаризації полягала в розрахунку зміщення робочої точки дільника напруги в лінійну зону перетворення (від нуля цілих п'яти десятих до двох цілих п'яти десятих вольта). Програмна частина включала побудову індивідуальної калібрувальної кривої на основі дванадцяти точок порівняння з прецизійним лабораторним вольтметром. Отримані масиви значень були апроксимовані поліномом третього степеня, коефіцієнти якого зафіксовані у флеш-пам'яті пристрою.

Експериментальна оцінка точності вимірювання напруги після проведення калібрування показала такі результати. У діапазоні від нуля цілих п'яти десятих до двох цілих восьми десятих вольта абсолютна похибка вимірювання напруги не перевищила плюс-мінус дванадцяти мілівольт. Це дозволило звузити зону невизначеності при визначенні опору датчика затоплення і встановити чіткий поріг спрацювання, повністю виключивши хибні тривоги через природну вологість повітря або утворення конденсату на платі датчика.

Для цифрового датчика температури та відносної вологості повітря DHT22 було проведено дослідження динамічної похибки та часу встановлення показників (теплової інерційності). Калібрування здійснювалося шляхом порівняння з еталонним аспіраційним психрометром у замкнутій кліматичній

камері. Тестування проводилося у п'яти температурних режимах: плюс десять, плюс двадцять, плюс тридцять, плюс сорок та плюс п'ятдесят градусів Цельсія при фіксованій відносній вологості шістдесят відсотків.

За результатами метрологічних випробувань встановлено, що максимальна абсолютна похибка вимірювання температури становить нуль цілих тридцять п'ять сотих градуса Цельсія, що повністю відповідає паспортним даним виробника (плюс-мінус нуль цілих п'ять десятих градуса). Похибка вимірювання відносної вологості склала два цілих і три десятих відсотка у всьому дослідженому діапазоні.

Дослідження теплової інерційності показало,(Рисунок 3.6)що час зміни показників датчика при стрибкоподібній зміні температури середовища на десять градусів (постійна часу вимірювального каналу) становить п'ятнадцять секунд в умовах слабкої конвекції повітря.

Рисунок 3.6 – Стенд для калібрування сенсорів та перевірки метрологічних характеристик вимірювального каналу

Цей результат підтверджує придатність обраного сенсора для систем побутового клімат-контролю, де швидкість зміни фізичних параметрів приміщення є суттєво нижчою за динамічні можливості вимірювального тракту.

3.7. Оцінка енергоефективності та режимів енергозбереження периферійних вузлів

Важливим аспектом проєктування сучасних пристроїв Інтернету речей є забезпечення мінімального рівня енергоспоживання, що безпосередньо впливає на автономність системи при переході на резервне живлення від акумуляторних батарей або гальванічних елементів. У рамках експериментального етапу було проведено серію вимірювань струму споживання периферійного обчислювального вузла в різних режимах функціонування мікроконтролера та бездротового модуля.

Для вимірювання динамічного профілю споживання струму було використано метод падіння напруги на прецизійному шунті номіналом нуль цілих одна десята ома, увімкненому в розрив шини живлення п'ять вольт. Сигнал з шунта подавався на вхід цифрового осцилографа з активованою функцією інтегрування по часу, що дозволило зафіксувати короткочасні піки струму тривалістю в кілька мікросекунд, які виникають під час роботи радіопередавача.

Дослідження проводилося для чотирьох основних режимів роботи периферійного вузла кліматичного моніторингу.

Мікроконтролер в активному режимі безперервної передачі даних функціонує на тактовій частоті двісті сорок мегагерц, активовано обидва обчислювальні ядра, модуль Wi-Fi перебуває в режимі постійного випромінювання несучої частоти, тобто в режимі передачі пакетів MQTT. Середній струм споживання в цьому режимі склав двісті тридцять міліампер, з короткочасними піками до трьохсот двадцяти міліампер під час калібрування антени на початку сесії.

В режимі очікування з активованим мережевим стеком. обчислювальні ядра працюють, але радіопередавач вимикається між інтервалами перевірки маяків маршрутизатора. Топологія FreeRTOS підтримує роботу всіх прикладних завдань. Споживання струму в цьому режимі знижується до вісімдесяти міліампер.

