МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВЕТЕРИНАРНОЇ МЕДИЦИНИ ТА БІОТЕХНОЛОГІЙ ІМ. С.З. ҐЖИЦЬКОГО
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

першого (бакалаврського) рівня вищої освіти

на тему:

«АВТОМАТИЗАЦІЯ ПРОЦЕСУ УПРАВЛІННЯ ЕЛЕМЕНТАМИ ІНТЕРНЕТУ РЕЧЕЙ»

Виконав: здобувач групи Акт-42сп
спеціальності 174 «Автоматизація,
комп'ютерно-інтегровані технології
та робототехніка»

Свищ О. О.
(прізвище та ініціали)

Керівник: Пташник В. В.
(прізвище та ініціали)

ДУБЛЯНИ-2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Перший (бакалаврський) рівень вищої освіти
Спеціальність 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____
(підпис)
д.т.н., професор, Тригуба А. М.
(вч. звання, прізвище, ініціали)
"____" _____202 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Свищу Олександру Олеговичу
(прізвище, ім'я, по батькові)

1. Тема роботи *«Автоматизація процесу управління елементами Інтернету речей»*
керівник роботи *к. т. н., доцент., Пташник В. В.*
(наук.ступінь, вч. звання, прізвище, ініціали)
затверджені наказом Львівського НУП *від 25.02.2025 року № 123/к-с.*

2. Строк подання студентом роботи *10 червня 2025 року*
3. Вихідні дані до роботи: *Характеристика сучасних систем автоматизованого моніторингу та керування елементами Інтернету речей із використанням бездротових протоколів (ZigBee, Wi-Fi), архітектурних рішень на базі мікрокомп'ютерів Raspberry Pi, технічні вимоги до сучасних систем керування IoT-пристроями в умовах реального часу, включаючи вимоги до енергоефективності, надійності, безпеки та масштабованості систем.*
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ
1. Аналіз архітектурних підходів до побудови мереж інтернету речей
2. Дослідження апаратно-програмної платформи для керування компонентами IoT-систем
3. Налаштування і адаптація системи управління елементами інтернету речей
4. Охорона праці
Висновки
Список використаних джерел

5. Перелік графічного матеріалу

Графічний матеріал подається у вигляді презентації

6. Консультанти розділів

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата		Відмітка про виконання
		завдання видав	завдання прийняв	
1, 2, 3	*Пташник В. В., к.т.н., доцент*			
4	*Городецький І. М., к.т.н., доцент*			

7. Дата видачі завдання *25 лютого 2025 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Відмітка про виконання
1	*Складання інженерної характеристики об'єкту проектування*	*25.02.2025 – 31.03.2025*	
2	*Дослідження апаратно-програмної платформи для керування компонентами IoT-систем*	*01.04.2025 – 20.04.2025*	
3	*Налаштування і адаптація системи управління елементами інтернету речей*	*21.04.2025 – 20.05.2025*	
4	*Розгляд питань з охорони праці*	*21.05.2025 – 31.05.2025*	
5	*Завершення оформлення розрахунково-пояснювальної записки та презентаційного матеріалу*	*01.06.2025 – 06.06.2025*	
6	*Завершення роботи в цілому. Підготовка до захисту кваліфікаційної роботи*	*07.06.2025 – 10.06.2025*	

Здобувач _____ *Свищ О.О.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Пташник В. В.*
(підпис) (прізвище та ініціали)

УДК 681.521 / 681.518

Автоматизація процесу управління елементами Інтернету речей. Свищ О. О. Кафедра інформаційних технологій – Дубляни, Львівський НУВМБ ім. С.З. Ґжицького, 2025.

Кваліфікаційна робота: 61 сторінка текстової частини, 33 рисунки, 12 таблиць, 18 джерел літератури.

Мета кваліфікаційної роботи полягає у створенні ефективної, надійної та масштабованої системи моніторингу та керування елементами Інтернету речей на основі мікрокомп'ютера Raspberry Pi із використанням бездротової технології ZigBee та платформи Home Assistant.

Об'єктом дослідження є процеси моніторингу та автоматизованого керування елементами Інтернету речей у розподілених сенсорних системах.

Предмет дослідження вивчає методи і засоби автоматизації моніторингу та керування елементами Інтернету речей, включаючи використання бездротових сенсорів, алгоритмів реагування на події, інструментів візуалізації даних та програмного забезпечення для віддаленого управління пристроями. У роботі проаналізовано предметну область, розглянуто архітектуру IoT-систем, обґрунтовано вибір апаратної та програмної платформи, а також досліджено можливості інтеграції датчиків температури, вологості, руху, відкриття дверей та виявлення витоків води. Проведено техніко-економічне порівняння альтернативних мікрокомп'ютерів, реалізовано програмні сценарії автоматизації, налаштовано інформаційні панелі та перевірено стабільність роботи системи в умовах реального часу. Отримані результати дозволяють оцінити ефективність запропонованого підходу та окреслити перспективи його подальшого розвитку.

Ключові слова: автоматизація, Інтернет речей, Raspberry Pi, ZigBee, Home Assistant, моніторинг, сенсорна система.

ЗМІСТ

ВСТУП

Інтернет є невід'ємною складовою сучасного суспільства – він потрібен для обміну інформацією, пошуку та зберігання даних. Завдяки розвитку технологій з'явилися розумні пристрої, що змінюють наше життя. Розумні будинки регулюють освітлення та опалення, а приладами можна керувати зі смартфона.

Термін IoT (Інтернет речей) охоплює підключені до мережі пристрої, що взаємодіють між собою, обмінюються даними без участі людини (M2M) та генерують великі обсяги інформації для аналізу та керування. IoT-пристрої охоплюють мільярди об'єктів, забезпечуючи підвищення ефективності та якості життя.

Розгортання IoT-систем потребує комплексного підходу до архітектури, мереж і програмного забезпечення. Зі збільшенням кількості пристроїв зростає потреба в ефективному моніторингу, керуванні, оптимізації ресурсів та безпеці.

Автоматизація актуальна як для бізнесу, так і для звичайних споживачів. Тому темою роботи обрано дослідження IoT-мереж, технологій і протоколів, а також визначення мінімальних апаратних та програмних вимог для побудови систем керування елементами IoT.

У роботі розроблено систему моніторингу IoT-пристроїв на базі Raspberry Pi. Вона створює компактну мережу з підключенням до Інтернету, забезпечує захист, контроль і онлайн-моніторинг сенсорів. Користувачі можуть взаємодіяти з нею в реальному часі. Система підтримує підключення широкого спектра пристроїв, має високу енергоефективність, доступність і продуктивність.

Метою є аналіз інструментів для управління й моніторингу IoT. Для цього потрібно дослідити архітектуру, структуру й компоненти IoT, типи мереж і протоколів, оцінити апаратне забезпечення та програмне середовище, здійснити налаштування, а також сформувати практичні рекомендації.

РОЗДІЛ 1
АНАЛІЗ АРХІТЕКТУРНИХ ПІДХОДІВ ДО ПОБУДОВИ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Аналіз сучасних технологій, протоколів і типів мереж у середовищі IoT

Свою назву «Інтернет речей» отримав завдяки Кевіну Ештону, співзасновнику Auto-ID Center Бостонського університету. Він разом зі своєю командою розробив концепцію використання тегів радіочастотної ідентифікації (RFID) для підключення об'єктів до Інтернету. Ештон уперше використав термін «Інтернет речей» у 1999 році, і відтоді він набув широкого вжитку (рис. 1.1).

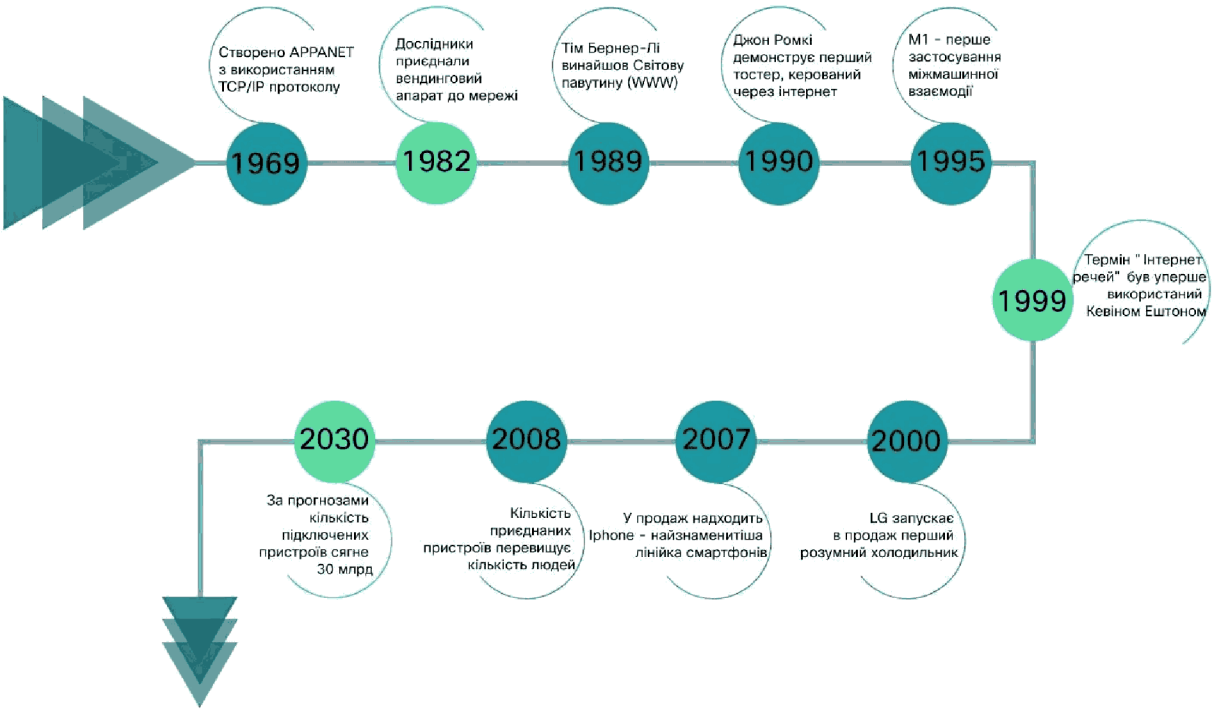

Рисунок 1.1 – Етапи розвитку технології Інтернету речей

Інтернет речей (IoT) – це концепція мережі, у якій фізичні об'єкти оснащені технологіями для обміну інформацією між собою та навколишнім середовищем. До них належать пристрої, датчики та автоматизовані системи, здатні підключатися до Інтернету для виконання різних завдань. IoT – динамічно зростаюча сфера, яка розширює можливості традиційного Інтернету. Очікується, що до 2030 року кількість IoT-пристроїв у світі зросте з 15,1 до понад 29 мільярдів. Підключення через дротові й бездротові технології створює потужне джерело даних і взаємодії між інтелектуальними машинами. Варто зазначити, що базові технології IoT існують уже давно [1].

Системи моніторингу та керування стали важливою частиною безпеки та зручності. Завдяки Інтернету й бездротовим сенсорним мережам можна контролювати обладнання в реальному часі. Вони дають змогу віддалено моніторити, діагностувати, оновлювати ПЗ і знижувати витрати на обслуговування [1].

Керування розумним будинком через Інтернет підвищує комфорт і безпеку, особливо у відсутність власника. Дистанційний моніторинг дає змогу оперативно реагувати на пожежі, витоки чи вторгнення, своєчасно інформуючи екстрені служби [8].

Сьогодні IoT стрімко входить у повсякденне життя. Цьому сприяють розвиток цифрових технологій, зростання кількості Wi-Fi-пристроїв і широке використання смартфонів як засобу керування [11].

Інтернет речей нині широко застосовується в різних сферах діяльності (рис. 1.2), в логістиці, розумних будинках і містах, медицині, виробництві, торгівлі та сільському господарстві. Він поділяється на локальний і глобальний, дротовий і бездротовий, домашній і промисловий IoT [8]. Глобальний IoT об'єднує пристрої на великих відстанях, здебільшого через бездротові з'єднання. Локальний IoT використовує як дротові, так і бездротові технології. Наприклад, «розумний дім» – це локальна система, де всі пристрої взаємодіють між собою, а доступ має лише власник, що гарантує безпеку [6].

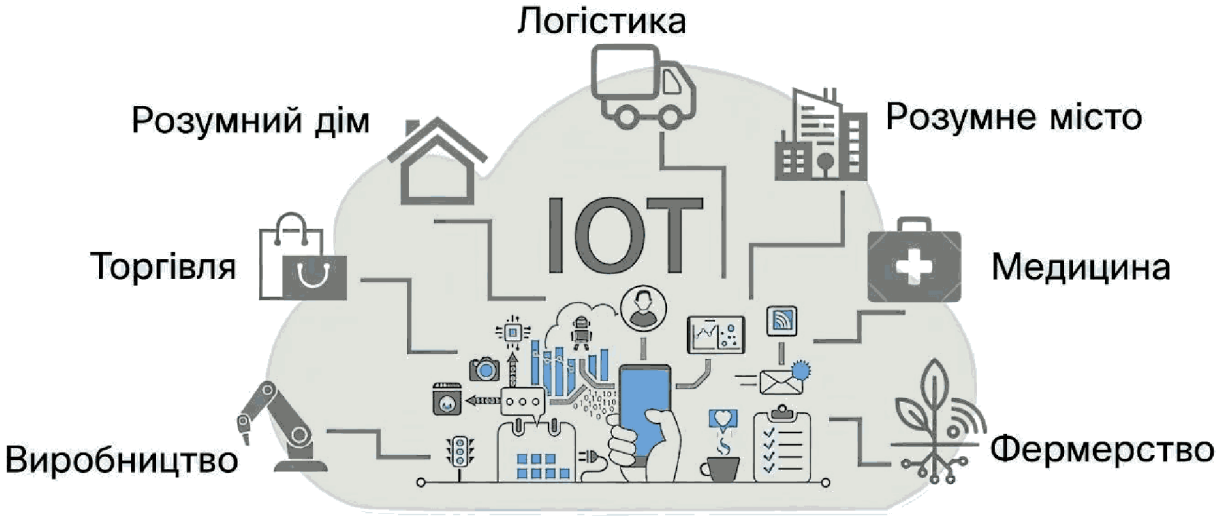

Рисунок 1.2 – Основні сфери застосування IoT

Дротовий IoT використовують там, де важлива надійність і захист даних, зокрема на промислових об’єктах. Він забезпечує стабільний обмін інформацією та контроль процесів. Бездротовий IoT поширений завдяки мобільності, швидкості передачі й простоті розгортання.

У промисловості (IIoT) такі системи автоматизують процеси, а в побуті – полегшують щоденні завдання й дозволяють дистанційно керувати технікою. IoT об’єднує фізичні об’єкти з цифровим середовищем для обміну даними. Його аналіз охоплює збір інформації, зв’язок, обчислення, безпеку та стандарти.

IoT-системи працюють у різних мережах – від локальних до глобальних. Для пристроїв із тривалим часом автономної роботи часто використовують малопотужні технології. Wi-Fi є найпоширенішим, але має обмежений радіус і високе енергоспоживання. Bluetooth підходить для коротких відстаней, а Zigbee та Z-Wave – для домашньої автоматизації.

LPWAN (зокрема LoRaWAN) забезпечує зв’язок на великі відстані з низьким споживанням енергії. Стільникові технології, як-от 4G LTE і 5G, забезпечують високу швидкість і масштабованість. LTE Cat-0, Cat-1, LTE-M і NB-IoT – рішення для передавання невеликих обсягів даних. Sigfox дозволяє підключати велику кількість малопотужних пристроїв.

Наступним етапом дослідження є аналіз протоколів, що забезпечують обмін даними між IoT-пристроями. Вони регламентують сумісність обладнання та маршрути зв'язку на різних рівнях архітектури системи.

На прикладному рівні MQTT забезпечує ефективний обмін повідомленнями, AMQP – структуровану доставку з підтвердженням, CoAP – легкий протокол «запит–відповідь» для обмежених пристроїв. DDS підходить для масштабованих систем, HTTP – для взаємодії з хмарою, WebSocket – для реального часу.

Транспортний рівень представлений TCP (гарантована доставка) і UDP (швидкість без гарантій). Мережевий рівень охоплює IP-адресацію, маршрутизацію та протоколи Ethernet, Wi-Fi, Bluetooth, Zigbee. IPv6 вирішує проблему адрес, а 6LoWPAN адаптує його для малопотужних мереж.

Канальний рівень забезпечує передачу та корекцію помилок (CRC, контрольні суми). IEEE 802.15.4 визначає бездротовий зв'язок для малопотужних мереж (наприклад, Zigbee, 6LoWPAN).

LPWAN включає LoRaWAN, що забезпечує енергоефективний зв'язок на великі відстані через шлюзи, конкуруючи з NB-IoT і LTE-M.

На фізичному рівні дані передаються між пристроями за допомогою сигналів, зокрема радіохвиль або інфрачервоного випромінювання. Ethernet використовується для з'єднання IoT-пристроїв із мережами через кабелі.

