

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

«До захисту допущено»

Завідувач кафедри

_____Анатолій МАКАРЕНКО

« ____ » _____ 20__ р.

Дипломна робота
на здобуття ступеня бакалавра
зі спеціальності 172 Телекомунікації та радіотехніка
на тему: «Застосування технології Інтернету речей при реалізації концепції
«Розумний будинок»»

Виконав:

студент IV курсу, групи ТС-22

Ригас Валентин Володимирович _____

Керівник:

Старший викладач кафедри ЕКІР, к.т.н.

Новіков Валерій Іванович _____

Рецензент:

Професор кафедри ТК, д.т.н., професор

Лисенко Олександр Іванович _____

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.

Студент (-ка) _____

Київ – 2026 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«___» _____ 20__ р.

ЗАВДАННЯ

на дипломну роботу студенту

Ригасу Валентину Володимировичу

1. Тема роботи «Застосування технології Інтернету речей при реалізації концепції «Розумний будинок»», керівник роботи Старший викладач, к.т.н. Новіков Валерій Іванович, затверджені наказом по університету від «26» травня 2026 р. № 1912 - С
2. Термін подання студентом роботи 09 червня 2026
3. Вихідні дані до роботи Науково-технічні матеріали щодо архітектури Інтернету речей (IoT) та систем «Розумний будинок», специфікації бездротових протоколів передачі даних (ZigBee, Wi-Fi, BLE), офіційна документація на апаратні платформи (Raspberry Pi) і програмне забезпечення (Home Assistant, MQTT), а також матеріали з методів забезпечення кібербезпеки локальних мереж.
4. Зміст роботи Обґрунтувати актуальність застосування технологій Інтернету речей (IoT) для реалізації концепції «Розумний будинок». Виконати комплексний аналіз архітектури IoT-систем, бездротових протоколів передачі даних та методів забезпечення їх кібербезпеки. Сформулювати завдання для проектування системи домашньої автоматизації та обрати платформу Home Assistant для її координації. Визначити ключові показники ефективності роботи

обладнання та сформувати базові сценарії автоматизації (освітлення, клімат, безпека). Побудувати практичну модель системи на базі Raspberry Pi та протоколу MQTT й провести дослідження обміну даними між IoT-компонентами. Виконати аналіз результатів експериментального тестування та обґрунтувати доцільність застосування розроблених рішень для підвищення надійності й енергоефективності житлових об'єктів.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

1. Тема, мета, завдання, об'єкт та предмет дослідження.
2. Загальна концептуальна схема взаємодії елементів у системі Інтернету речей (M2M взаємодія).
3. Архітектура мережевих протоколів IoT та порівняння топологій (зірка, дерево, mesh-мережа).
4. Хронологія еволюції концепції Інтернету речей та основні сфери застосування (Smart Home, IIoT, Smart City, IoMT).
5. Структура внутрішньої мережі та комбіноване використання дротових і бездротових з'єднань системи «розумного будинку».
6. Порівняльна характеристика технологій та протоколів передачі даних (Wi-Fi, ZigBee, Z-Wave, Bluetooth).
7. Основні напрямки автоматизації процесів: системи керування освітленням, клімат-контролю та безпеки.
8. Віддалене керування та моніторинг: взаємодія з хмарними сервісами, мобільними додатками та голосовими помічниками.
9. Основні кіберзагрози для IoT-систем та комплексні методи захисту даних (шифрування, автентифікація, сегментація).
10. Практична реалізація: головна панель керування та загальна схема підключення IoT-пристроїв до системи Home Assistant.
11. Налаштування автоматизацій у Home Assistant та логічна схема керування освітленням на основі датчика руху.
12. Аналіз взаємодії компонентів системи: принцип роботи MQTT-брокера та алгоритм обміну повідомленнями.
13. Критерії оцінки ефективності функціонування IoT-системи.
14. Результати тестування: аналіз часу реакції системи на події та моніторинг стабільності використання ресурсів.
15. Оцінка енергоефективності, надійності передачі даних та ключові переваги реалізованої системи на базі Home Assistant.
16. Можливості масштабування локальної мережі та перспективи розвитку IoT-технологій у концепції розумного будинку.
17. Висновки за результатами дипломної роботи.

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Дослідження теоретичних основ Інтернету речей та концепції «Розумний будинок»	15.03.2026	Виконано
2	Аналіз особливостей побудови та управління системами «розумного будинку» на основі IoT	15.04.2026	Виконано
3	Реалізація та оцінка ефективності IoT-системи на базі Home Assistant	15.05.2026	Виконано
4	Вступ, Висновки	04.06.2026	Виконано
5	Чистовий варіант дипломної роботи, презентація	08.06.2026	Виконано

Студент

Валентин РИГАС

Керівник роботи

Валерій НОВІКОВ

РЕФЕРАТ

Розмір пояснювальної записки – 82 арк., містить 28 ілюстрацій, 6 таблиць.

Ця дипломна робота присвячена темі «Застосування технології Інтернету речей при реалізації концепції «Розумний будинок»», а саме дослідженню архітектури, мережевих протоколів та практичній реалізації системи автоматизації житлового приміщення на базі локального сервера керування.

У роботі проведено комплексний аналіз сутності технології Інтернету речей та багаторівневої архітектури систем «розумного будинку». Розглянуто топології внутрішніх мереж, здійснено порівняльний аналіз сучасних бездротових протоколів передачі даних (Wi-Fi, ZigBee, Z-Wave, Bluetooth) та визначено їхню ефективність для побудови надійних і безпечних систем домашньої автоматизації.

Особливу увагу приділено практичному аспекту — розробці та впровадженню IoT-системи на базі одноплатного комп'ютера Raspberry Pi та програмної платформи Home Assistant. У дипломній роботі детально описано процес інтеграції кінцевих пристроїв і налаштування локальної мережі з використанням протоколу ZigBee та MQTT-брокера. Представлено приклад практичного застосування — реалізацію системи автоматизованого керування освітленням на основі датчика руху, що дозволяє оптимізувати енергоспоживання та забезпечити автономне функціонування освітлювальних приладів.

Також здійснено експериментальну оцінку ефективності розробленої системи, зокрема проаналізовано час реакції, стабільність доставки повідомлень та показники енергоспоживання, що підтвердило надійність та доцільність обраних інженерних рішень.

Ключові слова: розумний будинок, Інтернет речей, автоматизація освітлення, Home Assistant, ZigBee, Raspberry Pi, MQTT-брокер.

ABSTRACT

The explanatory note consists of 82 pages, 28 illustrations, and 6 tables.

This diploma thesis is devoted to the topic "Application of Internet of Things technology in the implementation of the 'Smart Home' concept", specifically focusing on the study of the architecture, network protocols, and the practical implementation of a residential automation system based on a local control server.