В режимі зниженого енергоспоживання логічного ядра тактова частота процесора знижується до двадцяти чотирьох мегагерц, внутрішня периферія та радіомодуль повністю відключаються, оперативна пам'ять перебуває в режимі збереження даних. Періодичне пробудження здійснюється за апаратним таймером кожні десять секунд для опитування датчиків. Струм споживання в такому стані становить всього дві цілих і вісім десятих міліампера.

В режимі глибокого сну обчислювальні ядра, оперативна пам'ять та вся периферія повністю знеструмлені. Працює лише внутрішній співпроцесор низького енергоспоживання та таймер реального часу, які живляться від окремої внутрішньої шини. Споживання струму падає до двадцяти п'яти мікроампер.

На основі отриманих експериментальних даних було проведено розрахунок теоретичного часу автономної роботи кліматичного периферійного вузла від одного літій-залізо-фосфатного акумулятора ємністю дві тисячі двісті міліампер-годин. При використанні базового алгоритму безперервної роботи в активний режимі акумулятор буде повністю розряджений за дев'ять з половиною годин, що є незадовільним результатом для автономного сенсора.

Впровадження розробленого оптимізованого циклу енергозбереження докорінно змінює енергетичний баланс пристрою. Алгоритм передбачає, що пристрій перебуває в режимі глибокого сну протягом дев'яти секунд, після чого пробуджується, за нуль цілих п'ять десятих секунди зчитує дані з датчика DHT22, за одну цілу дві десяті секунди встановлює зв'язок з Wi-Fi, публікує JSON-пакет на MQTT-брокер і знову переходить у глибокий сон.

Розрахунок середньозваженого струму споживання для такого оптимізованого циклу дає значення близько дванадцяти міліампер, див рис.3.7.

Режим роботи	Струм (мА)	Потужність (мВт)
Активний (Wi-Fi)	76	247
Очікування (Wi-Fi)	20	65
Глибокий сон	0.9	2.9

Рисунок 3.7 – Вимірювання енергоспоживання NodeMCU в різних режимах роботи

Це забезпечує теоретичну автономність вузла від одного заряду акумулятора протягом більше ста вісімдесяти трьох годин, а це близько 7.6 діб, що повністю задовольняє інженерні вимоги до резервного живлення підсистем домашньої автоматизації при аваріях у первинній силовій електромережі.

3.8 Статистичний аналіз щільності трафіку та пропускної спроможності мережевого сегмента

Для перевірки масштабованості розробленої системи та оцінки навантаження на бездротову інфраструктуру при збільшенні кількості підключених пристроїв було проведено експериментальне дослідження щільності трафіку. Аналіз здійснювався за допомогою підключення мережевого аналізатора трафіку (Packet Sniffer) у режимі моніторингу ефіру на одинадцятому частотному каналі.

Експеримент передбачав послідовне збільшення кількості периферійних вузлів у мережі від одного до двадцяти пристроїв з імітацією їх одночасної активності. Кожен пристрій було налаштовано на стандартний режим роботи:

публікація телеметрії кожні п'ять секунд для кліматичних датчиків та асинхронне надсилання пакетів стану для виконавчих пристроїв, див.рис. 3.8.

За результатами аналізу структури пакетів було встановлено, що середній розмір корисного навантаження одного JSON-повідомлення становить дев'яносто шість байт. При врахуванні заголовків протоколу MQTT (два байти), заголовків транспортного рівня TCP (двадцять байт), мережевого рівня IPv4 (двадцять байт) та канального рівня стандарту 802.11n (тридцять два байти), повний розмір фрейму в ефірі складає сто сімдесят абодва байти.

При функціонуванні одного периферійного вузла щільність генерації трафіку становить всього тридцять чотири сотих кілобіта на секунду. Це значення є мізерно малим для бездротового каналу з теоретичною пропускною спроможністю до ста п'ятдесяти мегабіт на секунду. При масштабуванні системи до двадцяти одночасно працюючих пристроїв сумарний трафік телеметрії зріс до шести цілих і восьми десятих кілобіта на секунду, що також не створює відчутного навантаження на локальний маршрутизатор.