Bluetooth Low Energy (BLE) – енергоощадна версія Bluetooth, популярна в мобільних пристроях завдяки низькому споживанню енергії. LTE забезпечує швидку передачу даних із низькою затримкою на великих відстанях.

NFC працює на коротких відстанях (до 10 см) і використовується для платежів та ідентифікації. RFID дозволяє безконтактно зчитувати ідентифікатори об'єктів на різних дистанціях. Wi-Fi забезпечує обмін даними, хоча має обмежений радіус і високе енергоспоживання.

У таблиці 1.1 наведено порівняльний опис основних мережевих технологій.

Таблиця 1.1 – Порівняльні характеристики ключових мережевих технологій

Технологія	ZigBee	Wi–Fi	BLE
Стандарт зв'язку	IEEE 802.15.4	IEEE 802.11	IEEE 802.15.1
Швидкість передачі даних	до 0,25 Мбіт/с	до 300 Мбіт/с	до 3 Мбіт/с
Споживання енергії	Низьке	Високе	Дуже низьке
Частотний діапазон	2,4 ГГц	2,4 ГГц	2.400 – 2.4835 ГГц
Радіус роботи	до 100 м	до 100 м	30 м
Максимальна кількість вузлів у мережі	65535	32	7
Базова топологія	Сітка (mesh)	Зірка	Piconet

Серед найпоширеніших технологій в IoT – Zigbee, Wi-Fi і BLE. Їх популярність зумовлена широким функціоналом, адаптивністю до умов і ефективністю в практичному застосуванні, кожна має свої переваги та оптимальні сфери використання.

1.2 Основні компоненти інфраструктури IoT

У мережах IoT функціонують різні типи пристроїв, що взаємодіють, збирають, обробляють і передають дані. Ключову роль відіграють мікроконтролери (MCU) – компактні комп’ютери з вбудованим CPU, RAM і ROM, що керують простими функціями. Вони мають низьке енергоспоживання, підтримують Wi-Fi, Bluetooth, Zigbee, LoRa, шифрування й підключення модулів.

Мікропроцесори (MPU) мають вищу обчислювальну потужність, сумісні з більшістю протоколів і оснащені засобами безпеки. Вбудовані системи, що

ґрунтуються на MCU або MPU, виконують конкретні функції та застосовуються в автоматизації, техніці, промисловості й транспорті.

Інтелектуальні системи, часто з елементами ШІ, мають більшу обчислювальну потужність і здатні аналізувати інформацію з довкілля. Вони використовуються в розумних будинках і містах, медицині та сільському господарстві для управління освітленням, здоров'ям, зрошенням тощо. Існують і прості пристрої – датчики, приводи, які лише збирають і передають дані. Транслятори забезпечують зв'язок між такими пристроями та IoT-мережею, перетворюючи аналогові сигнали на цифрові для подальшої обробки.

Для вибору пристроїв і розуміння роботи IoT-системи важливо проаналізувати її інфраструктуру. Інтернет речей спрощує повсякденне життя, дозволяючи пристроям і датчикам обмінюватися даними через мережу, підвищуючи ефективність, комфорт і безпеку. Для повноцінної реалізації його можливостей потрібна надійна архітектура, яка забезпечує взаємодію всіх компонентів. Аналіз інфраструктури є ключовим етапом розробки IoT-рішень – він допомагає виявити зв'язки, сформулювати вимоги та передбачити проблеми.

IoT охоплює широку екосистему інструментів і технологій. Розуміння основних компонентів і їхньої інтеграції критично важливе для проєктування систем. IoT включає підключені пристрої з датчиками й вбудованими обчислювальними ресурсами, і навіть локально з'єднані пристрої можуть формувати повноцінну систему без прямого доступу до Інтернету. Основні компоненти інфраструктури наведено в таблиці 1.2.

Важливим аспектом IoT-інфраструктури є безпека. Датчики – ключові елементи системи, які застосовуються, наприклад, для моніторингу температури або відстеження транспорту через GPS. Вони живляться від батарей або джерел постійного струму. Більшість IoT-систем мають датчики, але деякі можуть працювати без них – як-от системи розумного освітлення, якими керують через мобільний застосунок лише за допомогою контролера.

Таблиця 1.2 – Компоненти інфраструктури Інтернету речей

Елемент інфраструктури IoT	Опис
Датчики	Використовуються для вимірювання фізичних величин, якими IoT–пристрої діляться через мережу
Контролери	Мозок пристрою; виступають мостом між датчиком і мережею, виконують обчислення і зберігають дані
Мережа	Технологія, що використовується для обміну даними з іншими пристроями в системі або хмарою
Хмара	Обчислювальні ресурси, сховища та шлюзи, доступні через Інтернет
Користувацькі програми	Мобільні та веб–додатки, які дозволяють користувачеві взаємодіяти з системою IoT
Аналітика даних	Інструменти та ресурси, які дозволяють користувачам отримувати інформацію від системи IoT.

Контролер IoT – мозок системи: він зв’язує датчики з мережею й виконує локальні обчислення. Сучасні контролери мають більшу пам’ять і продуктивність, що сприяє розвитку периферійних обчислень – обробки даних поблизу джерела. Як і датчики, вони можуть працювати від батарей або зовнішнього живлення.

Щоб пристрій був IoT-пристроєм, він повинен мати мережеве з’єднання – інакше це лише автономний мікрокомп’ютер. Повноцінна IoT-система передбачає обмін даними між пристроями або з хмарними платформами.

Існують різні типи підключень: локальні або хмарні. Для останніх застосовуються або власні хмарні інфраструктури, або сервіси сторонніх провайдерів. Такі платформи включають обробку даних (віртуальні машини, служби додатків), зберігання (кешовані бази даних) і шлюзи – наприклад, HTTP/MQTT або WebSocket-сервери (рис. 1.3).

Масштабування є критичним чинником хмарної інфраструктури IoT, особливо для підприємств із великою кількістю пристроїв. Саме тому компанії часто відмовляються від власних серверів на користь хмарних IoT-платформ, які забезпечують гнучке й просте розширення інфраструктури.

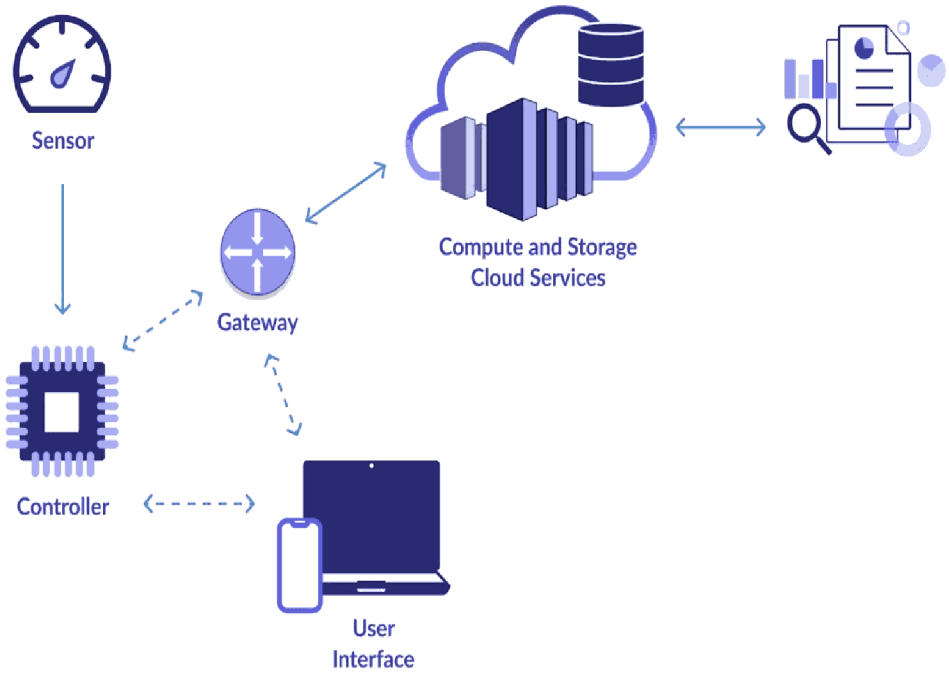

Рисунок 1.3 – Архітектурні складові IoT-системи

Залежно від архітектури, хмарна інфраструктура може взаємодіяти з мобільними та вебзастосунками, дозволяючи користувачам переглядати дані й надсилати команди. Такі функції, як реєстрація, вхід, відновлення пароля та API-доступ, є невід'ємною її частиною.

Зі зростанням кількості пристроїв збільшується обсяг даних, що надходять у хмару. Це відкриває можливості для аналітики, машинного навчання й отримання практично корисної інформації. Хмарна інфраструктура забезпечує зберігання, обробку та аналіз даних.

Безпека є ключовим аспектом під час проєктування. Захист потрібен як при передаванні, так і при зберіганні інформації – наприклад, використання HTTPS замість HTTP. У складніших системах впроваджуються контролери з апаратним шифруванням, політики доступу до баз даних, обмеження мережевого трафіку.

У випадках обробки персональних даних важливо дотримуватися чинного законодавства й регулярно проводити аудит безпеки. Незважаючи на варіативність IoT-проєктів, перелічені елементи залишаються основою для побудови стійкої, масштабованої та економічної системи [9].

1.3 Підходи до моніторингу в системах Інтернету речей

Моніторинг IoT-пристроїв передбачає постійне відстеження їхнього стану, продуктивності й безпеки в режимі реального часу (рис. 1.4). Це забезпечує стабільну роботу інфраструктури та дозволяє завчасно виявляти проблеми й уникати збоїв.

Система IoT включає такі основні компоненти (рис. 1.4):

– речі (датчики й контролери),

– мережу для передавання даних,

– хмару для зберігання й обробки,

– інтерфейс користувача (мобільний або вебдодаток).

Моніторинг охоплює апаратне забезпечення, прошивку й програмне середовище. Можна відстежувати напругу, струм, температуру, вологість, а також задавати порогові значення для автоматичних сповіщень. У разі перевищення порогу надсилається сигнал, що дозволяє швидко реагувати.

Також можливий моніторинг з'єднань окремих сенсорів, що сприяє точнішому контролю роботи пристроїв.

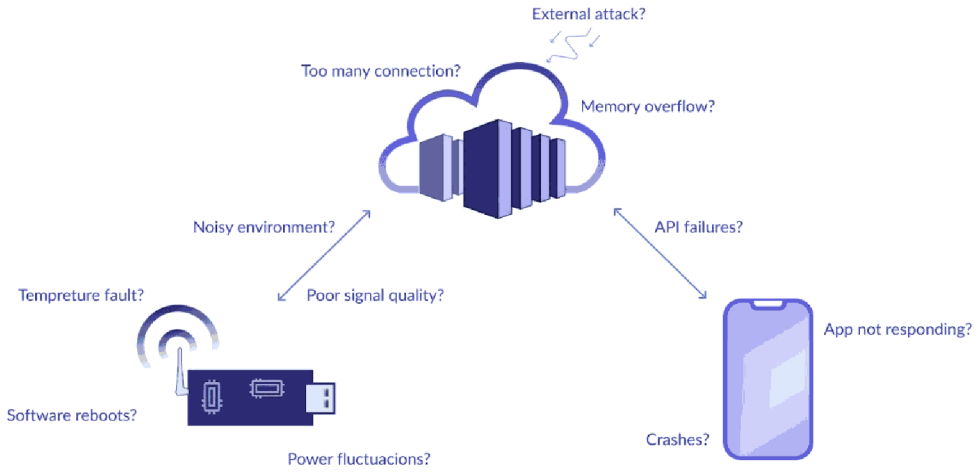

Рисунок 1.4 – Загальна концепція моніторингу в IoT

Для перевірки підключення сенсора можна періодично сканувати шину I2C та надсилати сповіщення при його зникненні. Постійні нулі або максимальні значення також можуть свідчити про несправність. У мікропрограмі доцільно контролювати кількість перезавантажень, рівень пам'яті та коди помилок – часті перезапуски або перевантаження сигналізують про проблеми в коді чи перевищення ресурсів.

Залежно від сценарію, важливими можуть бути інші параметри. Наприклад, у пристроях із режимом сну – час виходу з нього. У розумному дверному замку BLE-детекція активує пристрій лише за потреби, економлячи заряд. Це критично для автономних IoT-рішень.

Важливим є також моніторинг мережі: затримки, втрати пакетів, джиттер, тайм-аути. Якщо пристрій зі SIM-картою має постійні обриви зв'язку – слід розглянути зміну оператора. Зашумлене середовище (наприклад, біля двигуна) може викликати помилки контрольної суми.

У хмарному моніторингу слід відстежувати навантаження CPU, використання пам'яті, кількість з'єднань і невдалі запити. Наприклад, велика кількість помилкових з'єднань може вказувати на DDoS або проблему з прошивкою. Зростання трафіку свідчить про потребу в масштабуванні інфраструктури.

Інтерфейс користувача слід оцінювати за кількістю збоїв, ANR-повідомлень та помилок API. Дані можна передавати постійно, подієво або шляхом опитування з хмари. Важливо налаштувати сповіщення (email, мобільні) для оперативного реагування.

Інформаційні панелі дають змогу контролювати пристрої, переглядати дані, отримувати повідомлення. Вони мають бути налаштовані на відображення лише актуальної інформації. При виборі інструменту моніторингу слід враховувати функціональність, масштабованість, безпеку, сумісність з пристроями і підтримку протоколів.

Зручний інтерфейс та легке налаштування сприяють швидкому впровадженню. Важлива й технічна підтримка: оперативність, оновлення, виправлення. Необхідно також зіставити вартість із функціональністю для вибору найкращого рішення.

Згодом система може реагувати автоматично – наприклад, надсилати SMS у разі відмови сервера або вимикати перегрітий компонент. Однак моніторинг виявляє симптоми, а не завжди причини. Наприклад, перевантаження сервера може бути наслідком DDoS-атаки або збою в прошивці пристрою. Для точного усунення проблеми потрібне глибоке розуміння архітектури системи й ретельний аналіз.

Важливо враховувати попередній досвід – аналіз помилок допомагає уникати їх у майбутньому.

Переваги моніторингу IoT:

Відстеження продуктивності пристроїв сприяє оптимальному розподілу ресурсів і забезпечує стабільну роботу мережі. Проактивне реагування на збої підвищує ефективність системи.

Моніторинг дозволяє передбачати потребу в обслуговуванні, запобігаючи поломкам і скорочуючи час простою.

Зі зростанням кількості пристроїв управління ними ускладнюється. Моніторинг забезпечує централізований контроль і допомагає масштабувати систему без втрати продуктивності та безпеки.

Реагування в режимі реального часу надає змогу швидко усувати проблеми, підтримуючи стабільність усіх підключених пристроїв.

Також моніторинг зменшує потребу у фізичних інспекціях – стан обладнання можна відстежувати дистанційно через інформаційні панелі.

Загалом моніторинг є основою для побудови надійної та масштабованої IoT-системи. Постійний контроль кожного компонента дозволяє сформувати ефективну стратегію моніторингу для вашого проєкту.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ АПАРАТНО-ПРОГРАМНОЇ ПЛАТФОРМИ ДЛЯ КЕРУВАННЯ КОМПОНЕНТАМИ IoT-СИСТЕМ

2.1 Огляд технічних характеристик Raspberry Pi та його функціональних аналогів

Для ефективного функціонування систем контролю й моніторингу необхідно правильно підібрати апаратне забезпечення, здатне виконувати поставлені завдання.

IoT-рішення набувають популярності, оскільки підвищують корисність продуктів і забезпечують додатковий прибуток. Наприклад, вентилятор, який автоматично вимикається при досягненні певної температури, дозволяє заощаджувати енергію. Ще цінніше – пристрій, здатний виявляти присутність людини.

Технології стають «розумними» завдяки трьом чинникам:

– конструктивним рішенням, що формують логіку інтелектуальної поведінки.

– апаратним засобам, які забезпечують збір, обробку інформації та прийняття рішень, спрощуючи реалізацію складних функцій.

– інтеграції з іншими системами – наприклад, опалення може реагувати на погодні прогнози, отримані через датчики або з Інтернету. У таких випадках система діє розумно, адаптуючись до зовнішніх умов.

Слід зазначити, що для користувача обидва варіанти реалізації (з вбудованою метеостанцією або підключенням до Інтернету) виглядають однаково – тому клієнт готовий платити однакову ціну. Проте варіант із використанням Інтернету значно дешевший для виробника.

Зі зростанням кількості розумних і підключених пристроїв відкриваються нові можливості, які умовно поділяються на чотири категорії: моніторинг, керування, автоматизація, автономність.

Кожна функція є самостійно важливою й водночас виступає основою для наступного рівня. Наприклад, моніторинг створює основу для керування та автоматизації. Компанії можуть комбінувати ці функції, щоб зробити свої продукти кориснішими для споживача й зміцнити позиції на ринку.

Прикладом є автоматизовані теплиці, здатні самостійно поливати рослини, регулювати температуру, вологість і освітлення. Це особливо актуально під час відпусток, відряджень або тривалої відсутності.

Моніторинг вирішує ключові питання – чи є вода, яка температура, скільки спожито енергії. Можливість перегляду цих даних у будь-який момент підвищує цінність пристрою для користувача, який готовий платити більше.