The paper provides a comprehensive analysis of the essence of Internet of Things technology and the multi-level architecture of "smart home" systems. Internal network topologies are considered, a comparative analysis of modern wireless data transmission protocols (Wi-Fi, ZigBee, Z-Wave, Bluetooth) is carried out, and their efficiency for building reliable and secure home automation systems is determined.

Special attention is paid to the practical aspect — the development and implementation of an IoT system based on a Raspberry Pi single-board computer and the Home Assistant software platform. The thesis describes in detail the process of integrating end devices and configuring a local network using the ZigBee protocol and an MQTT broker. An example of practical application is presented — the implementation of an automated lighting control system based on a motion sensor, which allows for optimizing energy consumption and ensuring the autonomous operation of lighting devices.

An experimental evaluation of the developed system's efficiency was also carried out; in particular, the response time, message delivery stability, and energy consumption indicators were analyzed, which confirmed the reliability and feasibility of the chosen engineering solutions.

Keywords: smart home, Internet of Things, lighting automation, Home Assistant, ZigBee, Raspberry Pi, MQTT broker.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ	9
ВСТУП.....	11
1 ТЕОРЕТИЧНІ ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ ТА КОНЦЕПЦІЇ «РОЗУМНИЙ БУДИНОК».....	13
1.1 Сутність та принципи функціонування Інтернету речей.....	13
1.2 Поняття та структура системи «Розумний будинок»	21
1.3 Архітектура та технічні вимоги до систем розумного будинку.....	27
1.4 Основні компоненти IoT-систем у житлових об'єктах	30
1.5 Висновки до розділу 1	33
2 ОСОБЛИВОСТІ ПОБУДОВИ ТА УПРАВЛІННЯ СИСТЕМАМИ «РОЗУМНОГО БУДИНКУ» НА ОСНОВІ IoT	35
2.1 Організація внутрішніх мереж у житлових приміщеннях	35
2.2 Технології та протоколи передачі даних Wi-Fi, ZigBee, Z-Wave, Bluetooth.....	39
2.4 Віддалене керування та моніторинг системи	47
2.5 Проблеми безпеки та захисту даних	50
2.6 Висновки до розділу 2	53
3 РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ IoT-СИСТЕМИ НА БАЗІ HOME ASSISTANT.....	54
3.1 Реалізація та налаштування системи.....	54
3.2 Аналіз взаємодії компонентів системи	63
3.3 Оцінка ефективності роботи системи	65
3.4 Аналіз результатів та перспективи розвитку	70
3.5 Оцінка ефективності функціонування розробленої системи.....	73
3.6 Висновки до розділу 3	75
ВИСНОВКИ.....	77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	82

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

АЦП — Аналогово-цифровий перетворювач.

ДБЖ — Джерело безперебійного живлення.

МН — Машинне навчання.

ШІМ — Широтно-імпульсна модуляція.

6LoWPAN — IPv6 over Low-Power Wireless Personal Area Networks, стандарт передачі пакетів протоколу IPv6 безпосередньо через малопотужні радіоканали.

AES-128 — Advanced Encryption Standard, алгоритм симетричного шифрування, який використовується для захисту даних у локальних радіомережах.

AIoT — Artificial Intelligence of Things, концепція штучного інтелекту речей.

API — Application Programming Interface, стандартизований інтерфейс прикладного програмування.

BLE — Bluetooth Low Energy, технологія бездротового зв'язку з ультранизким енергоспоживанням.

CPU — Central Processing Unit, центральний процесор (обчислювальна потужність).

DDoS — Distributed Denial of Service, тип мережевої кібератаки з метою перевантаження серверів або порушення доступу.

HAOS — Home Assistant OS, оптимізована операційна система для розгортання сервера Home Assistant.

HCI — Human-Computer Interaction, традиційна модель взаємодії «людина-комп'ютер».

HVAC — Heating, Ventilation, and Air Conditioning, комплексні системи клімат-контролю (опалення, вентиляції та кондиціонування).

IEEE 802.15.4 — стандарт бездротових персональних мереж, який лежить в основі протоколу ZigBee.

IIoT — Industrial Internet of Things, промисловий Інтернет речей.

IoMT — Internet of Medical Things, Інтернет медичних речей.

IoT — Internet of Things, Інтернет речей — гетерогенна інформаційна інфраструктура фізичних пристроїв.

IPv6 — Internet Protocol version 6, інтернет-протокол маршрутизації мережевого рівня версії 6.

M2M — Machine-to-Machine, міжмашинна взаємодія (безпосередній обмін даними між пристроями).

MEMS — Мікроелектромеханічні системи.

Mesh-мережі — комірчасті, самоорганізовані та самовідновлювані топології бездротових мереж.

MQTT — Message Queuing Telemetry Transport, поширений протокол обміну повідомленнями у системах Інтернету речей.

NDIR — Non-Dispersive Infrared, інфрачервоний недисперсійний сенсор (наприклад, для вимірювання рівня вуглекислого газу).

NFC — Near Field Communication, технологія бездротового зв'язку малого радіуса дії.

PIR — Passive Infrared, пасивний інфрачервоний детектор руху.

QoS — Quality of Service, якість обслуговування (рівень надійності доставки даних у мережі).

RAM — Random Access Memory, оперативна пам'ять.

RFID — Radio Frequency Identification, технологія радіочастотної ідентифікації.

SCADA — Системи диспетчерського управління та збору даних (Supervisory Control And Data Acquisition).

TLS / SSL — Transport Layer Security / Secure Sockets Layer, криптографічні протоколи для безпечного (зашифрованого) IP-з'єднання.

VLAN — Virtual Local Area Network, віртуальна ізольована локальна мережа.

WPA3 — Сучасний протокол захисту бездротових мереж Wi-Fi.

WSN — Wireless Sensor Networks, бездротові сенсорні мережі.

YAML — Yet Another Markup Language, мова розмітки для написання програмного коду та конфігураційних файлів.

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується стрімкою цифровізацією та інтеграцією обчислювальних систем у всі сфери життя людини. Одним із найбільш перспективних напрямів є технологія Інтернету речей (IoT), яка забезпечує взаємодію фізичних пристроїв між собою та з користувачем через мережу Інтернет. Завдяки цьому створюються інтелектуальні системи, здатні автоматично збирати, аналізувати та передавати дані, мінімізуючи необхідність прямого втручання людини. [3]

Особливо активно технології IoT впроваджуються у побутову сферу, де формується концепція «розумного будинку». Така система передбачає автоматизацію керування освітленням, опаленням, безпекою, побутовими приладами та іншими елементами житлового середовища. Використання «розумного будинку» дозволяє підвищити рівень комфорту, безпеки та енергоефективності, а також оптимізувати використання ресурсів. [3] [4]

Актуальність теми зумовлена зростанням потреби у впровадженні енергоощадних та інтелектуальних рішень для житлових приміщень, а також широкими можливостями сучасних IoT-платформ для створення доступних систем автоматизації. У цьому контексті особливу увагу привертає використання програмної платформи Home Assistant у поєднанні з мікрокомп'ютером Raspberry Pi, що дозволяє реалізовувати гнучкі та масштабовані системи керування «розумним будинком».