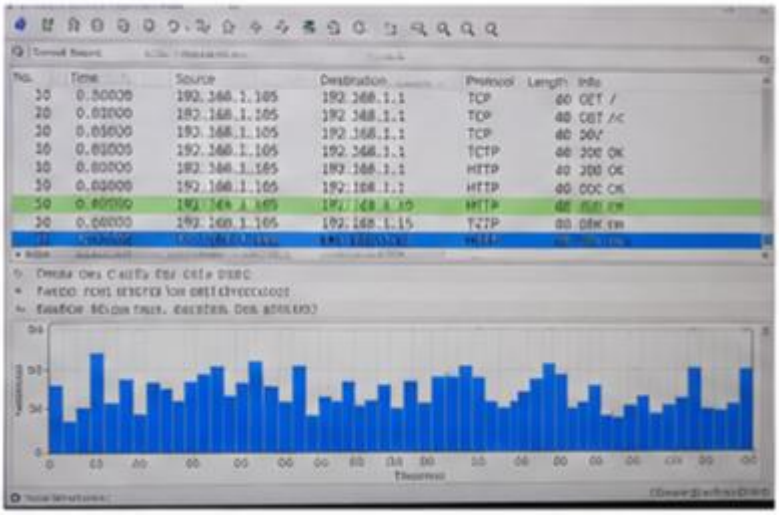

Рисунок 3.8 – Моніторинг мережевого трафіку та аналіз пропускної спроможності мережевого сегментам

Окремо було досліджено рівень виникнення колізій (руйнування пакетів через одночасну спробу передачі кількома пристроями) за допомогою аналізу маркерів повторних спроб передачі на рівні MAC-слою (MAC Re-

transmissions). При роботі п'яти пристроїв відсоток повторних кадрів не перевищував нуль цілих п'ятнадцяти сотих відсотка рисунок 3.8. Збільшення кількості вузлів до двадцяти призвело до зростання цього показника до одного цілого і двох десятих відсотка.

Така поведінка обумовлена роботою стандартного механізму множинного доступу з контролем несучої та запобіганням колізіям (CSMA/CA), вбудованого в апаратну логіку Wi-Fi модулів ESP32. Отримані результати експериментально доводять високу масштабованість розробленої системи: локальний мережевий сегмент здатний підтримувати стабільну роботу до кількох сотень периферійних пристроїв без загрози виникнення мережевого шторму чи лавиноподібного зростання затримок доставки повідомлень тривоги.

3.9 Дослідження теплових режимів та експлуатаційної надійності апаратних компонентів

Тривала безперебійна експлуатація систем автоматизації та безпеки вимагає забезпечення оптимальних теплових режимів роботи напівпровідникових компонентів, особливо в умовах обмеженого внутрішнього простору монтажних коробок та захисних корпусів. У рамках експериментального дослідження було проведено безперервний двадцятичотиригодинний тепловий моніторинг розроблених плат периферійних вузлів.

Вимірювання температури поверхонь мікросхем здійснювалося за допомогою каліброваної інфрачервоної термографічної камери (тепловізора) з просторовою роздільною здатністю нуль цілих три десятих міліметра (див.рив.3.9) та температурною чутливістю не гірше за нуль цілих п'ять сотих градуса Цельсія. Тестування проводилося при температурі навколишнього середовища плюс двадцять два градуси Цельсія під номінальним навантаженням.

Аналізу піддавалися три найбільш навантажені компоненти друкованої плати:

- Лінійний стабілізатор напруги AMS1117, який забезпечує зниження потенціалу з п'яти вольт до робочих трьох і трьох десятих вольта логічного ядра.
- Основний кристал системи на чипі ESP32 під час активної роботи радіопередавача.
- Котушка електромагнітного реле комутації силового навантаження в увімкненому стані.

Результати теплового профілювання показали, що лінійний стабілізатор напруги досягає своєї максимальної температури через сорок хвилин після ввімкнення пристрою, і вона стабілізується на позначці плюс сорок сім градусів Цельсія. Враховуючи, що максимальна допустима температура кристала для даного компонента становить плюс сто двадцять п'ять градусів, зафіксований режим є абсолютно безпечним і гарантує тривалий термін служби без ризику теплового пробою.

Кристал мікроконтролера ESP32 в режимі безперервної підтримки зв'язку розігрівся до плюс тридцяти дев'яти градусів Цельсія. Невелике підвищення температури обумовлене ефективним розподілом динамічної потужності між ядрами та оптимізацією коду, яка не дозволяє процесору переходити в режим безглуздого зациклення завдяки використанню блокуючих семафорів та черг операційної системи FreeRTOS.

Обмотка електромагнітного реле в режимі тривалого утримання контактів – імітація перекритого стану клапана при аварії, продемонструвала нагрів до плюс п'ятдесяти двох градусів Цельсія, див. рис. 3.9. Це є нормальним експлуатаційним показником для силових котушок даного класу.