Отже, просте у впровадженні рішення з дистанційним моніторингом може продаватися за вищу ціну, забезпечуючи виробникам додатковий прибуток. Споживча цінність зростає, коли система не лише моніторить умови, а й дозволяє користувачу керувати ними.

Для досягнення поставлених цілей було обрано та придбано одноплатний мікрокомп’ютер Raspberry Pi 4 Model B. Він здатен виконувати як прості практичні завдання – ознайомлення з комп’ютерами та їх основним використанням, перегляд вебсторінок, відтворення відео чи прослуховування аудіофайлів, – так і більш складні задачі, наприклад, функціонувати як елемент системи IoT, тобто як сервер, що використовується для керування й моніторингу компонентів Інтернету речей [5].

Raspberry Pi 4 Model B – це мініатюрний комп’ютер розміром з кредитну картку, базова модель якого коштує приблизно 35 доларів США, а топова – близько 75 доларів. Усі моделі Raspberry Pi 4 побудовані на системі-на-чіпі Broadcom BCM2711. Цей чип містить чотириядерний 64-розрядний процесор

Cortex-A72 (ARM v8), що працює на частоті 1,5 ГГц, а також графічний процесор VideoCore VI із частотою 500 МГц. За даними виробника, системи на базі нової архітектури працюють на 50 % швидше, ніж пристрої попередніх поколінь Raspberry Pi (рис. 2.1).

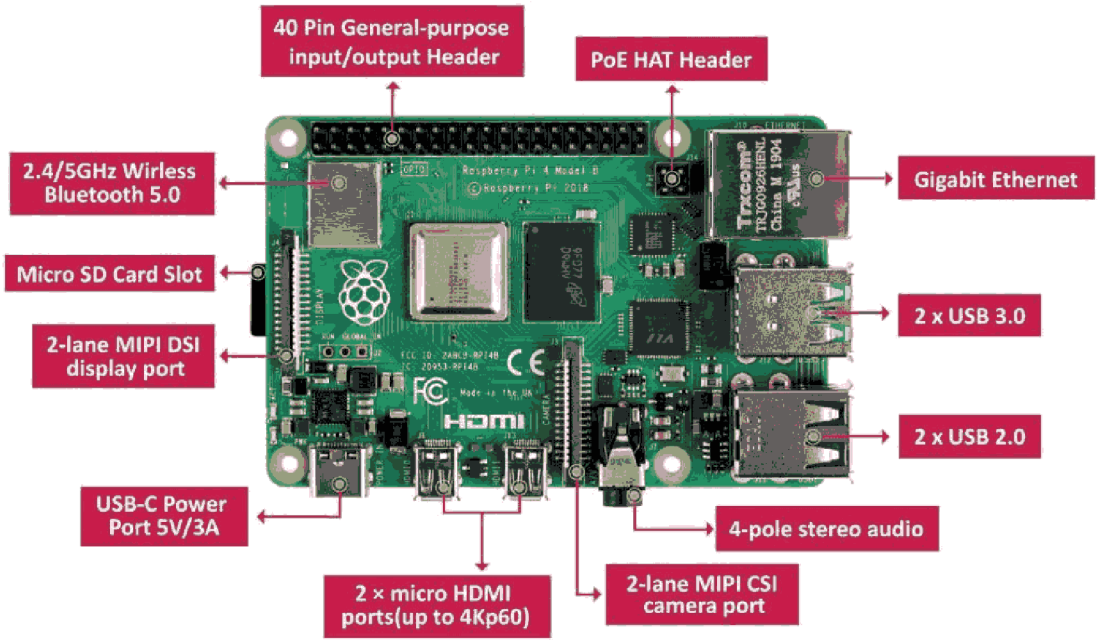

Рисунок 2.1 – Зовнішній вигляд мікрокомп’ютера Raspberry Pi 4 Model B

Ця модель оснащена 4 ГБ пам’яті SDRAM, яку використовують як центральний, так і графічний процесори. Ресурсів мікрокомп’ютера з такою кількістю оперативної пам’яті достатньо для перегляду вебсторінок у кількох вкладках і обробки великих файлів в офісних програмах.

Контролер підтримує апаратне декодування H.265/HEVC (до 4Kp60) та H.264 (до 1080p60). Це знижує навантаження на процесор під час обробки потокового відео через Інтернет або перегляду великих відеофайлів у режимі Media Center.

Бездротовий модуль підтримує стандарти Wi-Fi 802.11 b/g/n/ac та протокол Bluetooth 5.0 BLE [5].

Для підключення дисплеїв, моніторів і телевізорів передбачено два роз'єми micro HDMI 2.0, які дозволяють виводити зображення на кілька екранів одночасно.

Raspberry Pi 4 має 40 контактів GPIO (рис. 2.2) для підключення цифрових датчиків, модулів розширення та інших периферійних пристроїв. Розпіновка GPIO повністю сумісна з попередніми версіями Raspberry Pi, тому користувачі можуть без труднощів переносити наявні проєкти.

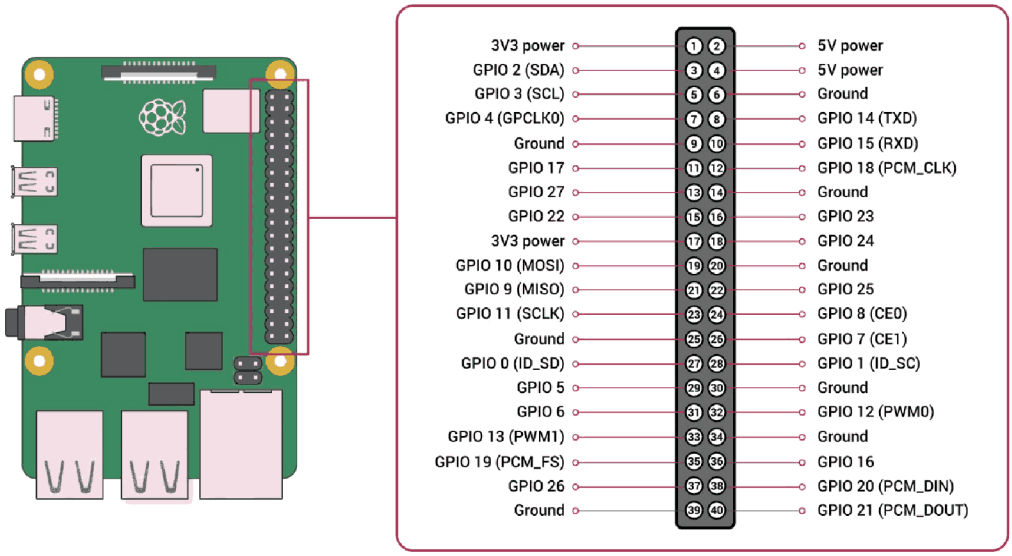

Рисунок 2.2 – Контактна панель GPIO на Raspberry Pi 4 Model B

На бічній панелі контролера є два порти USB 2.0 і два порти USB 3.0. Для комфортної роботи до них підключається стандартна периферія: клавіатура, миша, джойстик та інші USB-пристрої.

Порт MIPI CSI використовується для підключення камери Raspberry Pi. Для прямого підключення до модуля дисплея потрібен порт MIPI DSI. Аудіо- та відеовиходи поєднані в один 4-контактний 3,5-мм роз'єм, що забезпечує аналоговий аудіо- та композитний відеовихід.

У нижній частині плати є роз'єм USB Type-C для живлення. Рекомендується джерело живлення з вихідною напругою 5 вольт і силою струму 3 ампера [5].

На ринку є пристрої, альтернативні Raspberry Pi. Ці альтернативи включають Orange Pi Prime, Banana Pi M3, Rock64, ASUS Tinker board S, Libre Computer Renegade, Odroid H2. Розглянемо їх докладніше.

Orange Pi Prime відрізняється від Raspberry Pi тим, що він має лише 2 ГБ оперативної пам'яті, а AllWinner H5 SoC має вбудований відеоприскорювач Mali-450 GPU, який дозволяє відтворювати лише відео 2K. З цікавих особливостей варто відзначити наявність інфрачервоного приймача; платою можна керувати за допомогою пульта дистанційного керування або деяких моделей мобільних телефонів, які мають вбудовані інфрачервоні світлодіоди. Нестандартні пристрої також включають вбудований мікрофон і відеоінтерфейс CSI, який підтримує потокове відео до 1080p при 30 кадрах в секунду (рис. 2.3).

На бічній панелі контролера розміщено два порти USB 2.0 і два порти USB 3.0. До них можна підключати стандартну периферію: клавіатуру, мишу, джойстик та інші USB-пристрої для комфортної роботи.

Порт MIPI CSI використовується для підключення камери Raspberry Pi, а для прямого підключення до дисплейного модуля потрібен порт MIPI DSI. Аудіо- та відеовиходи об'єднано в один чотириконтактний 3,5-мм роз'єм, що забезпечує аналоговий аудіовихід та композитне відео.

У нижній частині плати розташований роз'єм USB Type-C для живлення. Рекомендоване джерело живлення повинно мати вихідну напругу 5 вольт і силу струму 3 ампери [5].

На ринку представлені пристрої, що є альтернативами Raspberry Pi. Серед них – Orange Pi Prime, Banana Pi M3, Rock64, ASUS Tinker Board S, Libre Computer Renegade, Odroid H2. Розглянемо їх докладніше.

Orange Pi Prime відрізняється від Raspberry Pi тим, що має лише 2 ГБ оперативної пам'яті, а SoC AllWinner H5 оснащено вбудованим відеоприскорювачем Mali-450 GPU, який підтримує відтворення відео тільки до 2K. До цікавих особливостей варто віднести наявність інфрачервоного приймача –

керування платою можливе за допомогою пульта дистанційного керування або деяких моделей мобільних телефонів із вбудованими ІЧ-світлодіодами. Також до нестандартних елементів належать вбудований мікрофон і відеоінтерфейс CSI, що підтримує потокове відео з роздільною здатністю до 1080p при 30 кадрах на секунду (рис. 2.3).

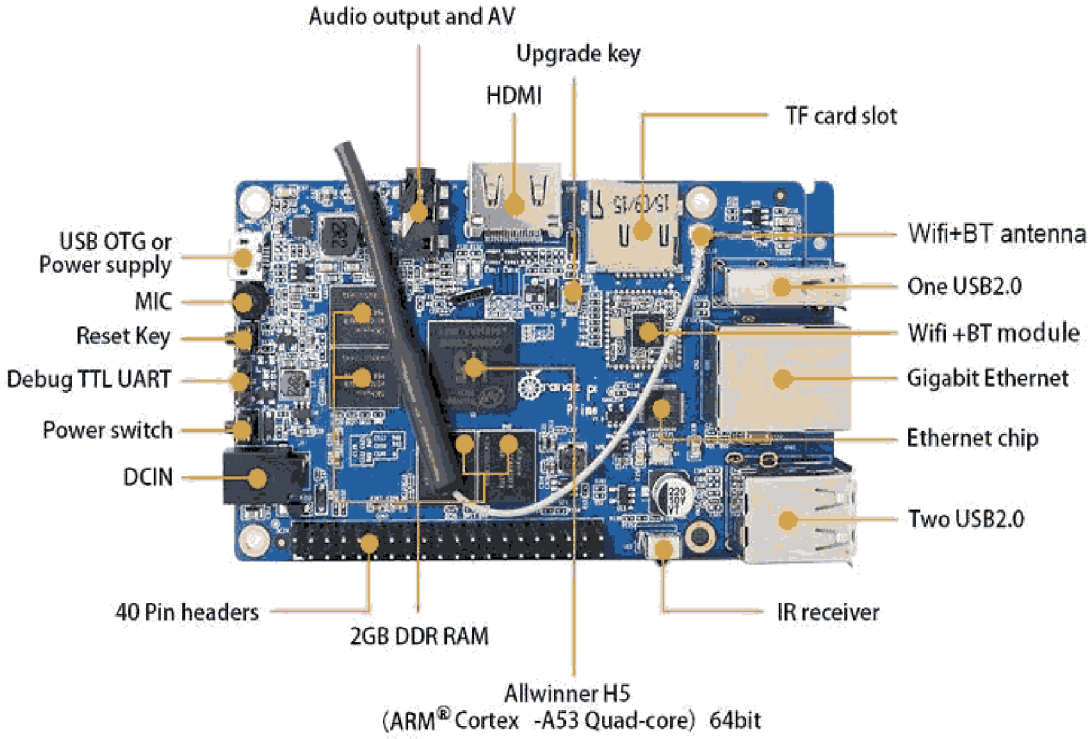

Рисунок 2.3 – Зовнішній вигляд мікрокомп’ютера Orange Pi Prime

Плата розміром 98 × 60 мм оснащена слотом для карт пам’яті (об’ємом до 32 ГБ), модулями Wi-Fi 802.11 b/g/n, Bluetooth 4.0, Gigabit Ethernet, чотирма портами USB (три USB 2.0 host і один USB 2.0 OTG) та роз’ємом GPIO. Також передбачено окремий інтерфейс UART, який виводить сигнали рівня TTL, що дозволяє спостерігати за процесом завантаження операційної системи в терміналі.

Що стосується аудіопристроїв, окрім згаданого вище мікрофона, передбачено лінійний аудіовихід і HDMI-аудіовихід. Відеоприскорювач підтримує OpenGL ES 2.0 та OpenVG 1.1. Підтримувані операційні системи включають Ubuntu, Debian і Android 5.1.

Флагманська модель Banana Pi M3 побудована на восьмиядерному SoC Allwinner A83T (процесор ARM Cortex-A7, графічний процесор PowerVR SGX544MP1) з тактовою частотою 1,8 ГГц, і працює з 2 ГБ оперативної пам'яті та 8 ГБ флеш-пам'яті. Окрім Gigabit Ethernet, двох USB-портів, Wi-Fi 802.11 b/g/n, Bluetooth 4.0 і HDMI, материнська плата також оснащена роз'ємом SATA (рис. 2.4).

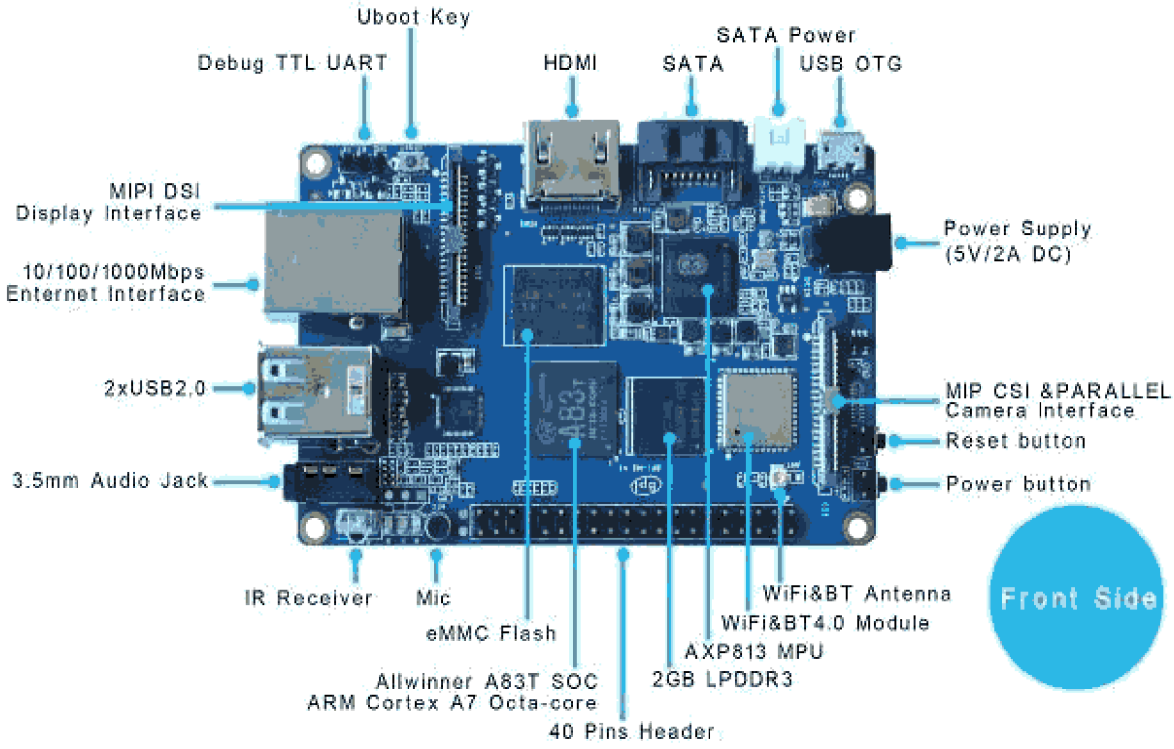

Рисунок 2.4 – Зовнішній вигляд мікрокомп'ютера Banana Pi M3

Як і Orange Pi Prime, Banana Pi M3 має ІЧ-приймач, відеоінтерфейс CSI, оцінювальний UART, мікрофон, лінійний аудіовихід і HDMI-аудіовихід. На відміну від Orange, Banana також оснащена дисплейним інтерфейсом MIPI DSI, який поєднується з I^2C для підключення сенсорного екрана. Крім того, передбачено гребінку GPIO.