Метою даної дипломної роботи є дослідження технології Інтернету речей та її застосування при реалізації концепції «розумного будинку», а також практична розробка й оцінка ефективності локальної IoT-системи на базі Home Assistant із реалізацією сценаріїв автоматизації побутових процесів.

Для досягнення поставленої мети визначено такі завдання:

- 1) проаналізувати принципи та особливості технології Інтернету речей;
- 2) дослідити архітектуру та компоненти систем «розумного будинку»;

3) порівняти сучасні мережеві протоколи передачі даних, що використовуються в IoT-середовищі;

4) здійснити практичну реалізацію системи на базі Home Assistant та Raspberry Pi;

5) налаштувати автоматизовані сценарії керування пристроями;

6) оцінити ефективність та перспективи розвитку розробленої системи.

Об'єктом дослідження є система «розумний будинок» як приклад кіберфізичної IoT-екосистеми.

Предметом дослідження виступають технології, програмні та апаратні засоби Інтернету речей, що використовуються для автоматизації та керування житловим середовищем.

1 ТЕОРЕТИЧНІ ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ ТА КОНЦЕПЦІЇ «РОЗУМНИЙ БУДИНОК»

1.1 Сутність та принципи функціонування Інтернету речей

Стрімка еволюція інформаційно-комунікаційних систем, безпрецедентний рівень мініатюризації обчислювальних апаратних платформ та розвиток бездротових технологій передачі даних на початку ХХІ століття зумовили перехід до нової технологічної парадигми — Інтернету речей (Internet of Things, IoT).

У сучасному науково-технічному дискурсі концепція IoT розглядається як масштабна, гетерогенна інформаційна інфраструктура, що функціонує на декількох ієрархічних рівнях. Як показано на рисунку 1.1, архітектура IoT-системи (зокрема, у контексті «Розумного будинку») базується на чотирьох ключових етапах обробки та передачі інформації:

1. Рівень сприйняття (Фізичні пристрої): Це фундамент системи, що складається з кінцевих вузлів («речей») — датчиків температури, вологості, руху, а також виконавчих пристроїв (розумних замків, приводів). Саме на цьому рівні реалізується безпосередня M2M взаємодія (міжмашинна), де пристрої обмінюються даними між собою для миттєвого реагування на зміну середовища.

2. Мережевий рівень (Комунікація): Забезпечує транспортування зібраних даних (Data Flow) через IoT-шлюзи за допомогою різноманітних протоколів (ZigBee, Z-Wave, Wi-Fi, Bluetooth LE). Тут відбувається агрегація даних та їх спрямування до централізованих систем обробки.

3. Рівень обробки хмари та даних: На цьому етапі інформація накопичується в хмарних платформах, де здійснюється глибока аналітика, працюють двигуни ШІ/МН (штучного інтелекту та машинного навчання) і формуються віддалені команди для керування пристроями.

4. Прикладний рівень (Інтерфейс користувача): Верхній рівень, що надає людині інструменти для моніторингу, конфігурації сценаріїв та управління через мобільні додатки «Розумний дім» або веб-портали.

Технологія IoT забезпечує якісний перехід від традиційної моделі взаємодії «людина-комп'ютер» (HCI) до автоматизованої моделі, де процеси управління кліматом, безпекою та енергоспоживанням відбуваються автономно. Це дозволяє системі не просто виконувати команди, а самостійно приймати рішення на основі аналізу потоку даних, мінімізуючи необхідність ручного втручання користувача. [15]



Рисунок 1.1 – Загальна концептуальна схема взаємодії елементів у системі Інтернету речей (M2M взаємодія)

Основні поняття та багаторівнева архітектура IoT

Для забезпечення інтероперабельності, масштабованості та надійності систем Інтернету речей застосовується багаторівнева еталонна архітектура. Хоча різні міжнародні консорціуми пропонують власні моделі (наприклад, трирівнева, п'ятирівнева або семирівнева модель IoT World Forum), з

інженерної точки зору найбільш доцільним є поділ архітектури на чотири базові рівні.

Перший рівень — фізичний рівень або рівень сприйняття (Perception Layer). Він формує апаратну основу мережі та безпосередньо контактує з фізичним середовищем. До його складу входять кінцеві вузли (End Nodes), які поділяються на дві основні категорії: сенсори (або датчики) та актуатори. Сенсори відповідають за перетворення неелектричних фізичних величин (температура, вологість, рівень освітленості, концентрація газів, наявність руху) в електричні сигнали та їх подальшу оцифровку. Актуатори, у свою чергу, є виконавчими механізмами (реле, сервоприводи, димери, електромагнітні клапани), які отримують цифрові команди з верхніх рівнів та виконують фізичні дії (наприклад, перекриття подачі води у разі фіксації протікання). Окремим елементом цього рівня є технології радіочастотної ідентифікації (RFID) та мітки NFC, які дозволяють ідентифікувати об'єкти в просторі. [3]

Другий рівень — мережевий або транспортний (Network Layer). Цей рівень є критично важливим ядром системи, оскільки він забезпечує надійну маршрутизацію та передачу даних від масиву сенсорів до центрів обробки інформації та передачу керуючих команд у зворотному напрямку. Враховуючи специфіку «розумного будинку», де прокладання додаткових кабельних трас часто є економічно недоцільним або неможливим, домінуючу роль тут відіграють бездротові технології. Серед них виділяють Wi-Fi (для передачі великих обсягів даних, наприклад, відеопотоків з камер спостереження), Bluetooth Low Energy (BLE) та спеціалізовані протоколи сітчастих (mesh) мереж — ZigBee та Z-Wave. [10]

Варто наголосити, що середовище IoT у межах житлових приміщень часто зіштовхується з проблемою фізичних перешкод (стіни, перекриття) та радіоелектронних завад, що може призводити до втрати пакетів даних. Тому для побудови надійної інфраструктури «розумного будинку» критично важливою є підтримка топології комірчастої мережі (mesh-мережі). Завдяки

спеціальним алгоритмам маршрутизації, кожен пристрій (наприклад, розумна розетка або вимикач), що підключений до стаціонарного живлення, може виступати ретранслятором сигналу для інших вузлів. Це забезпечує динамічне знаходження оптимальних шляхів передачі даних в обхід перешкод та гарантує високу відмовостійкість і площу покриття системи без необхідності встановлення додаткових підсилювачів сигналу.