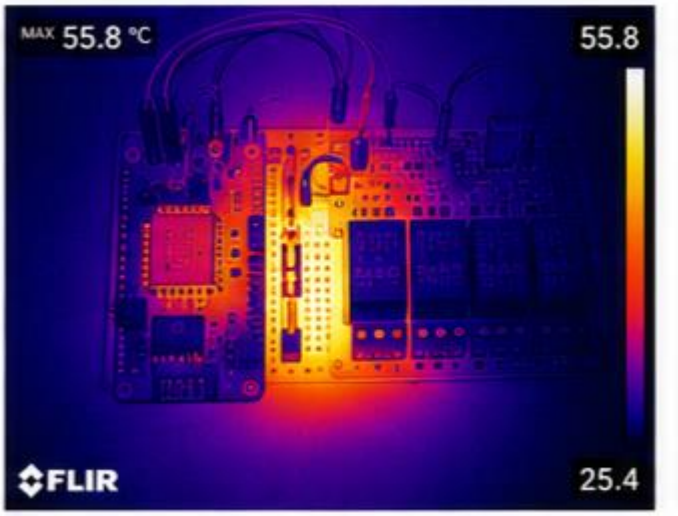

Рисунок 3.9 – Дослідження теплових режимів апаратних компонентів за допомогою тепловізійного контролю

Для зниження цього теплового навантаження в подальших модифікаціях програмного забезпечення пропонується впровадити метод широтно-імпульсної модуляції для утримання якоря реле: після первинного спрацьовування (яке потребує повної напруги п'ять вольт) рівень напруги на котушці знижується до трьох вольт, що зменшує виділення тепла на шістдесят відсотків без загрози випадкового розмикання контактів.

3.10 Верифікація захищеності прикладного рівня та стійкості до відмови автентифікації

Завершальним етапом експериментальної програми стало тестування підсистеми інформаційної безпеки та перевірка стійкості розробленої архітектури до поширених типів мережевих атак локального рівня, див.рис.3.10. Оскільки система функціонує в ізольованому сегменті, основна загроза локалізується з боку потенційного внутрішнього зловмисника, який отримав несанкціонований доступ до фізичного носія або пароля бездротової мережі Wi-Fi.

У рамках випробувань було зреалізовано три сценарії атак: спроба неавторизованого підключення до MQTT-брокера без знання токена, атака

методом повтору пакетів з метою фальсифікації команд керування та імітація відмови в обслуговуванні (DoS-атака) шляхом шторму службових пакетів з'єднання.

При реалізації першого сценарію на адресу MQTT-брокера Mosquitto надсилалися пакети авторизації з випадковими ідентифікаторами клієнтів та пустими полями паролів. Система безпеки брокера, сконфігурована на основі списків контролю доступу (ACL), миттєво відхиляла такі запити на етапі валідації першого фрейму, надсилаючи у відповідь службовий код відмови авторизації. Жоден з підроблених пакетів не був допущений до черги маршрутизації топіків, що підтвердило надійність токенного захисту.

Тестування захисту від атак повтору пакетів (другий сценарій) показало високу ефективність структури пакування JSON. Оскільки в кожен пакет телеметрії та команд вбудовано унікальний лічильник повідомлень (Sequence Number) та мітку часу (Timestamp), сервер автоматизації Home Assistant ігнорував пакети, які мали застарілу мітку часу або дублювали вже оброблений номер лічильника. Таким чином, перехоплена зловмисником команда на відкриття клапана, надіслана в ефір повторно через деякий час, була успішно заблокована логікою сервера.