З таблиці можна зробити висновок, що вартість Raspberry Pi 4B є найнижчою серед усіх моделей і становить лише 35 доларів. Banana Pi M3 має найбільшу кількість ядер – 8, що є важливим для паралельної обробки даних.

Odroid H2 працює на базі процесора Intel Celeron J4105 і графічного адаптера Intel UHD Graphics 600, що забезпечує йому перевагу в обробці графіки. Розміри моделей варіюються від 54 × 86 мм до 110 × 110 мм, що також слід враховувати під час складання системи. Багато моделей оснащено процесорами ARM з різними конфігураціями ядер і графічними прискорювачами, що забезпечує широкий вибір залежно від потреб користувача. Загалом вибір конкретної моделі залежить від вимог, бюджету та необхідної продуктивності (рис. 2.5).

Таблиця 2.1 – Порівняння характеристик Raspberry Pi та аналогів

Модель	SoC	Процесор	Графіка	Ядра	Частота, ГГц	Розмір, мм	Ціна, $
Raspberry Pi 4B	Broadcom BCM2711	ARM Cortex–A72	Broadcom VideoCore VI	4	1.5	85.6 × 56.5	35
Orange Pi Prime	AllWinner H5	ARM Cortex–A53	Mali–450	4	1.4	98 × 60	68
Banana Pi M3	Allwinner A83T	ARM Cortex–A7	PowerVR 544MP1	8	1.8	92 × 60	68

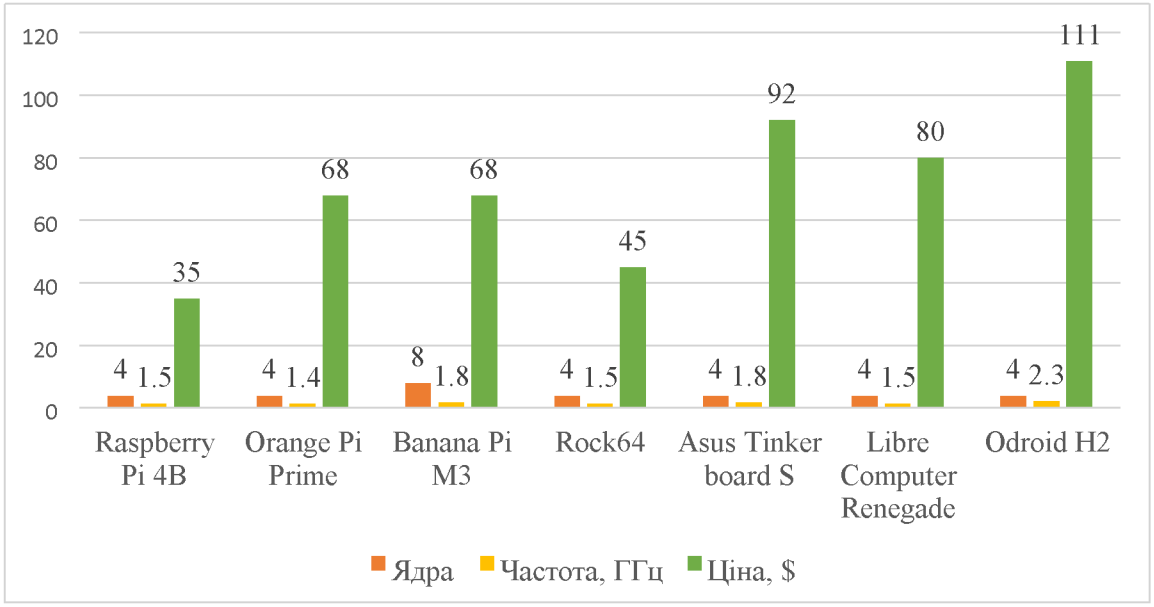

Рисунок 2.5 – Діаграма порівняння за ціною, кількістю ядер і частотою

У таблиці 2.2 наведено порівняльні характеристики підтримуваних інтерфейсів та обсягу оперативної пам’яті.

Таблиця 2.2 – Порівняння підтримки інтерфейсів у Raspberry Pi та аналогах

Модель	ОЗП	Флеш	GPIO	USB	Ethernet	Wi–Fi	Bluetooth
Raspberry Pi 4B	4 Гб LPDDR4 3200	Слот MicroSDHC	40	4	1000 Мбіт/с	802.11b/g/n/ac 2.4/5 ГГц	5 BLE
Orange Pi Prime	2 Гб LPDDR3	Слот MicroSDHC	40	4 (3 ×2.0, 1 ×OTG)	1000 Мбіт/с	802.11 b/g/n	4
Banana Pi M3	2 Гб LPDDR3	8 Гб eMMC	64	3 (2 ×2.0, 1 ×OTG)	1000 Мбіт/с	802.11 b/g/n	4

Отже, шляхом порівняння та аналізу встановлено, що найкращим варіантом за співвідношенням ціни та технічних характеристик для даного дослідження є одноплатний комп’ютер Raspberry Pi 4 Model B..

2.2 Вибір апаратних компонентів для реалізації IoT-системи

Вибір необхідного обладнання є важливим етапом, оскільки потрібен не лише сам центральний пристрій, наприклад, раніше обраний мінікомп’ютер Raspberry Pi, а й відповідне периферійне обладнання.

Оскільки міні-ПК Raspberry Pi не має вбудованої пам’яті, було обрано карту пам’яті Samsung microSDHC на 32 ГБ EVO Plus (рис. 2.6). Має 32 ГБ постійної пам’яті, якої достатньо для встановлення операційної системи та подальшої роботи. Для встановлення карту необхідно вставити у слот microSD. Оскільки мінікомп’ютер Raspberry Pi не оснащений вбудованим модулем ZigBee, було обрано адаптер SONOFF Zigbee 3.0 USB Dongle Plus.

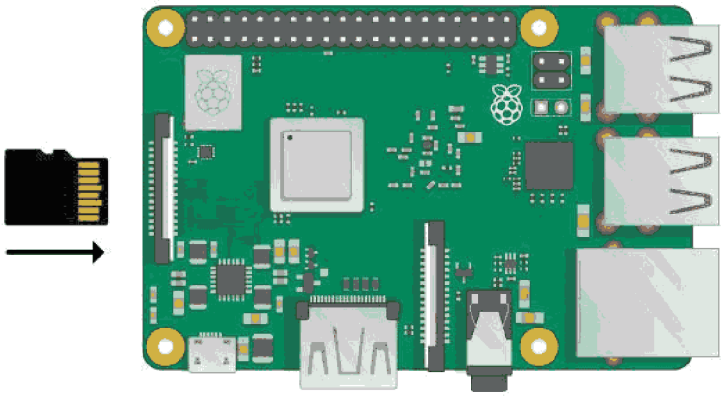

Рисунок 2.6 – Підключення карти пам’яті до Raspberry Pi

SONOFF Zigbee 3.0 USB Dongle Plus – це універсальний USB-координатор-шлюз ZigBee, призначений для безпосереднього підключення до комп’ютера або мінікомп’ютера Raspberry Pi. Він може використовуватися як координатор або маршрутизатор мережі ZigBee на платформах автоматизації з відкритим кодом, таких як Home Assistant (через ZHA) або Zigbee2MQTT.

Цей модуль підтримує роботу з широким спектром пристроїв і може використовуватися як шлюз ZigBee 3.0 на платформі автоматизації з відкритим кодом для керування різними підпорядкованими пристроями від різних виробників, або як маршрутизатор для розширення зони покриття мережі. До підтримуваних пристроїв належать, зокрема: BASICZBR3, S31 Lite zb, SNZB01, SNZB02, SNZB03, SNZB04, ZBMINI, S26R2ZB тощо. Для встановлення цього адаптера його необхідно вставити в роз’єм USB Type-A (рис. 2.7).

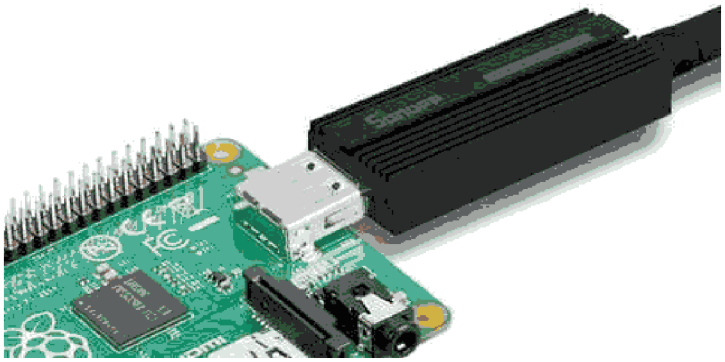

Рисунок 2.7 – Підключення ZigBee-адаптера до Raspberry Pi

Під час тестування зібраної системи я помітив досить високу температуру процесора. Коли температура досягає 80 °C, відбувається перегрів і починається тротлінг: процесор починає пропускати цикли, щоб запобігти подальшому підвищенню температури. Для забезпечення стабільної роботи системи необхідно усунути перегрів і тротлінг.

Оптимальним вибором для цього є кулер ICE Tower – радіатор з активним охолодженням, дизайн якого розроблено компанією Raspberry Pi (рис. 2.8).

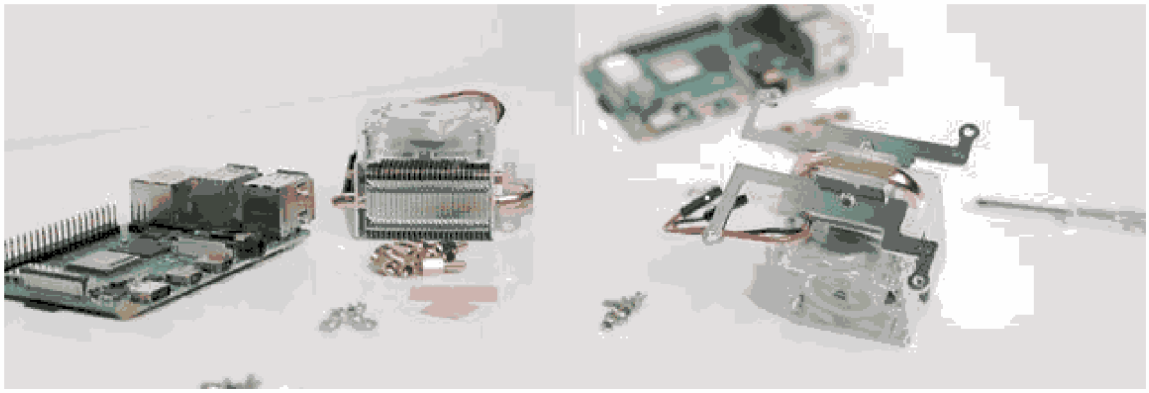

Рисунок 2.8 – Встановлення радіатора з кулером на Raspberry Pi

Після завершення всіх тестів за допомогою утиліт vcgencmd і sysbench було отримано такі результати (табл. 2.3).

Таблиця 2.3 – Порівняння температури ЦП із охолодженням і без нього

Навантаження на ЦП, %	Температура без охолодження, °C	Перегрів (без охолодження)	Температура з охолодженням, °C	Перегрів (без охолодження)
3	48	Ні	28	Ні
15	53	Ні	29	Ні
32	61	Ні	30	Ні
53	65	Ні	32	Ні
55	73	Ні	36	Ні
67	81	Так	37	Ні
89	80	Так	38	Ні
100	80	Так	38	Ні

Для наочного порівняння температурних показників із встановленим кулером та без нього побудуємо графік, який відображає значення температури за кожного рівня навантаження. Це дає змогу візуально оцінити ефективність охолодження та вплив кулера на зниження температури процесора (рис. 2.9).

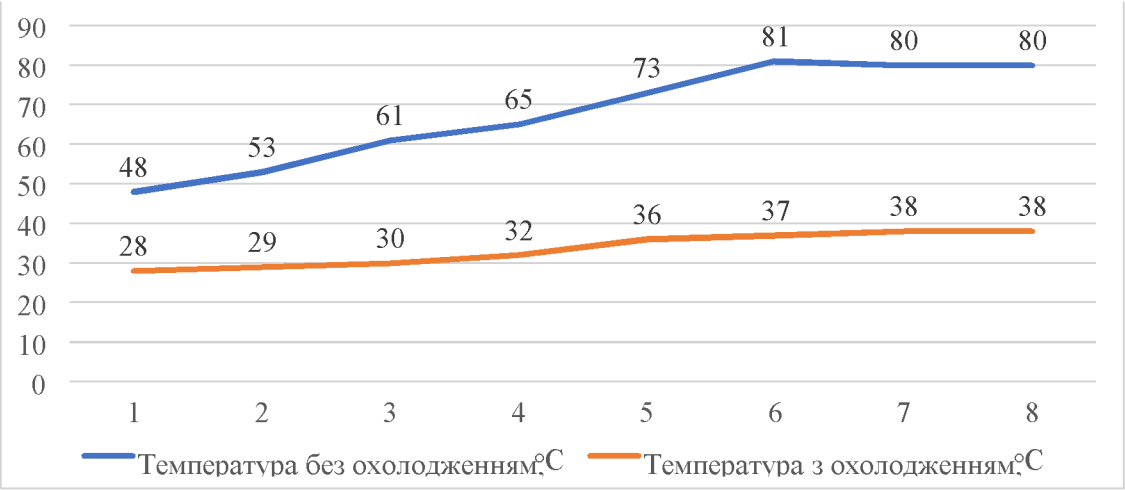

Рисунок 2.9 – Графік температурного режиму системи

Різниця є надзвичайно помітною. Додаткове охолодження не лише знижує температуру процесора, а й подовжує термін служби пристрою, тобто показник MTBF (середній час безвідмовної роботи) зростає в кілька разів.

Однак для стабільної роботи в режимі 24/7 необхідне також якісне електроживлення. З цією метою було обрано джерело безперебійного живлення (ДБЖ) MARSRIVA KP3 (рис. 2.10).

Рисунок 2.10 – Пристрій безперебійного живлення Marsriva Smart Mini UPS KP3

Джерело безперебійного живлення Marsriva Smart Mini UPS KP3 призначене для забезпечення безперервного живлення модемів, маршрутизаторів, мінікомп'ютерів, акваріумного обладнання, камер відеоспостереження та інших електроприладів. Перемикання Marsriva Smart Mini UPS KP3 на автономну роботу відбувається миттєво. Надійна батарея ємністю 10 000 мА·год може одночасно живити кілька пристроїв через роз'єми DC та USB із загальною потужністю до 18 Вт. Пристрій оснащений інтелектуальними схемами захисту від перезаряду, надмірного розряду та короткого замикання, а також дає змогу вибирати вихідну напругу 5 В / 9 В / 12 В постійного струму.

Для підключення мікрокомп'ютера Raspberry Pi до ДБЖ необхідно використовувати кабель живлення USB Type-A – Type-C. З погляду елементів IoT як датчик температури та вологості було обрано Tuya IH-K009 – мініатюрний бездротовий пристрій, призначений для моніторингу температурних і вологісних показників [3].

Завдяки показанням цього датчика в системах розумного будинку можна реалізовувати різні сценарії автоматизації. Наприклад, коли температура повітря знижується нижче певного значення, автоматично вмикається опалення. Або витяжний вентилятор у ванній кімнаті вимикається лише після того, як вологість знизиться до заданого рівня (через керування реле).

Датчик температури працює за протоколом бездротового зв'язку ZigBee, що дає змогу мінімізувати розміри корпусу пристрою та підвищити його енергоефективність. Джерелом живлення є мініатюрна батарейка CR2450, ресурсу якої зазвичай вистачає на кілька років роботи. У процесі експлуатації датчик демонструє стабільність і надійність (рис. 2.11).

Датчик відкриття дверей Tuya TS0203 призначений для забезпечення безпеки приміщень. Пристрій працює шляхом надсилання сигналу через Інтернет на підключений пристрій у момент розмикання магнітних контактів.

Рисунок 2.11 – ZigBee-датчик температури й вологості Tuya IH–K009

Цей інтелектуальний датчик не лише підвищує рівень безпеки будинку чи офісу, надсилаючи миттєві сповіщення про відкриття дверей або вікон, а й може використовуватися для реалізації різноманітних сценаріїв автоматизації, тим самим підвищуючи комфорт користувачів.

Наприклад, при відкритті дверей автоматично вмикається світло в коридорі; при зачиненні вікна активується система кондиціонування, а в разі виходу з дому вимикається освітлення. Водночас при відкритті вікна кондиціонер може автоматично вимикатися тощо (рис. 2.12).

Рисунок 2.12 – ZigBee-датчик відкриття дверей Tuya TS0203

Датчик руху Tuya 809WZT призначений для виявлення руху людей або тварин. Його кут огляду становить 120 градусів, а дистанція виявлення – до 5 метрів. Датчик забезпечує моніторинг у режимі реального часу як вдень, так і вночі. Його основна функція – підвищення рівня безпеки, зокрема, коли вдома нікого немає.

Цей пристрій є частиною системи безпеки, яка дає змогу користувачам відстежувати події, пов'язані з рухом, і отримувати сповіщення, навіть перебуваючи поза межами дому. Завдяки надійній роботі та зручному інтерфейсу він є незамінним рішенням для підвищення рівня безпеки та контролю у вашому приміщенні (рис. 2.13).