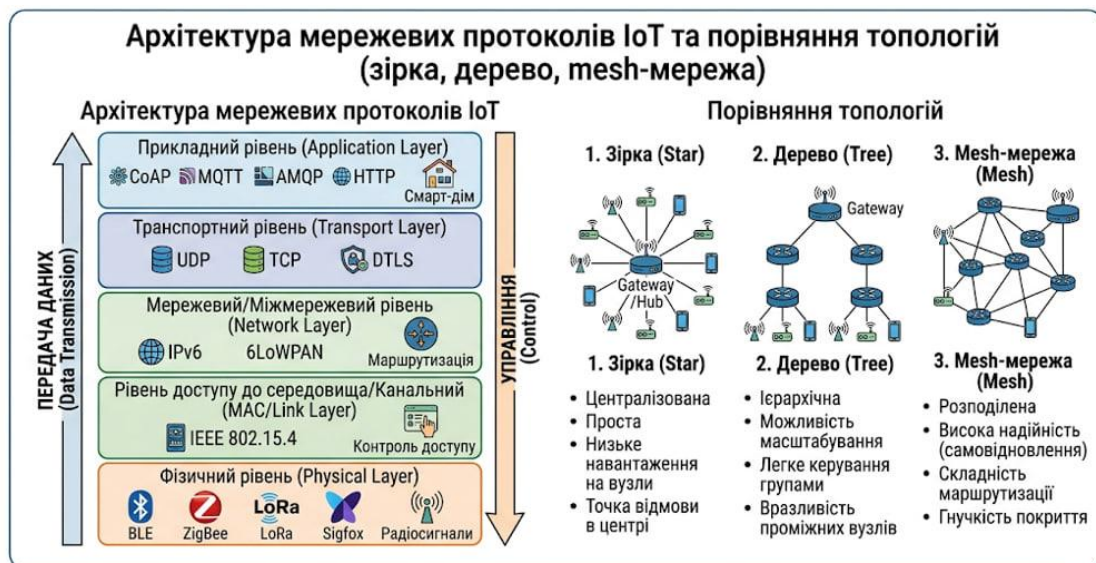


Рисунок 1.2 – Архітектура мережевих протоколів IoT та порівняння топологій

Третій рівень — рівень проміжного програмного забезпечення та периферійних обчислень (Middleware / Edge Computing Layer). На стику локальної сенсорної мережі (наприклад, мережі Z-Wave) та глобальної мережі Інтернет (TCP/IP) встановлюються апаратні шлюзи (Gateways) або хаби. Їхня функція полягає у трансляції протоколів, первинній агрегації та фільтрації даних. У сучасних архітектурах спостерігається тенденція до зміщення обчислювальних потужностей ближче до джерела даних (Edge Computing), що дозволяє приймати критичні рішення локально, без необхідності звернення до хмарних серверів. Це суттєво зменшує затримку мережі (latency) та підвищує відмовостійкість системи «розумного будинку» у разі тимчасової втрати інтернет-з'єднання.

Четвертий рівень — прикладний та хмарний рівень (Application and Cloud Layer). Включає в себе глобальні хмарні сервери, де акумулюються великі масиви даних (Big Data), та програмні інтерфейси (мобільні додатки, веб-панелі), через які користувач взаємодіє з системою. Саме на цьому рівні розгортаються алгоритми машинного навчання та предиктивної аналітики, які аналізують поведінкові патерни мешканців будинку для автоматичної корекції сценаріїв роботи обладнання.

Історія розвитку технології

Хоча термін «Інтернет речей» став загальноновживаним у науковій та популярній літературі лише у XXI столітті, технологічні та теоретичні передумови для його виникнення формувалися протягом кількох десятиліть. Еволюційний шлях IoT можна розділити на кілька ключових етапів, кожен з яких характеризувався подоланням певних технологічних бар'єрів.

Епоха ранньої телеметрії та M2M-взаємодії (1960-ті – 1990-ті роки). Задовго до появи глобальної мережі Інтернет у промисловому секторі та на об'єктах критичної інфраструктури почали впроваджуватися системи диспетчерського управління та збору даних (SCADA). Ці системи дозволяли зчитувати інформацію з віддалених датчиків та керувати механізмами на відстані. Проте їхнім головним недоліком була ізольованість: вони використовували дротові лінії зв'язку та пропрієтарні закриті протоколи, що унеможливлювало інтеграцію обладнання від різних виробників у єдину глобальну мережу.

Зародження концепції та термінології (кінець 1990-х років). Офіційне авторство терміну «Internet of Things» приписують Кевіну Ештону (Kevin Ashton), британському інноватору та досліднику Массачусетського технологічного інституту (MIT). У 1999 році, під час презентації для корпорації Procter & Gamble, Ештон запропонував концепцію використання технології радіочастотної ідентифікації (RFID) для оптимізації глобальних ланцюгів постачання. Фундаментальна ідея полягала в тому, щоб дозволити комп'ютерам

збирати інформацію про фізичні об'єкти самостійно, без необхідності ручного введення даних людиною, яка, за словами Ештона, має обмежений час, увагу та точність.

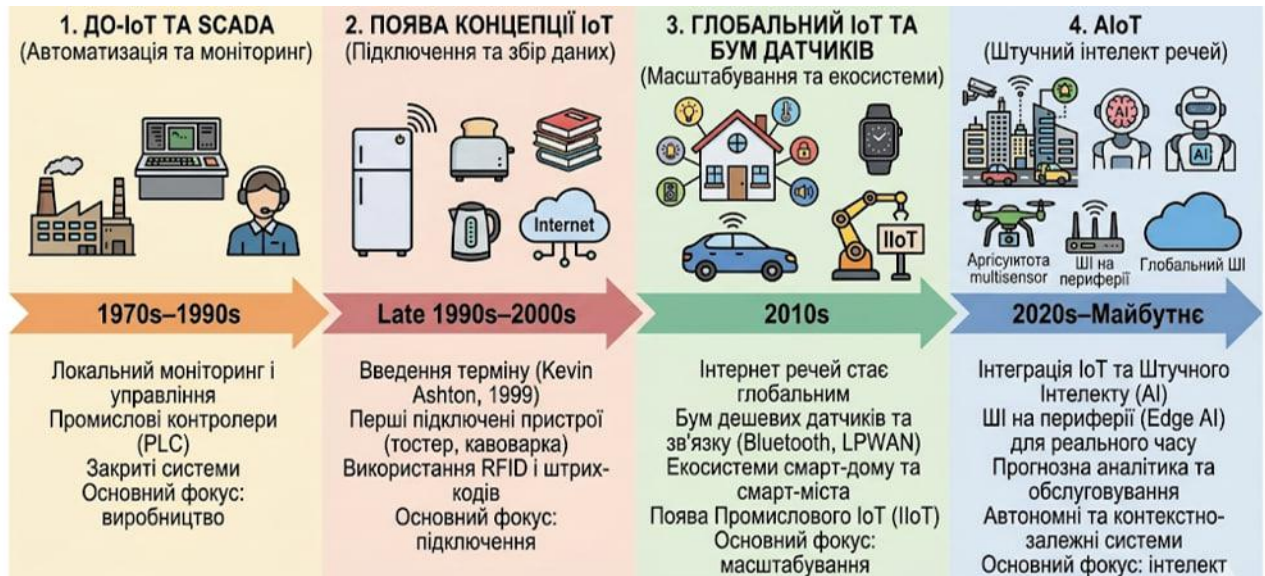


Рисунок 1.3 – Хронологія еволюції концепції Інтернету речей (від SCADA до AIoT)]