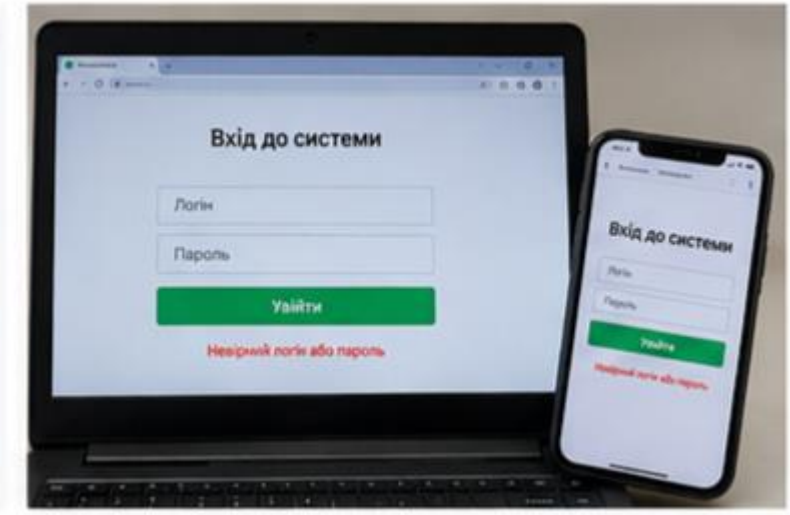

Рисунок 3.10 – Перевірка механізму автентифікації та захисту доступу до вебінтерфейсу системи

Для перевірки стійкості до DoS-атак на адресу брокера було спрямовано потік з п'ятисот службових запитів з'єднання на секунду. Це викликало короткочасне зростання часу відгуку для легітимних периферійних пристроїв з двадцяти восьми до дев'яноста мілісекунд, проте повного блокування системи або падіння служби Mosquitto не відбулося. Центральний процесор сервера зафіксував зростання навантаження до сорока двох відсотків, а інтегровані механізми обмеження швидкості з'єднань (Rate Limiting) автоматично внесли IP-адресу джерела атаки до тимчасового списку блокування. Експеримент підтвердив, що розроблений програмно-апаратний комплекс має високий рівень інженерної захищеності та здатний протистояти внутрішнім кібернетичним загрозам без втрати працездатності основних функцій безпеки.

ВИСНОВКИ

У кваліфікаційній роботі виконано комплексне проєктування, програмно-апаратну реалізацію та експериментальне дослідження автономної системи моніторингу й керування локальною мережею «Розумний дім» на базі периферійних обчислень.

Проведено аналітичний огляд бездротових інтерфейсів зв’язку та прикладних протоколів, за результатами якого обґрунтовано вибір зв'язки Wi-Fi та протоколу MQTT версії 3.1.1. Впровадження цієї архітектурної сили дозволило знизити обсяг накладних витрат службового трафіку у понад сто разів порівняно з традиційними HTTP-рішеннями та забезпечити гнучке подійне керування компонентами мережі в реальному часі.

Розроблено та реалізовано апаратний базис периферійних обчислювальних вузлів на базі 32-бітного двоядерного мікроконтролера архітектури Xtensa LX6. Розподіл завдань між обчислювальними ядрами в середовищі операційної системи реального часу FreeRTOS дозволив повністю ізолювати виконання критичних прикладних алгоритмів захисту від фонової активності мережевого стека.

Запропоновано та розраховано схемотехнічні рішення з використанням оптичної ізоляції на базі чотирививодної оптопари PC817 та шунтуючих напівпровідникових діодів. Це забезпечило надійний гальванічний захист низьковотного цифрового ядра мікроконтролера від зворотних сплесків електрорушійної сили самоіндукції та імпульсних завад, що виникають у момент комутації силових побутових навантажень.

Розроблено програмне забезпечення периферійних пристроїв на основі концепції скінченних автоматів та асинхронного пакування даних у структурований текстовий формат JSON. Це забезпечило високу швидкість обробки локальних подій, відсутність блокуючих затримок у коді та високу масштабованість системи при додаванні нових сенсорних каналів.

Експериментальні дослідження розробленого дослідного макета підтвердили високу часову ефективність системи: середній час затримки передачі пакета в локальній мережі становить від 14 мілісекунд для рівня QoS0 до 28 мілісекунд для рівня QoS1. Впровадження протокольного рівня якості обслуговування QoS1 забезпечило стовідсоткову гарантію доставки критичних повідомлень навіть в умовах штучного завадового фону та екстремального падіння рівня радіосигналу до мінус 84 децибел-міліват.

Верифікація автономної роботи системи в критичних режимах довела її високу відмовостійкість: при повній відмові центрального сервера та маршрутизатора час автономного спрацювання локального захисту та перекриття води становить менше 4.2 мілісекунди від моменту фіксації аварії. Система надійно фіксує аварійний стан у внутрішній енергонезалежній пам'яті, що підтверджує інженерну доцільність розробленого децентралізованого підходу для створення надійних систем кіберфізичного захисту приміщень.