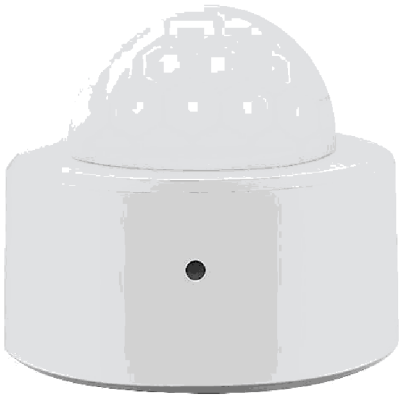

Рисунок 2.13 – ZigBee-датчик руху Tuya 809WZT

Розумний датчик води/повені ZigBee Tuya TS0207 призначений для виявлення затоплення в приміщеннях. Пристрій можна розміщувати у ванних кімнатах, під раковинами або ваннами, біля відкритих вікон, поруч із трубами, під дахами або в будь-якому іншому місці, де існує ризик затоплення чи витоку води [4]. За наявності води контакти датчика замикаються, надсилаючи сигнал тривоги про затоплення до центрального контролера (рис. 2.14).

За допомогою електричного приводу ZigBee Tuya можна налаштувати сценарій, за якого після спрацювання датчика витоку води привод автоматично перекриватиме подачу води.

Рисунок 2.14 – ZigBee-датчик протікання води Tuya TS0207

У таблиці 2.4 наведено повний перелік обладнання, його моделі та необхідну кількість.

Таблиця 2.4 – Список використаного обладнання для IoT-системи

Тип пристрою	Модель	Кількість
Міні–ПК	Raspberry Pi 4 Model B	1
ДБЖ	Marsriva Smart Mini UPS KP3	1
Кабель живлення	Ugreen USB Type-A – Type C	1
Карта пам’яті	Samsung microSDHC 32GB EVO Plus UHS-I Class 10	1
ZigBee адаптер	SONOFF ZBDongle–E	1
Кулер охолодження	ICE Tower 52Pi	1
Датчик температури та вологості	Tuya IH–K009	1
Датчик відкриття	Tuya TS0203	1
Датчик руху	Tuya 809WZT	1
Датчик протікання води	Tuya TS0207	1

Для забезпечення належного функціонування системи керування та моніторингу необхідно обрати апаратне забезпечення, здатне виконувати поставлені завдання й досягати визначених цілей. Тому як ядро системи було запропоновано мінікомп'ютер Raspberry Pi. Він може виконувати як прості практичні завдання, наприклад, вивчення основ роботи з комп'ютерами, відтворення відео чи прослуховування аудіо, так і більш складні – зокрема, функціонування як елемент системи Інтернету речей.

Також варто зазначити, що мінікомп'ютер Raspberry Pi є економічно вигідним вибором для побудови подібної системи, що цілком відповідає цілям даного дослідження.

Технічні характеристики мінікомп'ютера Raspberry Pi, а також перелік додаткового обладнання, необхідного для налаштування системи керування та моніторингу елементів Інтернету речей, наведено нижче.

2.3 Аналіз та обґрунтування вибору програмного забезпечення для моніторингу та керування елементами IoT

Більшість IoT-пристроїв мають обмежені ресурси, тому програмне забезпечення відіграє ключову роль у зборі, передачі й обробці даних, а також у забезпеченні стабільної роботи системи. Воно створює інтерфейс для автоматизації процесів, керування пристроями та перегляду даних у віддаленому режимі.

Серед переваг – швидка реєстрація, спрощена аутентифікація, моніторинг продуктивності, підключення й передавання даних у реальному часі. Навіть у складних мережах забезпечується централізоване керування конфігурацією, безпекою й прошивкою.

Захист інформації гарантують шифрування, контроль доступу та автентифікація. Оновлення прошивки на відстані підвищує безпеку й функціональність системи.

Важливо, щоб панелі керування дозволяли налаштовувати відображення параметрів і створювати інтерфейси для різних користувачів. Розширений моніторинг включає сповіщення, аналітику та звіти. Система має забезпечувати доступ до сенсорів температури, руху, відкривання дверей тощо.

Для безпеки слід обирати програмне забезпечення з підтримкою шифрування, багатофакторної автентифікації й від надійних розробників.

Система IoT має підтримувати масштабування, працювати з великою кількістю пристроїв і даних, бути сумісною з обладнанням різних виробників та інтегруватися з іншими системами. Кількість рішень для моніторингу IoT постійно зростає, а їх функціональність – розширюється.

Вибір програмного забезпечення впливає на ефективність IoT-мережі, тому важливо враховувати технічні вимоги. Одним із перспективних варіантів є Home Assistant – безкоштовна платформа з відкритим кодом на Python, яку можна розгорнути на Raspberry Pi. Вона підтримує гнучке налаштування, автоматизацію дій і має активну спільноту.

Платформа дозволяє створювати персоналізовані інформаційні панелі та запускати сценарії (наприклад, увімкнення світла при поверненні додому). Проте потребує ручного налаштування та регулярного обслуговування. При великій кількості інтеграцій може знижуватись продуктивність.

Альтернативою є OpenHAB – також відкрите рішення для досвідчених користувачів. Воно підтримує широкий спектр пристроїв, але має складнішу конфігурацію та менш зручний інтерфейс.

Home Assistant і OpenHAB можна встановлювати на Raspberry Pi, вони сумісні з різними ОС і мають активні спільноти. Обидві платформи підтримують мобільні додатки для Android та iOS, що дозволяють керувати системою,

використовувати геолокацію, виявлення присутності та отримувати push-сповіщення.

Ще одне рішення – Domoticz, яке вирізняється простотою налаштування через веб-інтерфейс. Хоча вона менш гнучка, Domoticz зручна для початківців. Однак її спільнота менша, документація часто застаріла, а підтримка нових пристроїв обмежена. Domoticz поступається Home Assistant і OpenHAB у гнучкості, масштабованості та сумісності з сучасними системами. Попри стабільність, платформа поступово втрачає популярність. Порівняння ключових характеристик трьох платформ подано в таблиці 2.5.

Таблиця 2.5 – Порівняльна характеристика платформ Home Assistant, OpenHAB, Domoticz

	Home Assistant	openHAB	Domoticz
Підтримувані пристрої та платформи	Raspberry Pi ODROID ASUS Tinkerboard Generic x86-64 Windows macOS Linux Docker VirtualBox KVM/Proxmox VMware ESXi/vSphere	Linux macOS Windows Raspberry Pi Docker	Raspberry Pi Linux Windows
Відкритий вихідний код	Так	Так	Так
Мова	Python	Java	C++
Мобільні додатки	Android та iOS	Android та iOS	Android та iOS
Підтримка	Так	Так	Так
Інтеграція зі сторонніми розробниками	2500+	2000+	Близько 100

Під час вибору системи для керування та моніторингу IoT важливим чинником є популярність платформи. Це зумовлено тим, що популярні рішення мають активні спільноти, кращу підтримку, більшу кількість доступних розширень і ширші можливості інтеграції з різними пристроями. Використання таких платформ полегшує розробку системи, пришвидшує впровадження і дає змогу користуватися досвідом інших розробників.

Home Assistant є лідером у цьому сегменті. Станом на листопад 2023 року кількість активних інсталяцій вбудованого аналітичного інструменту перевищила 270 000. Репозиторій Home Assistant Core на GitHub має понад 63 000 збережень і більше 25 000 поширень. Порівняно з ним, OpenHAB і Domoticz користуються меншою популярністю. Для оцінки динаміки зацікавлення ми також залучили такі інструменти, як Google Trends, який надає статистику щодо тенденцій у використанні цих платформ (рис. 2.14).

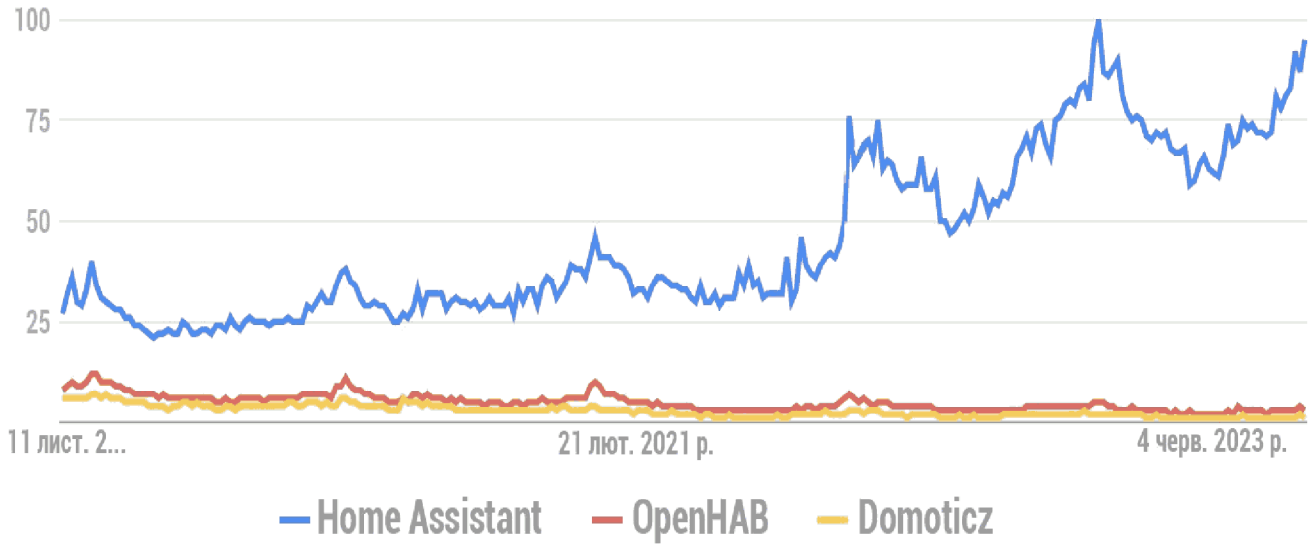

Рисунок 2.15 – Порівняння популярності платформ IoT у Google Trends (5 років)

Застосування Google Trends дає змогу об’єктивно оцінити популярність зазначених платформ і відстежити її зміну з часом. Це сприяє аналізу рівня охоплення та активності користувачів, а також порівнянню платформ між собою.

Показники на GitHub додатково відображають загальну довіру спільноти, якість розробки та популярність проєктів. У таблиці 2.6 наведено кількість зірочок для кожного з відповідних репозиторіїв.

Таблиця 2.6 – Рейтинг популярності систем автоматизації на GitHub

Платформа	Рейтинг (жовтень 2023)
Home Assistant	63800
OpenHAB	1800
Domoticz	3344

Хоча розмір спільноти на Reddit не є ключовим показником, для загального порівняння можна навести відповідні дані (табл. 2.7).

Таблиця 2.7 – Кількість учасників спільнот на Reddit

Платформа	Розмір спільноти (жовтень 2022)
Home Assistant	255000
OpenHAB	6000
Domoticz	972

За даними за грудень 2021 року, майже 40% активних інсталяцій Home Assistant працюють на Raspberry Pi 4, а загалом близько 57% – на різних моделях цього міні-комп'ютера. Це свідчить про його високу популярність серед користувачів. Друге місце за кількістю встановлень посідають віртуальні машини – 33%. Їх можна запускати на NAS, ноутбуках або міні-комп'ютерах, що забезпечує гнучкість і дозволяє адаптувати платформу до потреб користувача та доступних ресурсів. Таким чином, аналіз розподілу установок підтверджує широке використання Raspberry Pi, особливо моделі RPi4, а також демонструє можливість впровадження Home Assistant на різних типах пристроїв для реалізації систем керування IoT (рис. 2.15).

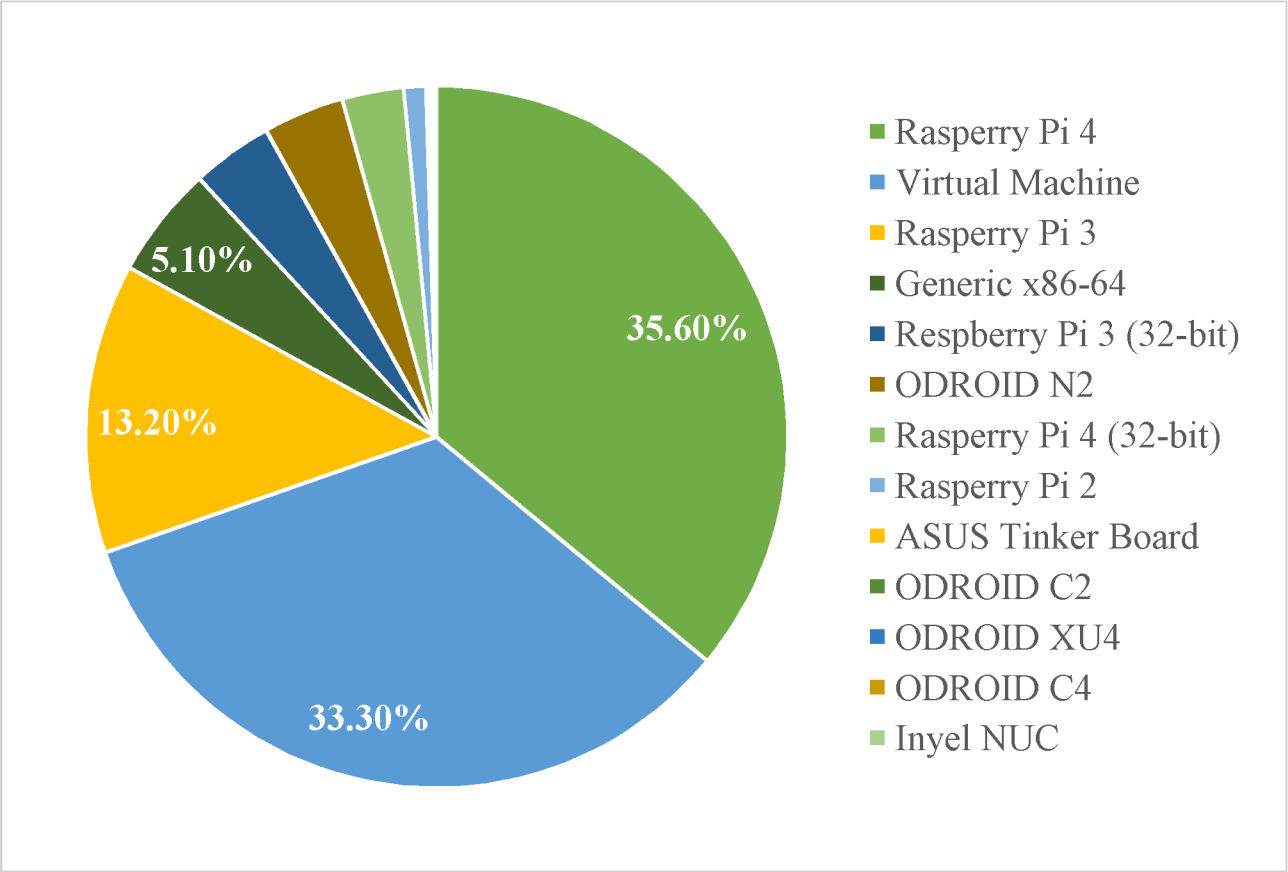

Рисунок 2.16 – Популярність апаратних платформ для інсталяції Home Assistant

Огляд проаналізованих платформ показав, що всі вони підтримують широкий функціонал і дозволяють керувати різноманітними інтелектуальними пристроями. Водночас вони відрізняються за рівнем зручності, сумісності та активністю спільноти. З огляду на всі наведені дані, для подальшої реалізації системи моніторингу та керування IoT було обрано платформу Home Assistant.

РОЗДІЛ 3
НАЛАШТУВАННЯ І АДАПТАЦІЯ СИСТЕМИ УПРАВЛІННЯ ЕЛЕМЕНТАМИ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Встановлення та конфігурація програмного середовища системи

Home Assistant – це універсальна безкоштовна операційна система для керування та автоматизації IoT-пристроїв різних виробників. Вона працює локально, не потребуючи постійного підключення до Інтернету, і підтримує протоколи Wi-Fi, ZigBee, Z-Wave, Bluetooth, IR та інші. Платформа надає широкі можливості для керування системами безпеки, освітленням, побутовою технікою, електропостачанням і моніторингом параметрів середовища, таких як температура, вологість, тиск або виявлення витоків.

Існує кілька варіантів інсталяції Home Assistant. Найпопулярнішим і найпростішим є Home Assistant OS – оптимізована операційна система, яку використовує понад 67% користувачів. Вона має обмеження на встановлення сторонніх програм, проте не виявлено значних недоліків. Інший варіант – Home Assistant Container, що працює у контейнерному середовищі, забезпечує гнучкість у керуванні, зокрема через Portainer. Ще один спосіб – Home Assistant Core, доступний як Docker-образ, але без можливості резервного копіювання чи встановлення додаткових контейнерів. Найбільш функціональним вважається Home Assistant Supervised, який містить усі можливості основної ОС і встановлюється поверх Linux, хоча не забезпечує автоматичного оновлення пакетів.