Етап стандартизації бездротових сенсорних мереж (2000-ні роки). Розвиток мікроелектромеханічних систем (MEMS) дозволив значно зменшити розміри датчиків та знизити їхню собівартість. Це дало поштовх до активного розвитку бездротових сенсорних мереж (Wireless Sensor Networks, WSN). Важливою віхою стала розробка стандартів, орієнтованих на низьке енергоспоживання. У 2004 році консорціум ZigBee Alliance випустив першу повноцінну специфікацію протоколу ZigBee (ZigBee Specification), який базується на стандарті IEEE 802.15.4. [2] Цей крок став каталізатором для розробки автономних пристроїв «розумного будинку», здатних працювати від одного елемента живлення роками. [1] Паралельно набирала оберти технологія Z-Wave, яка згодом кристалізувалася у специфікацію Z-Wave v.7.1x, забезпечивши високий рівень сумісності прикладного та мережевого рівнів для домашньої автоматизації. [5]

Ера глобальної IP-адресації та розширення (2010-ті роки – наш час). Аналітичний підрозділ компанії Cisco (Cisco IBSG) підрахував, що у період між 2008 та 2009 роками кількість пристроїв, підключених до Інтернету, перевищила чисельність населення планети. Саме цей момент вважається фактичним народженням глобального Інтернету речей. Проте масштабування системи наштовхнулося на проблему вичерпання адресного простору протоколу IPv4. Вирішенням став масовий перехід на інтернет-протокол версії 6 (IPv6) та розробка стандарту 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), що дозволило передавати IP-пакети безпосередньо через малопотужні радіоканали стандарту IEEE 802.15.4. Завдяки IPv6 кожен, навіть найменший сенсор, отримав можливість мати унікальну маршрутизовану IP-адресу у глобальній мережі.

Сфери застосування

Гнучкість мережевої архітектури та широка номенклатура кінцевих пристроїв дозволяють інтегрувати технології Інтернету речей практично в усі сфери життєдіяльності людини та сектори економіки. У сучасній літературі прийнято виділяти кілька основних доменів застосування IoT:

1. Розумний будинок (Smart Home) — це домен, що безпосередньо стосується теми даного дипломного дослідження. Інтеграція IoT у житловий простір передбачає створення конвергентної мережі, яка об'єднує підсистеми клімат-контролю (HVAC), освітлення, безпеки, управління мультимедіа та побутовою технікою. Використання датчиків присутності, температури та освітленості у комбінації з інтелектуальними алгоритмами управління дозволяє будувати адаптивні сценарії. Це не лише підвищує рівень комфорту мешканців, але й оптимізує споживання енергоресурсів (газу, електроенергії), зменшуючи комунальні витрати.

2. Промисловий Інтернет речей (Industrial IoT, IIoT). Є ключовим компонентом Четвертої промислової революції (Індустрія 4.0). Впровадження мереж датчиків на виробничому обладнанні дозволяє збирати телеметрію в режимі реального часу. Аналіз цих даних лежить в основі концепції

предиктивного (прогнозованого) технічного обслуговування, коли система завчасно попереджає про можливу поломку вузла агрегату, мінімізуючи фінансові втрати від позапланових простоїв підприємства.

3. Розумні міста (Smart Cities). Масштабування концепції IoT до рівня урбаністичної інфраструктури. Технології використовуються для вирішення проблем трафіку (інтелектуальні транспортні системи та світлофори), оптимізації вуличного освітлення (автоматичне димірування залежно від трафіку та часу доби), моніторингу стану навколишнього середовища (датчики якості повітря) та автоматизації служб житлово-комунального господарства (наприклад, розумні лічильники ресурсів — Smart Metering).

4. Охорона здоров'я (Internet of Medical Things, IoMT). Використання натільних медичних пристроїв та імплантатів, оснащених модулями бездротового зв'язку, дозволяє здійснювати безперервний дистанційний моніторинг фізіологічних показників пацієнтів (серцевий ритм, артеріальний тиск, сатурація кисню). Це критично важливо для людей із хронічними захворюваннями, оскільки дозволяє медичному персоналу оперативно реагувати на погіршення стану здоров'я.



Рисунок 1.4 – Сфери застосування технології Інтернету речей (Smart Home, IIoT, Smart City, IoMT)

Підсумовуючи розгляд сутності та принципів функціонування Інтернету речей, необхідно зазначити, що ця концепція є складним технологічним комплексом. Ефективність реалізації систем «розумного будинку» напряду залежить від грамотного проектування мережевого рівня, обґрунтованого вибору протоколів маршрутизації в умовах LLN та забезпечення надійного захисту даних на всіх рівнях архітектури.

1.2 Поняття та структура системи «Розумний будинок»

Історичний розвиток людського суспільства нерозривно пов'язаний із постійним прагненням до вдосконалення умов проживання, оптимізації побутових процесів та підвищення загального рівня безпеки і комфорту. Якщо в минулому столітті головним вектором розвитку житлової інфраструктури була базова електрифікація та механізація ручної праці за допомогою побутової техніки, то на сучасному етапі розвитку інформаційного суспільства та глобальної цифровізації ми спостерігаємо перехід до концептуально нових парадигм. Однією з таких інноваційних парадигм, що кардинально змінює підходи до організації житлового простору, є концепція «Розумного будинку» (Smart Home), яка виступає одним із наймасштабніших і найперспективніших напрямків практичної реалізації технології Інтернету речей (Internet of Things, IoT). [4]

З науково-технічної точки зору, поняття «Розумний будинок» не обмежується простим набором дистанційно керованих пристроїв. Це високотехнологічна, комплексна кіберфізична екосистема, яка інтегрує в єдину інформаційно-телекомунікаційну інфраструктуру різноманітні сенсорні вузли, виконавчі механізми (актуатори), мікропроцесорні контролери, а також гетерогенні мережі передачі даних. Головною метою функціонування такої системи є забезпечення максимальної автономності житлового середовища, проактивна автоматизація рутинних процесів, предиктивне управління

ресурсами задля підвищення енергоефективності, а також гарантування комплексного захисту та безпеки мешканців.