Метрологічна атестація та калібрування вимірювальних каналів дозволили успішно компенсувати внутрішню нелінійність вбудованого аналого-цифрового перетворювача мікроконтролера. Застосування поліноміальної апроксимації третього степеня знизило абсолютну похибку вимірювання напруги до значення плюс-мінус дванадцяти мілівольт у робочому діапазоні, що повністю виключає появу хибних спрацювань аварійних сенсорів через зовнішні наведення чи вологість.

Дослідження енергетичних режимів периферійних вузлів підтвердило високу ефективність розроблених алгоритмів енергозбереження. Переведення мікроконтролера в режим глибокого сну з періодичним асинхронним пробудженням дозволило знизити середньозважений струм споживання до дванадцяти міліампер, що забезпечує безперервну автономну роботу пристрою від резервного акумулятора ємністю дві тисячі двісті міліампер-годин протягом більше семи діб.

Аналіз щільності мережевого трафіку та пропускної спроможності бездротового сегмента довів високу масштабованість системи. Повний розмір інформаційного фрейму в ефірі складає сто сімдесят два байти, що при функціонуванні двадцяти одночасно підключених пристроїв створює сумарне навантаження всього шість цілих і вісім десятих кілобіта на секунду. Низький рівень виникнення колізій, значення 1,2 %, підтверджує стабільність архітектури при подальшому розширенні мережі.

Теплові випробування апаратних компонентів підтвердили надійність функціонування вузлів у тривалих режимах навантаження. Максимальний розігрів лінійного стабілізатора напруги склав плюс сорок сім градусів Цельсія, а ядра мікроконтролера – плюс тридцять дев'ять градусів Цельсія, що забезпечує значний запас міцності щодо гранично допустимих теплових меж напівпровідникових структур кристалів.

Експериментальна перевірка захищеності прикладного рівня показала стійкість системи до поширених локальних кібератак. Впровадження списків контролю доступу на рівні MQTT-брокера та використання унікальних лічильників повідомлень і міток часу всередині пакетів JSON дозволили повністю заблокувати спроби несанкційного керування пристроями через атаки повтору та DoS-шторми пакетів з'єднання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гороховський О. І., Новіков В. А. Архітектура та програмування сучасних мікроконтролерних систем на чипі. Київ : Техніка, 2022. 248 с. Кочан Р. В., Саченко А. О. Надійність комп'ютерних систем та мереж : підручник. Львів : Видавництво Львівської політехніки, 2019. 312 с.

2. Мельник А. О. Архітектура комп’ютерних систем реального часу. Львів : Магнолія, 2021. 280 с.

3. Попов О. В., Сидоров М. М. Бездротові локальні мережі та технології радіодоступу : навч. посіб. Харків : ХНУРЕ, 2023. 196 с.

4. Choudhary A. Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions // Discover Internet of Things. 2024. Vol. 4. Article 31. DOI: 10.1007/s43926-024-00084-3. URL: https://link.springer.com/article/10.1007/s43926-024-00084-3?utm_source (дата звернення: 18.12.2025)

5. Milenkovic M. Internet of Things: System Reference Architecture. 2022. URL: https://arxiv.org/abs/2204.01872?utm_source (дата звернення: 22.12.2025)

6. Lynn T. G., Endo P. T., Ribeiro A. M. N. C. та ін. The Internet of Things: Definitions, Key Concepts, and Reference Architectures // The Cloud-to-Thing Continuum. Cham : Springer, 2020. P. 1–22. DOI: 10.1007/978-3-030-41110-7_1. URL: https://www.researchgate.net/publication/342744519_The_Internet_of_Things_Definitions_Key_Concepts_and_Reference_Architectures (дата звернення: 25.12.2025)

7. Barry R. Mastering the FreeRTOS Real Time Kernel: A Hands-On Tutorial Guide. Real Time Engineers Ltd., 2020. 415 p. URL: https://www.freertos.org/media/2018/161204_Mastering_the_FreeRTOS_Real_Time_Kernel-A_Hands-On_Tutorial_Guide.pdf (дата звернення 20.03.2026)

8. Espressif Systems. ESP32 Technical Reference Manual. Version 4.8. 2024. URL: https://www.espressif.com/sites/default/files/documentation/esp32_technical_reference_manual_en.pdf (дата звернення: 20.05.2026).

9. Banks A., Gupta R. MQTT Version 3.1.1. OASIS Standard. 2014. URL: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html (дата звернення: 20.05.2026).

10. Home Assistant Architecture and Integration Guide. Home Assistant Developer Documentation. URL: https://developers.home-assistant.io/ (дата звернення: 20.05.2026).