Оскільки інші функції та можливості міні-ПК, окрім контролю й моніторингу елементів IoT, не досліджувалися, було обрано тип інсталяції

програмного забезпечення Home Assistant OS. Спочатку потрібно підготувати карту пам'яті. Для цього слід завантажити інсталятор ОС разом із утилітою для запису образів операційної системи на SD-карту – Raspberry Pi Imager, що відповідає операційній системі.

У програмі Raspberry Pi Imager необхідно вибрати тип пристрою – Raspberry Pi 4, операційну систему Home Assistant OS, носій (у нашому випадку карту пам'яті microSD) (рис. 3.1).

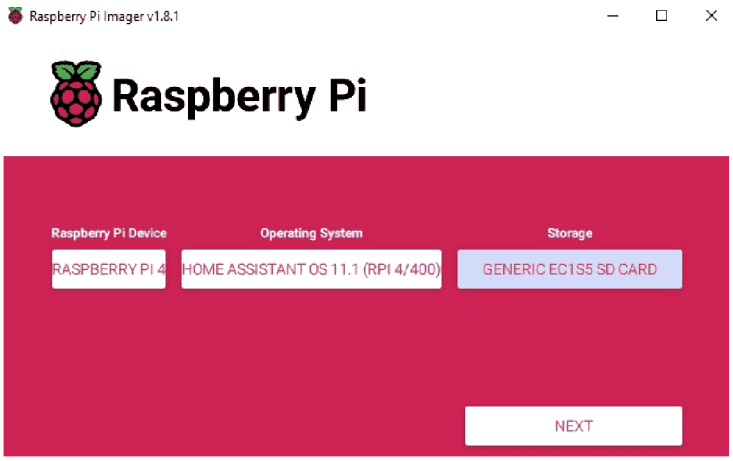

Рисунок 3.1 – Інтерфейс утиліти Raspberry Pi Imager (версія 1.8.1)

Потім встановлюємо підготовлену SD-карту в Raspberry Pi, підключаємо адаптер ZigBee, мережевий кабель і блок живлення для запуску. У браузері через кілька хвилин можна отримати доступ до Home Assistant за адресою homeassistant.local:8123 або http://XXXX:8123, де XXXX – це IP-адреса Raspberry Pi. Після успішного встановлення система запропонує створити обліковий запис (рис. 3.2). Цей обліковий запис матиме права адміністратора і зможе змінювати весь вміст системи [7]. Потрібно ввести своє ім'я, ім'я користувача, пароль і натиснути «Створити обліковий запис».

Далі слід вказали ім'я для розумного дому, встановили розташування та систему одиниць вимірювання. Натиснувши «Визначити», можна автоматично визначити місцезнаходження, часовий пояс та відповідні одиниці вимірювання. За потреби ці параметри також можна задати вручну (рис. 3.3).

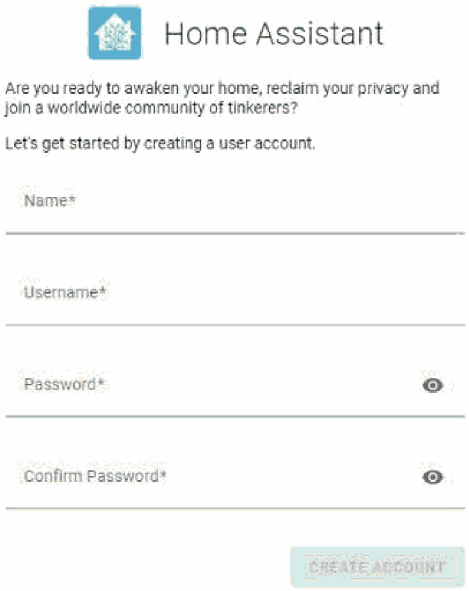

Рисунок 3.2 – Початкові налаштування Home Assistant

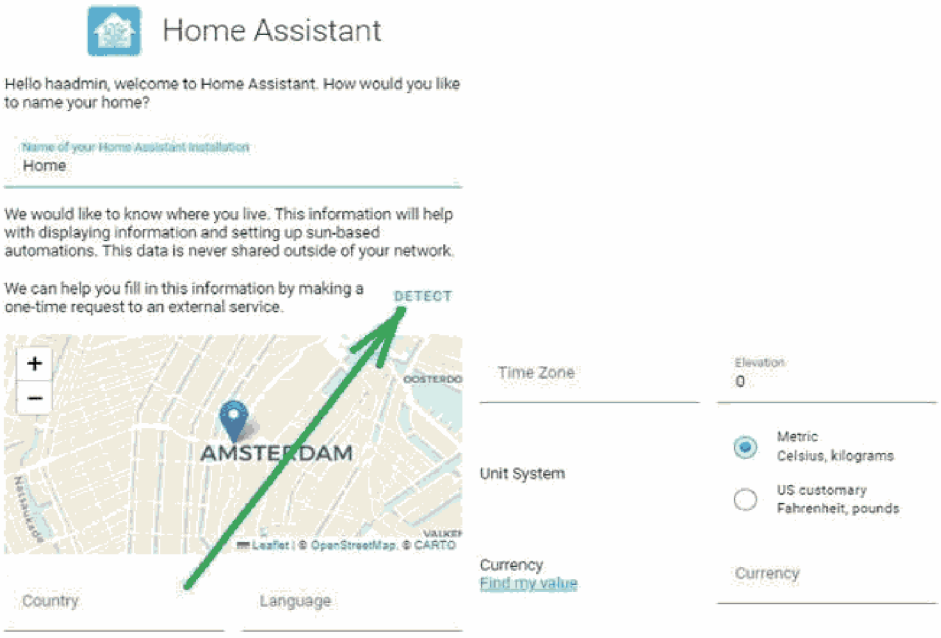

Рисунок 3.3 – Розширені налаштування Home Assistant

Після завершення всіх основних налаштувань виконуємо вхід, використовуючи встановлені логін і пароль (рис. 3.4). Як зазначалося раніше, мережевим координатором ZigBee було обрано адаптер Sonoff ZBDongle–E, який потребує відповідної конфігурації. Існує два способи його налаштування в Home Assistant: через Zigbee Home Automation (ZHA) або за допомогою плагіна Zigbee2MQTT.

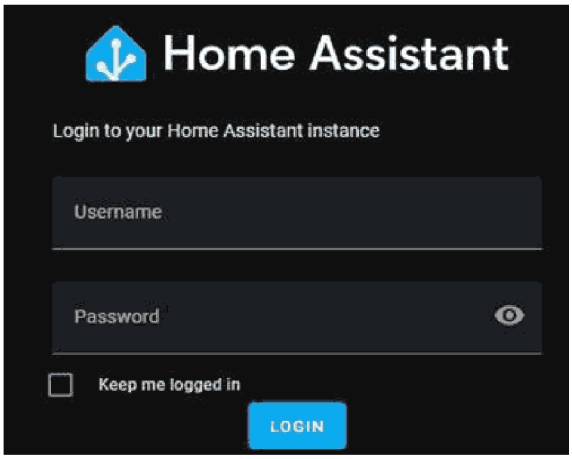

Рисунок 3.4 – Сторінка входу в Home Assistant

Було обрано Zigbee2MQTT – це програмне забезпечення, що дозволяє інтегрувати пристрої різних виробників, поєднуючи мережу ZigBee з протоколом MQTT. Воно підтримує понад 2200 пристроїв і відзначається високою надійністю завдяки активній спільноті та регулярним оновленням. Для коректної роботи необхідний сумісний шлюз, а для налаштування потрібен MQTT-брокер, і рекомендованим рішенням є Mosquitto, який можна встановити з «Магазину додатків» (рис. 3.5).

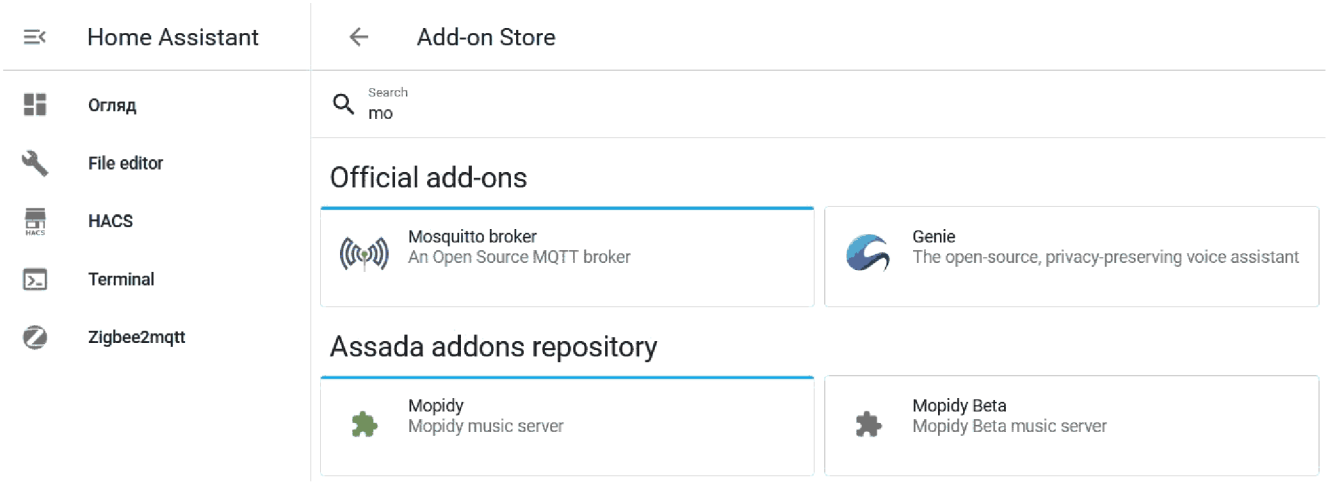

Рисунок 3.5 – Встановлення доповнення Mosquitto broker

Після цього потрібно відкрити вкладку «Конфігурація» на сторінці програми брокера Mosquitto. У параметрах, у пункті «Логіни», введіть ім’я користувача: mqtt та пароль: mqtt (рис. 3.6).

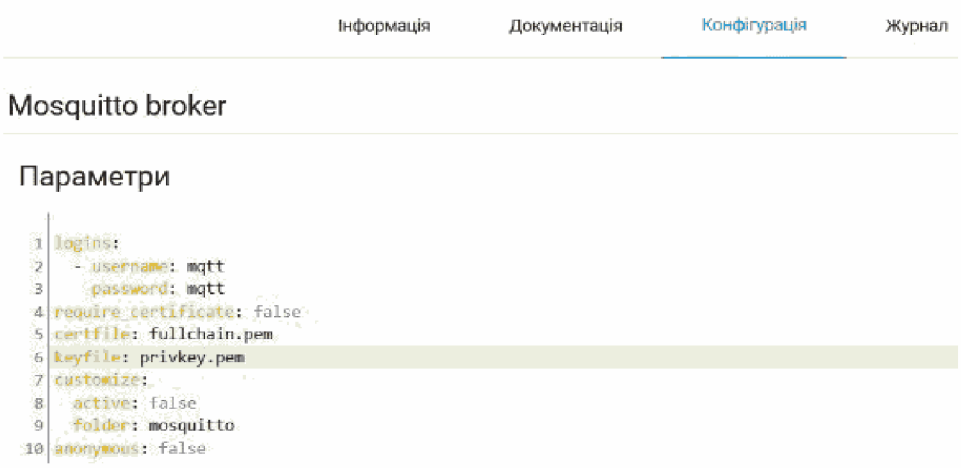

Рисунок 3.6 – Конфігурація параметрів Mosquitto broker

Щоб установити ZigBee2MQTT, необхідно додати відповідний репозиторій з github у магазині доповнень. Адреса сховища: https://github.com/Zigbee2mqtt/hassio-Zigbee2mqtt (рис. 3.7).

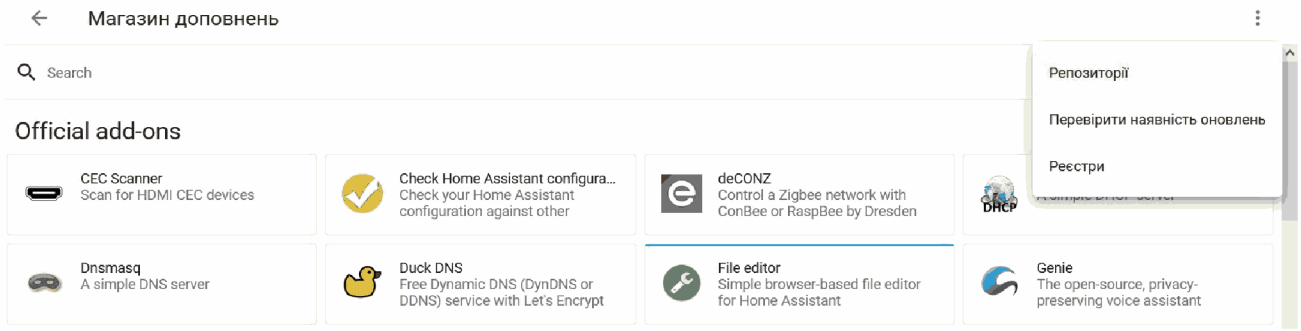

Рисунок 3.7 – Інсталяція доповнення ZigBee2MQTT (етап 1)

У магазині доповнень з’являться дві нові програми ZigBee2MQTT Edge – це версія з гілки розробки, яка раніше отримує підтримку нових пристроїв. Натисніть, щоб установити стандартну стабільну версію ZigBee2MQTT (рис. 3.8).

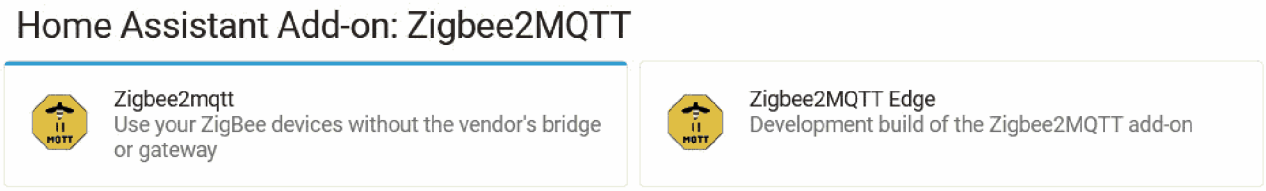

Рисунок 3.8 – Інсталяція доповнення ZigBee2MQTT (етап 2)

Після інсталяції плагіна ZigBee2MQTT слід додати датчики ZigBee, дозволяючи їм приєднатися до мережі. Після успішного додавання датчиків розміщуємо їх у відповідних місцях кімнати (рис. 3.9).

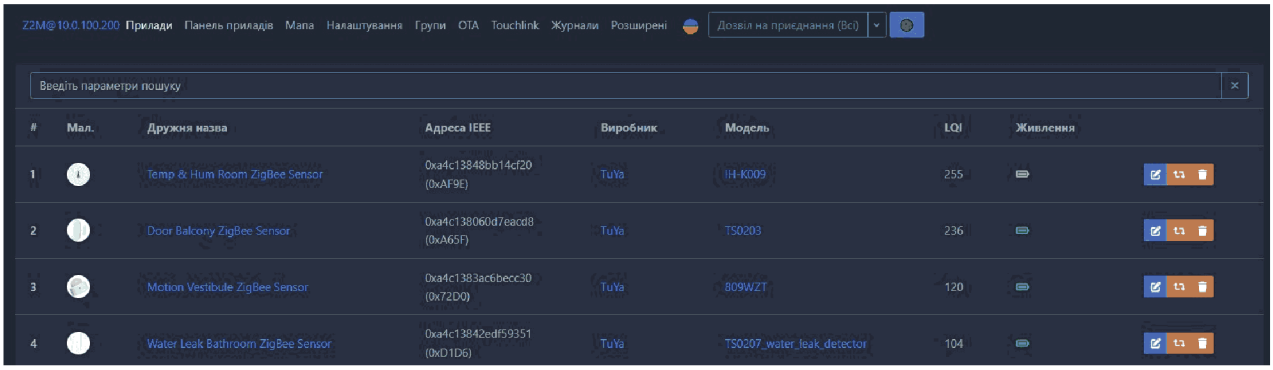

Рисунок 3.9 – Головна панель керування ZigBee2MQTT

Завантажте карту підключених до вашої мережі датчиків ZigBee (рис. 3.10).