За своєю логічною та фізичною структурою система «Розумного будинку» повністю успадковує та адаптує під свої потреби класичну багаторівневу архітектуру систем Інтернету речей. Згідно з дослідженнями в галузі побудови IoT-мереж, базову архітектуру доцільно розглядати через призму трьох фундаментальних взаємопов'язаних рівнів [11]:

1. Рівень сприйняття (Perception Layer), або фізичний рівень. Цей рівень є фундаментом усієї системи, оскільки саме він відповідає за первинну взаємодію цифрової екосистеми з реальним фізичним світом. До його складу входять різноманітні кінцеві вузли, які можна поділити на дві великі категорії: сенсори та актуатори. Сенсори виконують роль "органів чуття" розумного будинку: вони безперервно збирають метрики про стан навколишнього середовища (температуру, відносну вологість, рівень освітленості, концентрацію вуглекислого газу, наявність руху або звуку, стан вікон та дверей тощо). Актуатори, у свою чергу, виступають "м'язами" системи, перетворюючи цифрові керуючі сигнали у фізичні дії (замикання контактів розумних реле, обертання сервоприводів на трубах водопостачання, зміна інтенсивності світіння LED-ламп).

2. Мережевий рівень (Network Layer), або рівень транспортування даних. Головним завданням цього структурного елемента є забезпечення надійної, захищеної та своєчасної передачі інформаційних пакетів від рівня сприйняття до рівня обробки, а також трансляція керуючих команд у зворотному напрямку. [8] У контексті житлових приміщень прокладання дротових ліній зв'язку часто є економічно недоцільним або фізично неможливим, тому домінуючу роль тут відіграють сучасні бездротові технології. Як детально розглядається в, вибір конкретного протоколу передачі даних (Wi-Fi, Bluetooth Low Energy, ZigBee) є компромісом між пропускнуою здатністю, енергоспоживанням кінцевих вузлів та здатністю долати фізичні перешкоди (стіни, перекриття).[1]Зокрема, спеціалізовані протоколи сімейства

ZigBee [2] та Z-Wave [5] набули широкого поширення завдяки можливості побудови самоорганізованих комірчастих мереж (mesh-топологія), що нівелює проблему "мертвих зон" та значно підвищує відмовостійкість усієї системи.

3. Рівень додатків, агрегації та управління (Application Layer). Це інтелектуальне ядро екосистеми. Сюди відносяться локальні центральні контролери (хаби), віддалені хмарні сервери та бази даних, а також різноманітні користувацькі інтерфейси (мобільні застосунки, веб-портالي, сенсорні панелі, системи розпізнавання голосових команд). На цьому рівні зібрані розрізнені "сирі" дані агрегуються, структуруються та піддаються глибокому аналізу. Сучасні системи управління все частіше використовують алгоритми машинного навчання для виявлення прихованих закономірностей у поведінці користувачів, що дозволяє формувати складні адаптивні сценарії поведінки будинку.

Структурно-функціональна організація та інтеграція цих рівнів вимагає неухильного дотримання міжнародних галузевих стандартів.[3] [11] Наприклад, специфікації протоколу Z-Wave чітко регламентують не лише фізичні параметри радіосигналу, але й механізми маршрутизації, шифрування та логічної сумісності пристроїв від різних вендорів, що є критичною передумовою для вільного масштабування розумного будинку в майбутньому.

Основні функції системи

Аналізуючи функціональні можливості сучасних апаратно-програмних комплексів, що реалізують концепцію «Розумного будинку», варто зазначити, що їхній спектр є надзвичайно широким і охоплює практично всі без винятку аспекти життєдіяльності людини в межах житлового простору. Ці функції доцільно класифікувати за такими ключовими векторами:

- Комплексне керування мікрокліматом (HVAC-системи): Підтримка оптимальних кліматичних умов має безпосередній вплив не лише на комфорт, але й на здоров'я та фізіологічний стан людини. Система не просто керує окремими приладами, а комплексно синхронізує роботу інтелектуальних

термостатів, систем кондиціонування, зволожувачів повітря, теплої підлоги та вентиляційних установок з рекуперацією. Завдяки постійному моніторингу система здатна предиктивно змінювати режими роботи, спираючись на зовнішні метеорологічні дані або статистику присутності мешканців у певних зонах будинку.

- Інтелектуальне управління освітленням: Ця функція вийшла далеко за межі банального дистанційного вмикання та вимикання світла. Сучасний рівень розвитку дозволяє реалізовувати плавне димування, зміну колірної температури відповідно до циркадних ритмів людини (біодинамічне освітлення) та управління RGB-спектром. Формування складних світлових сценаріїв (наприклад, "Вечірнє читання", "Перегляд кіно", "Імітація присутності господарів під час відпустки") у поєднанні з датчиками освітленості та руху дозволяє мінімізувати нецільове використання електроенергії.

- Системи превентивної безпеки та моніторингу: Забезпечення безпеки поділяється на два масштабні блоки: захист від несанкціонованого проникнення (інтеграція датчиків розбиття скла, відкриття дверей, детекторів руху, систем відеоаналітики та розумних біометричних замків) та інженерна (техногенна) безпека. Остання включає критично важливі функції раннього виявлення витoku води із негайним автоматичним перекриттям магістральних електроклапанів, а також детекцію задимлення чи витoku побутового газу з паралельним сповіщенням екстрених служб та власника.

- Глибинний енергоменеджмент та ресурсозбереження: В умовах постійного зростання вартості енергоносіїв функція оптимізації витрат набуває особливої актуальності. Система здійснює безперервний моніторинг споживання електроенергії, води та газу в режимі реального часу, дозволяючи виявляти аномальні витрати (наприклад, несправні прилади) та оптимізувати роботу енергоємної техніки, зміщуючи її активність на періоди дії пільгових (нічних) тарифних планів.

Рівні автоматизації

Впровадження інноваційних методів обробки великих даних (Big Data) та штучного інтелекту дозволяє виокремити еволюційні етапи розвитку розумних житлових просторів. Системи «Розумного будинку» прийнято класифікувати за рівнями автоматизації, що відображають міру автономності системи від прямого директивного втручання користувача:

Рівень 0: Відсутність автоматизації (Традиційний формат). Управління всіма інженерними та побутовими приладами здійснюється виключно в ручному режимі шляхом безпересередньої фізичної взаємодії користувача з елементами управління (механічні вимикачі, запірні арматура, класичні пульти).

Рівень 1: Дистанційне або віддалене управління. Окремі прилади оснащуються комунікаційними модулями (переважно Wi-Fi або Bluetooth), що дозволяє власнику керувати ними зі смартфона. Однак на цьому етапі відсутня взаємодія пристроїв між собою — кожен з них є ізольованим "розумним" островцем.

Рівень 2: Програмована логічна автоматизація. Пристрої інтегруються в єдину інформаційну мережу під керівництвом центрального хабу. Користувач отримує можливість створювати алгоритмічні сценарії на базі булевої логіки "Якщо – То" (If This Then That). Наприклад: "Якщо спрацював датчик відкриття входних дверей і час доби після 20:00, увімкнути освітлення в передпокої на дві хвилини".

Рівень 3: Контекстно-залежна та адаптивна автоматизація. Система починає аналізувати ширший спектр змінних параметрів і самостійно приймати рішення в заданих межах. Враховується геофенсинг (геолокація смартфонів мешканців), астрономічний час, погодні умови за вікном тощо. Будинок здатний самостійно перейти в режим "Енергозбереження та охорона", просто "зрозумівши", що всі користувачі покинули периметр ділянки.

Рівень 4: Інтелектуальна (Предиктивна) автоматизація. Вершина розвитку екосистеми, що базується на застосуванні нейронних мереж. Розумний будинок

постійно аналізує історичні масиви даних, вивчає звички, графіки та вподобання своїх мешканців. З часом система здатна передбачати потреби користувача, автоматично підлаштовуючи температуру, освітленість та акустичний фон ще до того, як людина сформує відповідний запит. Роль людини зводиться до статусу спостерігача.

Переваги та недоліки

Масштабне впровадження концепції Інтернету речей у структуру житлового фонду має глибокий трансформаційний вплив на якість життя суспільства, однак цей процес супроводжується низкою вагомих інженерних, економічних та експлуатаційних викликів.

Основні переваги впровадження систем розумного будинку:

1. **Максимальна енергоефективність:** Завдяки виключенню людського фактору (наприклад, забутого увімкненого світла) та точній роботі клімат-контролю, загальні витрати на енергоносії можуть знижуватися на 15-30%, що також сприяє зменшенню вуглецевого сліду домогосподарства.
2. **Безпрецедентний рівень безпеки:** Автоматизовані системи здатні реагувати на аварійні ситуації (пожежа, затоплення) за мілісекунди, що мінімізує матеріальні збитки. А наявність систем імітації присутності є потужним психологічним бар'єром для зловмисників.
3. **Персоналізація простору:** Гнучкість налаштувань дозволяє миттєво трансформувати атмосферу житла відповідно до настрою або поточних задач користувача, стираючи межі між людиною та її оточенням.

Основні недоліки, технічні бар'єри та ризики:

1. **Високий фінансовий поріг входу:** Комплексне проєктування інфраструктури, закупівля сертифікованого обладнання та послуги кваліфікованих інсталяторів вимагають значних початкових капіталовкладень, які окупаються досить тривалий час.

2. Проблема фрагментації стандартів: Незважаючи на зусилля індустрії (наприклад, розробку уніфікованого протоколу Matter), на ринку досі панує "зоопарк" протоколів. Інтеграція пристроїв від різних виробників часто потребує налаштування складних програмних мостів і не завжди гарантує стабільну роботу.

3. Вразливість до перебоїв в інфраструктурі: Глибока автоматизація робить будинок залежним від стабільності електропостачання та наявності інтернет-з'єднання. Відсутність резервних джерел живлення (ДБЖ) може тимчасово паралізувати життєзабезпечення приміщення.

4. Загрози кібербезпеці та приватності: Будучи частиною глобальної мережі, кожен IoT-пристрій стає потенційною точкою входу для кіберзлочинців. Злам системи може призвести не лише до витоку персональних даних (перехоплення відеопотоків, графіків присутності вдома), але й дозволити зловмисникам фізично розблокувати двері або вивести з ладу інженерні комунікації.

Резюмуючи вищевикладене, слід зробити висновок, що розробка та впровадження сучасної системи «Розумного будинку» — це складна багатофакторна інженерна задача. Успішна реалізація таких проєктів, зокрема в рамках дипломного дослідження, вимагає ретельного системного аналізу, де вибір апаратної платформи та протоколів зв'язку має бути жорстко обґрунтований вимогами до надійності, енергоспоживання, безпеки та можливостей подальшої модернізації інфраструктури.

1.3 Архітектура та технічні вимоги до систем розумного будинку

Фундаментальною основою для проєктування та розгортання будь-якої інфраструктури Інтернету речей є вибір оптимальної архітектури. Архітектура системи розумного будинку визначає принципи взаємодії апаратних та програмних компонентів, топологію мережі, алгоритми обробки даних та загальну логіку прийняття рішень. Від правильності архітектурних рішень на

етапі проектування безпосередньо залежать масштабованість, відмовостійкість та функціональна гнучкість системи в процесі її довгострокової експлуатації.

Типи архітектур: централізована та децентралізована

Залежно від розподілу обчислювальних потужностей та логіки управління, сучасні системи смарт-будинків базуються на двох основних архітектурних парадигмах: централізованій та децентралізованій (розподіленій).

Централізована архітектура характеризується наявністю єдиного керуючого ядра — потужного локального контролера (хабу) або віддаленого хмарного сервера. У такій моделі всі кінцеві пристрої (сенсори) виконують виключно функцію збору та передачі "сирих" даних до центру, а актуатори лише пасивно очікують керуючих команд. Уся логіка (сценарії, таймери, аналітика) обробляється центральним вузлом. Топологія мережі у цьому випадку найчастіше нагадує "зірку". *Переваги:* Простота адміністрування, легкість налаштування логіки з єдиного інтерфейсу, нижча вартість кінцевих вузлів (оскільки вони не потребують потужних мікроконтролерів). *Недоліки:* Наявність єдиної точки відмови (Single Point of Failure). У разі апаратного збою центрального контролера або втрати зв'язку з хмарним сервером уся система повністю втрачає працездатність, залишаючи користувача без базових функцій управління. Крім того, централізована обробка в хмарі може викликати мережеві затримки (latency) при виконанні команд.

Децентралізована (розподілена) архітектура спирається на концепції граничних обчислень (Edge Computing) та туманних обчислень (Fog Computing). У такій моделі обчислювальні потужності частково або повністю делегуються на периферію. Кінцеві вузли оснащуються продуктивнішими мікроконтролерами, що дозволяє їм здійснювати первинну обробку даних, фільтрацію шумів та навіть приймати локальні рішення без постійного звернення до головного координатора. Пристрої можуть взаємодіяти між собою напряму за принципом Peer-to-Peer (P2P). *Переваги:* Висока відмовостійкість.

Вихід з ладу одного вузла не призводить до зупинки всієї системи (наприклад, розумний термостат продовжить підтримувати температуру навіть без зв'язку з хабом). Забезпечується мінімальний час відгуку та зменшується навантаження на загальну мережеву інфраструктуру. *Недоліки:* Вища вартість апаратного забезпечення, складність налаштування та маршрутизації сигналів.

Сучасним трендом є використання гібридних архітектур, де критично важливі функції (безпека, опалення) працюють децентралізовано за допомогою mesh-мереж (наприклад, на базі протоколів ZigBee або Z-Wave), а складна аналітика та ресурсоємні задачі виконуються централізовано.