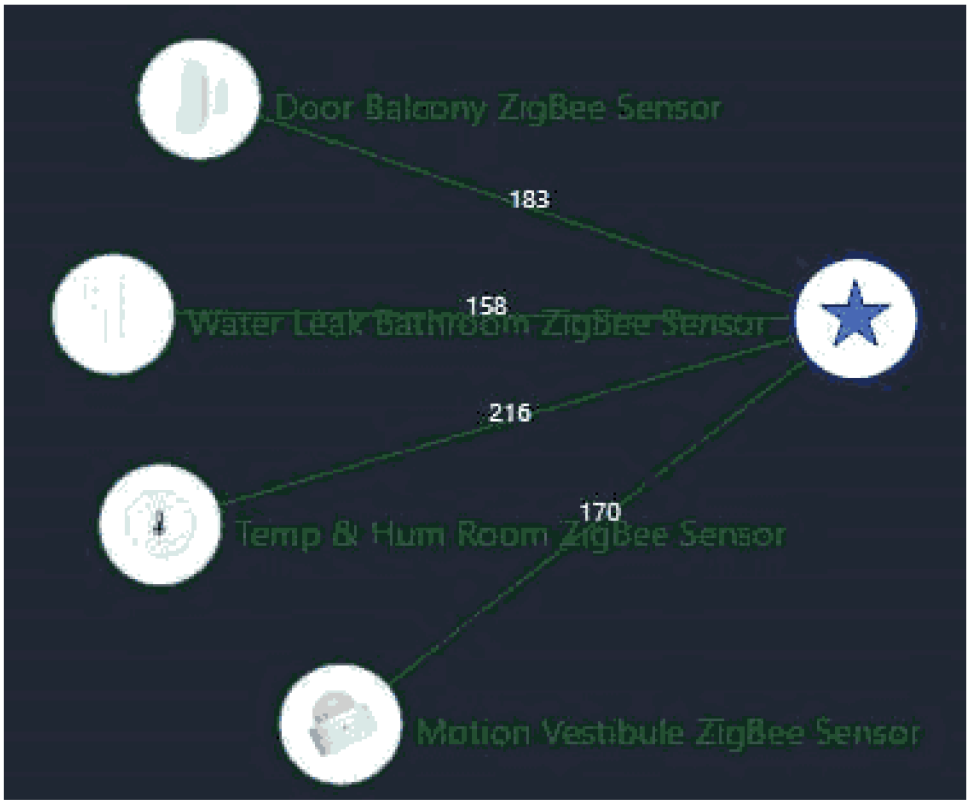

Рисунок 3.10 – Візуалізація мережі ZigBee у вигляді мапи

3.2 Розробка сценаріїв автоматизації та валідація функціонування IoT-системи

Щоб створити сцену роботи розумного будинку треба перейти до розділу «Налаштування» – «Автоматизація та сцени» – «Створити автоматизацію». Спершу налаштовуємо сценарій виявлення витоку води: як тригер обираємо «Entity» і вказуємо датчик витоку Tuya TS0207, доданий раніше. Умови виконання не задаються, щоб сценарій спрацьовував за будь-яких обставин. Як дію обираємо мобільний телефон і налаштовуємо надсилання сповіщення після активації (рис. 3.11).

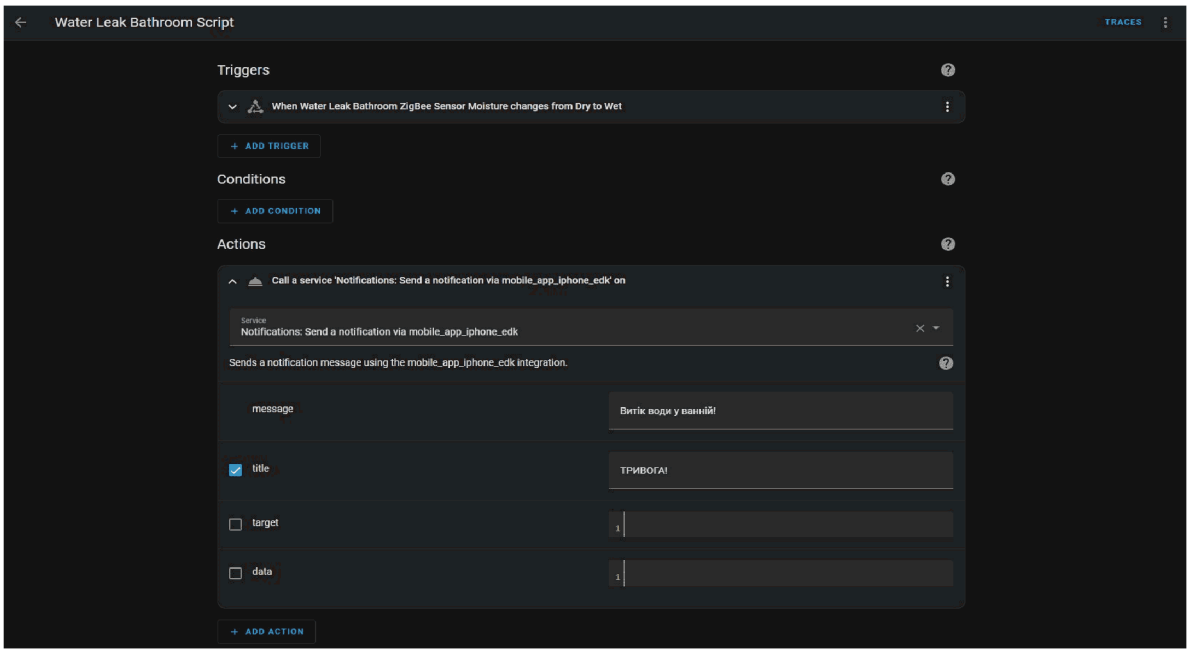

Рисунок 3.11 – Створення автоматизації для виявлення витоку води

Аналогічним чином створюються й інші сцени. У нашому випадку, якщо спрацьовує датчик руху в передпокої та відкриваються балконні двері, на мобільний телефон (з установленим додатком Home Assistant) надходить сповіщення (рис. 3.12).

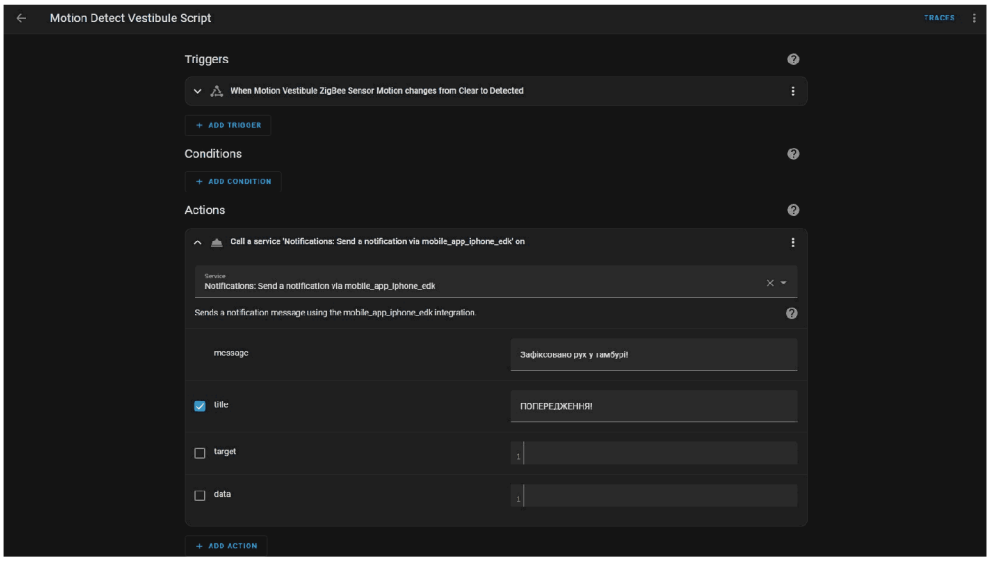

Рисунок 3.12 – Створення автоматизації на основі виявлення руху

Для створення сцени відкриття дверей у програмному забезпеченні Home Assistant також використовується вікно створення автоматизації (Create Automation) (рис. 3.13).

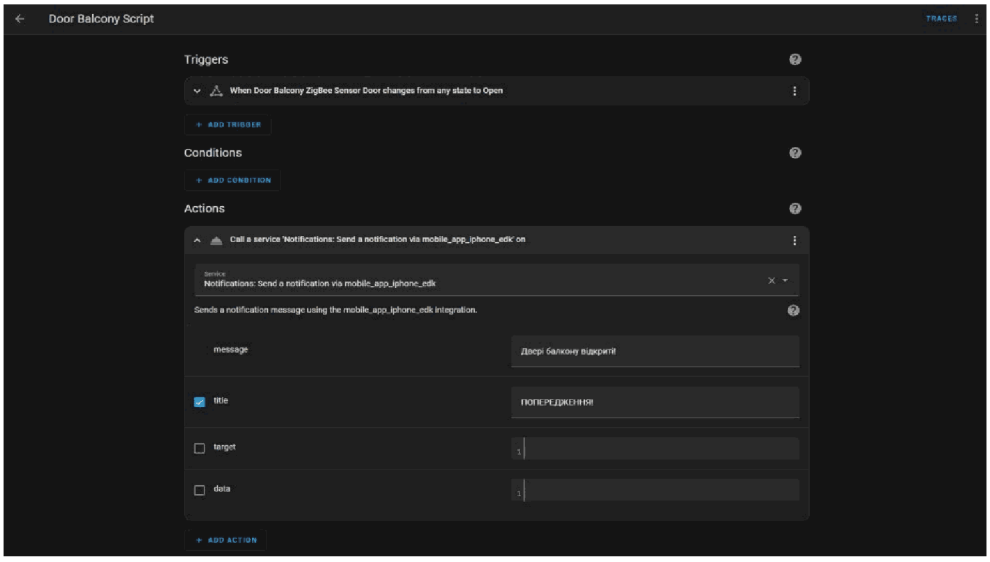

Рисунок 3.13 – Автоматизація відкриття дверей у Home Assistant

На наступному етапі дослідження було зосереджено увагу на тестуванні функціональності створених сценаріїв автоматизації. Для цього активували кожен встановлений датчик і спостерігали за реакцією системи, перевіряючи, чи надійшло відповідне сповіщення на смартфон (рис. 3.14).

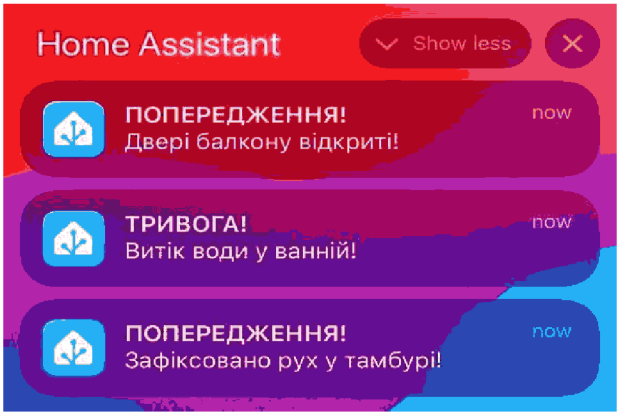

Рисунок 3.14 – Результати тестування створених сценаріїв автоматизації

Зазначимо, що мета дослідження полягає у визначенні мінімального набору інструментів і кроків, необхідних для створення власної системи керування та моніторингу елементів Інтернету речей. Таким чином, наведені вище дії є ключовими складовими цього дослідження та мають вирішальне значення для його успішного виконання.

3.3 Напрями вдосконалення архітектури засобів моніторингу та управління в IoT-середовищі

У системах моніторингу та керування елементами IoT важливо підвищувати функціональність і ефективність. Це включає розширення можливостей системи через додавання нових функцій, підтримку різноманітних пристроїв і протоколів, а також гнучке налаштування. Такий підхід дає змогу адаптувати IoT-системи до різних потреб і поступово їх модернізувати [7].

Одним із способів удосконалення таких систем є впровадження сценаріїв автоматизації, що забезпечують розумне реагування на події. У Home Assistant сценарії автоматизації можна створювати як у форматі YAML, що дозволяє

текстове описання взаємодії компонентів, так і за допомогою зручного графічного інтерфейсу з можливістю імпорту готових рішень.

Під час налаштування автоматизації використовуються так звані сутності – логічні представлення пристроїв, датчиків чи сервісів. Кожна сутність має унікальний ідентифікатор та набір атрибутів, які відображають її поточний стан. Наприклад, температурний датчик може містити інформацію про поточне, мінімальне й максимальне значення температури, а перемикач – про режим «увімкнено» чи «вимкнено» (рис. 3.15). Сутності є базовими елементами для налаштування автоматизації, побудови інтерфейсу користувача та взаємодії з пристроями й сервісами.

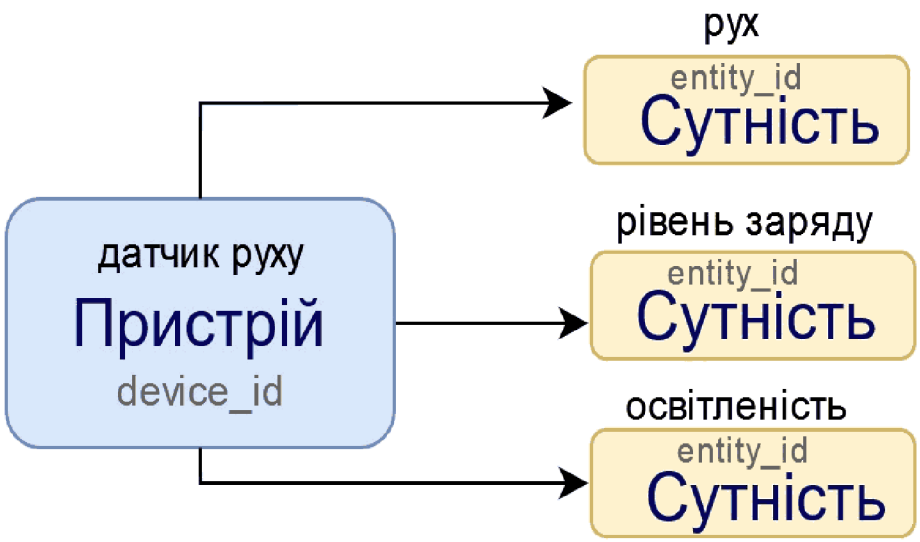

Рисунок 3.15 – Структура сутностей пристрою в Home Assistant

Тригер – це подія, яка запускає сценарій. Після активації тригера система перевіряє умови (якщо задано) і виконує визначену дію. Тригерами можуть бути зміна стану сутності, прибуття користувача, час доби тощо [7].

Дія – це те, що відбувається після виконання тригера та перевірки умов. Вона може включати керування пристроєм, виклик служби, затримку (рис. 3.16).

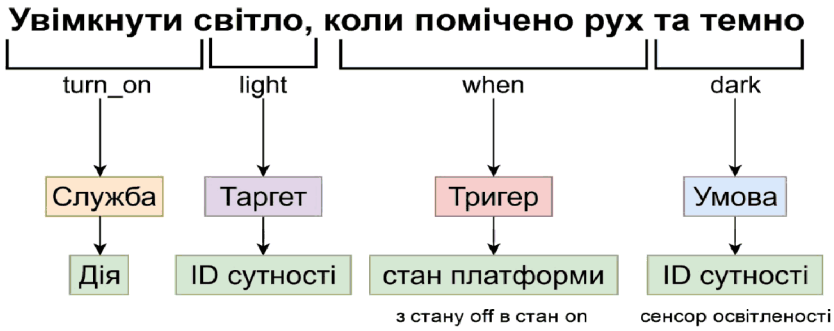

Рисунок 3.16 – Загальний процес реалізації автоматизації

Home Assistant надає різні типи тригерів, умов і дій для налаштування автоматизації (табл. 3.1).

Таблиця 3.1 – Компоненти автоматизації: тригери, умови та дії в Home Assistant

Тригер	Умова	Дія
Home Assistant	Або	if–then
MQTT	Не	Активувати сцену
Webhook	Та	Вибір
Геолокація	Тригер	Виклик служби
Зона	Зона	Виклик події
Календар	Сонце	Виконати паралельно
Подія	Стан	Відтворити
Пристрій	Час	Зупинити
Сонце	Числовий стан	Очікування спливання часу
Стан	Шаблон	Очікування тригера
Тег		Очікування шаблону
Час		Повторення
Числовий стан		Пристрій
Шаблон		Умова
Шаблон часу		

Додавання сценаріїв автоматизації підвищує доступність і ефективність IoT-систем. Користувачі можуть задавати бажані дії та реакції, що спрощує керування й забезпечує інтелектуальну взаємодію.

Один із способів удосконалення системи – додавання нових датчиків. Це дає змогу збирати більше інформації про середовище й точніше реагувати на зміни. Наприклад, датчики освітлення можуть автоматично вмикати світло при низькому рівні освітленості. Датчики газу дозволяють виявляти небезпечні речовини, як-от дим, CO_2 або пропан, а пожежні сенсори реагують на вогонь чи високу температуру, активуючи сигналізацію чи інші заходи безпеки.

Система на Raspberry Pi із Home Assistant є гнучкою й добре масштабованою. Вона підтримує численні інтеграції, що дає змогу легко додавати нові датчики, скрипти, автоматизації та сторонні сервіси [7].

Розширення системи забезпечує кращий контроль, автоматизацію, комфорт і безпеку. Рекомендується додавати додаткові координатори або шлюзи ZigBee для покращення покриття мережі.

Координатори розширюють зону дії, дозволяючи підключати більше пристроїв, особливо у великих приміщеннях або багатозонних об’єктах. ZigBee-шлюзи централізують зв’язок, забезпечуючи стабільну взаємодію з віддаленими пристроями. Вибір між цими варіантами залежить від розміру системи та специфіки її реалізації.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ

4.1 Потенційні небезпеки під час розробки та впровадження IoT-систем

Розробка та впровадження систем Інтернету речей (IoT) передбачає інтеграцію великої кількості електронних пристроїв, сенсорів, програмного забезпечення та мережевих технологій, що створює складне середовище з багатьма потенційними небезпеками. Такий тип систем охоплює як фізичні компоненти, що працюють у реальному середовищі, так і логічну інфраструктуру, яка обробляє та передає дані. Взаємодія цих елементів в умовах обмеженого контролю, високої складності та великої кількості змінних факторів створює ризики як для розробників, так і для кінцевих користувачів. Особливо небезпечними є ситуації, коли порушення в роботі IoT-пристроїв може призвести не лише до виходу системи з ладу, а й до фізичних ушкоджень, аварій або загроз безпеці людини.

Однією з ключових небезпек є електричне ураження. Пристрої Інтернету речей зазвичай потребують постійного електроживлення, часто з використанням змінного струму або акумуляторів. Під час проєктування та монтажу можуть виникати ситуації, коли розробник контактує з відкритими струмоведучими частинами або тестує вузли без належної ізоляції. Це особливо небезпечно при роботі з мережевими модулями, контролерами або реле, які керують потужними споживачами. У разі порушення техніки безпеки існує загроза короткого замикання, іскріння або навіть займання. Крім того, у випадку використання несправних блоків живлення, перевантаження схеми або неправильної

конфігурації електричних з'єднань можлива поява високих напруг на корпусах або провідниках.

Іншою небезпекою є теплове перевантаження елементів. Компактні IoT-пристрої часто не мають достатнього охолодження, що при тривалому використанні або роботі в агресивному середовищі (наприклад, при високих температурах чи в умовах пилу) може призвести до перегріву мікросхем, модулів живлення, бездротових передавачів. Висока температура сприяє прискореному старінню матеріалів, погіршенню електричних характеристик, а також може бути джерелом займання у випадку порушення термостабільності компонентів. Особливо це стосується пристроїв, що використовують літій-іонні акумулятори або працюють у закритих просторах без вентиляції.

Також слід згадати про небезпеку, пов'язану з електромагнітним випромінюванням. У процесі передачі даних бездротовими каналами – Wi-Fi, Bluetooth, ZigBee, LoRa – пристрої генерують електромагнітні хвилі, які в надмірній кількості або при порушенні норм розміщення антен можуть впливати на інші прилади або навіть викликати дискомфорт у користувачів. Окрему загрозу становлять потужні передавачі або випадки саморобної модернізації модулів, коли не дотримано стандартів електромагнітної сумісності. Неконтрольоване електромагнітне поле може впливати на роботу медичного обладнання, засобів зв'язку, а також створювати небезпеку для людей з електронними імплантатами.

Крім фізичних загроз, існують також інформаційні ризики. IoT-системи за своєю природою є мережецентричними, тобто їх елементи постійно обмінюються даними, часто передаючи інформацію через Інтернет або локальні мережі. Ненадійне збереження або передача даних, відсутність шифрування, слабкі паролі, відсутність аутентифікації та захисту доступу можуть призвести до несанкціонованого втручання в роботу пристроїв. У найгірших випадках це може стати причиною масштабних інцидентів: блокування обладнання, підміни даних, дистанційного вимкнення систем без відома оператора. Такі дії можуть призвести

до втрати керованості над інфраструктурою або навіть до аварій з загрозою для життя і здоров'я людей.

Ще одним фактором небезпеки є недосконаліть програмного забезпечення. Багато IoT-рішень створюються на базі відкритих платформ, з використанням бібліотек, що мають вразливості або помилки в логіці. Помилкове функціонування коду або апаратно-програмних інтерфейсів може спричинити збої в роботі сенсорів, виконавчих механізмів, логіки автоматизації. Наприклад, у разі невірного зчитування даних з датчика температури або руху система може неправильно відреагувати – не активувати сигналізацію, не вимкнути живлення або навпаки, без потреби ввімкнути аварійний режим.

4.2 Вимоги до охорони праці на робочому місці інженера з IoT

Робоче місце інженера з Інтернету речей (IoT) є унікальним середовищем, яке поєднує в собі елементи класичної електроніки, програмування, мережевих технологій та експлуатації складних апаратно-програмних систем. Це створює особливі вимоги до охорони праці, адже інженер взаємодіє одночасно з фізичними пристроями та віртуальним середовищем, часто працюючи в умовах підвищеної концентрації уваги, ризику електричних уражень, теплових перевантажень або навіть кібернебезпек. Тому правильна організація робочого місця має не лише сприяти ефективності праці, а й гарантувати безпеку, збереження здоров'я та мінімізацію професійних ризиків.

Насамперед, основою безпечного робочого місця є дотримання ергономічних принципів. Інженер IoT проводить тривалий час за комп'ютером, обробляючи великі обсяги інформації, пишучи код, аналізуючи дані з сенсорів та конфігуруючи пристрої. Це означає, що робочий стіл повинен бути підібраний за

висотою, з урахуванням анатомічних особливостей працівника, з достатнім простором для рук та електронного обладнання. Крісла з регульованими спинками та підлокітниками дозволяють підтримувати правильну поставу, запобігаючи перенавантаженню м'язів спини та шиї. Робоче місце має бути добре освітлене: перевага надається комбінованому освітленню – природному і штучному, при цьому джерела світла не повинні створювати відблисків на екрані чи платі. Локальне освітлення у вигляді лампи з регульованим кутом падіння світла є необхідним при пайці або роботі з дрібними деталями.

Електробезпека є одним із найважливіших аспектів охорони праці інженера з IoT. Більшість пристроїв, з якими працює фахівець, є джерелом потенційної небезпеки, оскільки живляться від мережі змінного струму або використовують джерела постійного струму з високими струмами навантаження. На робочому місці обов'язково має бути заземлення, справні розетки, автоматичні вимикачі з диференційним захистом, що дозволяють відключити живлення при виявленні витоку струму. Для зменшення ризику ураження електричним струмом інженер повинен використовувати інструменти з ізольованими ручками, працювати на спеціальному антистатичному килимку та носити антистатичний браслет. Це також важливо для захисту електронних компонентів, чутливих до електростатичних розрядів, які можуть бути знищені навіть слабким імпульсом.

Вимоги до організації вентиляції та мікроклімату також мають велике значення. Під час роботи з паяльними станціями, термоповітряними фенами або 3D-принтерами виділяються шкідливі речовини – пари флюсів, пластику або пил, що можуть подразнювати дихальні шляхи та очі. Робоче місце повинно бути обладнане ефективною системою загальної вентиляції, а у разі інтенсивної роботи з такими приладами – також витяжною вентиляцією або локальними витяжками. Температурний режим приміщення має відповідати санітарним нормам, оскільки перегрів або надмірна вологість можуть негативно впливати як на самопочуття працівника, так і на стабільність електронного обладнання.

Порядок на робочому місці не лише підвищує ефективність, а й є умовою безпеки. Кабелі живлення, сигнальні дроти, адаптери та інші з'єднувальні елементи мають бути акуратно організовані, не створювати загрозу спотикання, випадкового роз'єднання або короткого замикання. Усі елементи обладнання повинні мати чітке маркування та надійну фіксацію, щоб уникнути падіння чи пошкодження. Зберігання компонентів, інструментів та документів має бути впорядкованим, з дотриманням розмежування між електронікою та легкозаймистими матеріалами.

Оскільки IoT-технології передбачають часту роботу з бездротовими мережами та радіочастотними пристроями, необхідно враховувати особливості випромінювання. У разі роботи з потужними передавачами, інженер має дотримуватись безпечної відстані до антен, уникати надмірного перебування у зоні дії електромагнітних хвиль, особливо в герметичних або металізованих приміщеннях. Бажано періодично контролювати рівень випромінювання з використанням відповідних приладів, а також уникати роботи з саморобними передавачами без перевіреного захисту.

Психофізіологічне навантаження, яке виникає в результаті довготривалої розумової праці, роботи з великими масивами даних і відповідальності за працездатність систем, також повинне враховуватись. Робочий день інженера повинен включати регулярні перерви, рекомендовано проводити профілактичну гімнастику для очей та рук. В умовах тривалої дистанційної роботи або роботи на виїзді необхідно організовувати мобільні безпечні умови: використовувати переносні джерела енергії з вбудованим захистом, захищені канали зв'язку, захисні кейси для обладнання.

Таким чином, вимоги до охорони праці інженера з IoT охоплюють широкий спектр факторів – від ергономіки до електробезпеки та захисту від шкідливих умов. Тільки комплексний підхід до організації робочого середовища дозволяє забезпечити безпечну, ефективну і продуктивну.

4.3 Протипожежна безпека при експлуатації та тестуванні IoT-систем

Протипожежна безпека при експлуатації та тестуванні систем Інтернету речей (IoT) є одним із найважливіших аспектів загальної безпеки інженерного середовища, оскільки такі системи включають велику кількість електронних пристроїв, модулів живлення, акумуляторів, мікроконтролерів та бездротових комунікацій. Усі ці елементи є потенційними джерелами займистості, особливо в умовах тривалого використання, перевантаження, перегріву або при наявності дефектів у конструкції. Тестування IoT-пристроїв часто відбувається в лабораторіях або офісах, які не завжди пристосовані для роботи з електронікою, що додатково підвищує ризик виникнення пожежонебезпечних ситуацій. Тому дотримання норм і правил протипожежної безпеки є обов'язковим як під час розробки, так і при впровадженні таких систем.

Одним із основних джерел пожежної небезпеки є блоки живлення, які забезпечують стабільну подачу електроенергії до компонентів IoT-пристроїв. У разі порушення режимів експлуатації, перевантаження або неправильного підключення ці пристрої можуть перегріватися, що часто призводить до плавлення ізоляції, короткого замикання або займання. Особливо небезпечні ситуації виникають під час роботи з імпульсними джерелами живлення низької якості або саморобними зарядними пристроями, які не мають належного захисту від перевищення напруги або струму. Внаслідок цього критичні компоненти можуть вийти з ладу з одночасним виділенням тепла і навіть відкритим полум'ям.

Іншою суттєвою загрозою є акумуляторні батареї, які все частіше використовуються в IoT-системах для забезпечення автономної роботи пристроїв. Особливо це стосується літій-іонних та літій-полімерних акумуляторів, що мають високу енергетичну щільність і чутливі до механічних пошкоджень, перезаряду або коротких замикань. У разі порушення цілісності корпусу або збоїв у роботі контролера заряду можливе різке підвищення температури всередині елементу

живлення з подальшим займанням або вибухом. Це не лише створює прямий ризик для обладнання, а й становить загрозу для життя і здоров'я людини, оскільки під час займання літієвих акумуляторів виділяються токсичні продукти згоряння.

Також важливу роль у пожежонебезпечності відіграє якість самих електронних плат, зокрема друкованих плат (PCB), що використовуються в IoT-пристроях. Якщо при їх виготовленні були допущені помилки – наприклад, використано матеріали з низькою температурною стійкістю або порушено техніку паяння – при інтенсивному навантаженні доріжки можуть перегріватися, виникає локальне плавлення флюсу, а в деяких випадках і займання шару лаку або базового матеріалу. Під час тестування таких пристроїв у лабораторних умовах часто використовується змінне навантаження, що ускладнює виявлення критичних точок. За відсутності термоконтролю або автоматичного відключення пристрою у разі перегріву, подібні ситуації можуть призвести до серйозних інцидентів.

Не менш важливою є і роль навколишнього середовища, де працюють інженери. Робочі столи, на яких виконуються збирання або тестування IoT-систем, повинні бути виготовлені з негорючих матеріалів або покриті спеціальними вогнестійкими килимками. У зоні тестування не повинно бути легкозаймистих речовин, зокрема паперу, тканин, органічних розчинників або відкритих джерел вогню. Робота з електронними компонентами, що можуть нагріватися або іскрити, повинна проводитися на відстані від інших пристроїв, аби уникнути каскадного загоряння. Дуже часто системи Інтернету речей встановлюються у вузьких, слабо вентильованих приміщеннях, таких як розподільчі шафи або серверні кімнати. У таких умовах надзвичайно важливо забезпечити не тільки вентиляцію, а й постійний моніторинг температури, адже будь-який перегрів може залишитись непоміченим до моменту виникнення пожежі.

ВИСНОВКИ

У процесі виконання кваліфікаційної роботи було розроблено і впроваджено систему моніторингу та керування елементами Інтернету речей на базі мікрокомп'ютера Raspberry Pi.

Проведене дослідження охоплювало аналіз архітектури IoT-систем, класифікацію протоколів передачі даних, вибір апаратного та програмного забезпечення, а також реалізацію алгоритмів взаємодії між пристроями. Особливу увагу приділено вибору технічних рішень, зокрема обґрунтованому використанню одноплатного комп'ютера Raspberry Pi 4 Model B та ZigBee-адаптера SONOFF, які забезпечують сумісність із широким спектром сенсорів. Вибрані датчики температури, вологості, руху, відкривання дверей та витоку води були інтегровані в єдину систему, здатну виконувати автоматичні дії на основі заздалегідь визначених сценаріїв.

Для забезпечення стабільності роботи системи використано ефективне охолодження процесора та джерело безперебійного живлення. Як програмне середовище було застосовано Home Assistant — сучасну платформу з відкритим кодом, що підтримує високий рівень налаштування та візуалізації. Здійснено налаштування панелі керування, реалізовано віддалене керування, створено сценарії автоматизації. Експериментальні результати засвідчили стабільну роботу системи, швидке реагування на події та можливість масштабування.

Отримані результати доводять ефективність запропонованих технічних рішень і підтверджують доцільність застосування описаного підходу для побудови розумних середовищ. Робота має практичну цінність та може бути адаптована для моніторингу в побутових, комерційних або аграрних умовах. У подальшому перспективним є розширення функціоналу системи з інтеграцією методів машинного навчання для прогнозування подій і підвищення енергоефективності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Das S. First Things on Internet and Their History. Independently Published, 2019. С. 18–22.

2. Internet of Things: Architectures, Protocols and Standards / M. Picone, G. Fortino, R. Gravina, M. Mavromoustakis. – Wiley & Sons, Incorporated, John, 2018. – 408 с.

3. LTE Cat–M1 [Електронний ресурс]. – Режим доступу: https://www.4gltemall.com/ue-category/lte-catm1.html?limit=24 (дата звернення: 11.06.2025).

4. Bluetooth Low Energy (BLE): A Complete Guide [Електронний ресурс]. – Режим доступу: https://novelbits.io/bluetooth-low-energy-ble-complete-guide/ (дата звернення: 12.06.2025).

5. Raspberry Pi Documentation. Official resource [Електронний ресурс]. – Режим доступу: https://www.raspberrypi.com/documentation/ (дата звернення: 04.05.2025).

6. Headman V. Raspberry Pi 4 Advanced Users Guide: The Complete Guide to Mastering the Raspberry Pi 4: Raspberry Pi 4 Guide. – Independently Published, 2021. – 255 с.

7. Home Assistant Documentation. Official resource [Електронний ресурс]. – Режим доступу: https://www.home-assistant.io/ (дата звернення: 05.05.2025).

8. Kodali R. K., Jain V., Bose S., Boppana L. IoT based smart security and home automation system // 2016 International Conference on Computing, Communication and Automation (ICCCA), IEEE. – 2016. – С. 1286–1289.

9. Main Page domoticz. Official resource [Електронний ресурс]. – Режим доступу: https://www.domoticz.com/wiki/Main_Page (дата звернення: 13.05.2025).

10. openHAB Documentation. Official resource [Електронний ресурс]. – Режим доступу: https://www.openhab.org/docs/ (дата звернення: 13.06.2025).

11. Pavithra D., Balakrishnan R. IoT based monitoring and control system for home automation // 2015 Global Conference on Communication Technologies (GCCT), IEEE. – 2015. – С. 169–173.

12. Saha S., Ishraque H., Islam M. T., Rahman M. A. IoT based smart home automation and energy management // Thesis & Report, BSc (Electrical and Electronic Engineering), Brac University. – 2019. – 85 с.

13. Uncovering IoT Threats in the Cybercrime Underground // Trend Micro Research [Електронний ресурс]. – 2019. – Режим доступу: https://documents.trendmicro.com/assets/white_papers/wp-theinternet-of-things-in-the-cybercrime-underground.pdf (дата звернення: 20.06.2025).

14. 14. Основні проблеми розумних будинків і як їх можна вирішити? // Кластер. Інженерні системи та мережі [Електронний ресурс]. – 2019. – Режим доступу: https://klaster.ua/ua/stati-i-obzory/osnovnyeproblemy-umnyhdomov-i-kak-ih-mozhno-reshit/ (дата звернення: 05.06.2025).

15. 15. Полякова О. В. Класифікація функціональних складових елементів системи інтелектуального керування середовищем при проектуванні житла // Вісник Київського національного університету технологій та дизайну. Серія: Технічні науки. – 2016. – № 4. – С. 133–141.

16. MQTT Essentials [Електронний ресурс]. – Режим доступу: https://www.hivemq.com/mqtt-essentials/ (дата звернення: 15.04.2025).

17. Kranz M. Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry. – Wiley & Sons, Incorporated, John, 2016. – 272 с.

18. Madakam S. Internet of Things: Smart Things // International Journal of Future Computer and Communication. – 2015. – Vol. 4, no. 4. – P. 250–253. – Режим доступу: http://www.ijfcc.org/vol4/395-ICNT2014-2-203.pdf (дата звернення: 03.05.2025).