Надійність та безпека

Технічні вимоги до систем розумного будинку регламентують суворі критерії надійності, що зумовлено високою ціною помилки (наприклад, неспрацювання клапана перекриття води під час аварії). Надійність забезпечується на апаратному (дублювання каналів зв'язку, використання блоків безперебійного живлення, апаратні watchdog-таймери в мікроконтролерах) та мережевому рівнях (застосування самовідновлюваних комірчастих топологій, де у разі виходу з ладу одного маршрутизатора сигнал автоматично знаходить обхідний шлях).

Питання безпеки є ще більш багатограним і включає захист від соціотехнічних та кібернетичних загроз. Інфраструктура розумного будинку повинна відповідати наступним вимогам кібербезпеки:

1. Автентифікація та авторизація: Кожен пристрій, що підключається до мережі, повинен проходити криптографічну перевірку.
2. Шифрування трафіку: Усі дані, що передаються між пристроями та сервером, повинні бути зашифровані (наприклад, з використанням алгоритму AES-128 для локальних радіомереж та TLS/SSL для IP-з'єднань).
3. Захист периметра мережі: Використання брандмауерів, сегментація локальної мережі (створення окремої VLAN ізольованої підмережі для IoT-пристроїв, щоб унеможливити доступ до персональних комп'ютерів у разі

компрометації смарт-лампочки) та захист від DDoS-атак на рівні хмарних сервісів.

Сумісність пристроїв (Інтероперабельність)

Гетерогенність екосистеми IoT створює серйозну проблему сумісності. В одній системі можуть працювати пристрої з різними радіочастотними характеристиками, протоколами транспортного та прикладного рівнів. Технічні вимоги передбачають використання стандартизованих інтерфейсів прикладного програмування (API) та протоколів трансляції.

Інтероперабельність досягається за рахунок впровадження універсальних шлюзів (Gateways), які виконують функцію трансляторів між різними протоколами (наприклад, переклад пакетів з формату ZigBee у стандартні TCP/IP пакети для передачі по Ethernet). Останнім часом індустрія рухається до стандартизації через протоколи прикладного рівня, такі як Matter, що базується на IPv6 та дозволяє пристроям різних брендів безшовно спілкуватися в єдиній локальній мережі. [13]

1.4 Основні компоненти IoT-систем у житлових об'єктах

Апаратна реалізація смарт-будинку складається з множини гетерогенних пристроїв, які за своїм функціональним призначенням у загальній архітектурі обробки інформації поділяються на три основні категорії: сенсори (первинні перетворювачі), виконавчі пристрої (актуатори) та мережево-контролерне обладнання.

Сенсори (Датчики)

Сенсори є ключовою ланкою рівня сприйняття. Їхня головна функція — перетворення фізичних величин навколишнього середовища в електричний сигнал із подальшою його цифровізацією за допомогою аналогово-цифрових перетворювачів (АЦП). Залежно від призначення в житлових об'єктах використовуються такі класи сенсорів:

- Кліматичні: Датчики температури (термістори, напівпровідникові сенсори), гігрометри (вимірювання відносної вологості), датчики якості повітря (вимірювання концентрації летких органічних сполук та CO₂ за допомогою інфрачервоних недисперсійних сенсорів NDIR).
- Оптичні та акустичні: Датчики освітленості (фоторезистори або фотодіоди для визначення рівня люксів), мікрофони для розпізнавання голосових команд або детекції специфічних шумів (наприклад, розбиття скла).
- Просторові та охоронні: Пасивні інфрачервоні детектори руху (PIR), мікрохвильові радары присутності, магнітоконтатні геркони для контролю стану вікон та дверей, датчики протікання води (працюють за принципом замикання контактів через електропровідність рідини).

Більшість сучасних IoT-сенсорів є інтелектуальними: вони містять вбудовані мікроконтролери для первинної фільтрації шумів (наприклад, відсіювання руху домашніх тварин у PIR-датчиках) та бездротові модулі з ультранизьким енергоспоживанням, що дозволяє їм працювати від однієї батарейки протягом декількох років.

Виконавчі пристрої (Актuatorи)

Актuatorи знаходяться на протилежному кінці інформаційного ланцюга. Їхня мета — конвертація цифрових керуючих команд, отриманих від контролера, у фізичні дії або зміну стану середовища. Серед основних виконавчих механізмів виділяють:

- Релейні модулі та контактори: Використовуються для замикання або розмикання електричних кіл великої потужності (керування розетками, бойлерами, насосами). Для плавного регулювання (наприклад, димування світла або швидкості вентиляторів) застосовуються симісторні регулятори або ШІМ-контролери (широтно-імпульсна модуляція).
- Електромеханічні приводи: Сервоприводи та крокові двигуни, що встановлюються на кульові крани систем водо- та газопостачання,

моторизовані карнизи для штор, приводи вентиляційних заслінок та механізми розумних дверних замків.

- Кліматичне обладнання: Інфрачервоні трансмітери, які імітують сигнали пультів дистанційного керування для класичних кондиціонерів, а також інтегровані термостатичні головки для радіаторів опалення.

Контролери та мережеве обладнання

Це ядро та транспортна кровоносна система розумного будинку, що забезпечує логічний зв'язок між сенсорами та актуаторами.

- Центральні хаби (Шлюзи): Виступають координаторами мережі. Вони зазвичай оснащені кількома радіомодулями (Wi-Fi, ZigBee, Z-Wave, Bluetooth) та потужним мікропроцесором. Хаб здійснює трансляцію протоколів, акумулює дані, виконує скрипти автоматизації та підтримує зашифроване з'єднання з хмарними серверами та мобільними додатками користувача.

- Мікроконтролерні плати (Edge nodes): Для кастомних проєктів (зокрема, в рамках академічних досліджень) широко використовуються універсальні платформи з вбудованою підтримкою мережевих стеків, такі як сімейство мікроконтролерів ESP32 (з вбудованим Wi-Fi та BLE) або одноплатні комп'ютери класу Raspberry Pi, які здатні розгортати повноцінні локальні сервери управління (наприклад, Node-RED або Home Assistant).

- Мережеві ретранслятори (Routers): У комірчастих мережах будь-який пристрій із постійним живленням від електромережі (наприклад, розетка або настінний вимикач) автоматично виконує роль маршрутизатора. Він приймає пакети від віддалених датчиків, посилює сигнал та передає його далі до центрального хабу, формуючи надійну, самоорганізовану мережеву топологію, стійку до перешкод.

1.5 Висновки до розділу 1

У першому розділі дипломної роботи було здійснено комплексний теоретико-методологічний аналіз концепції Інтернету речей (IoT) в контексті її застосування для реалізації систем «Розумний будинок». На основі опрацьованого матеріалу можна зробити наступні ключові висновки:

- Еволюція та сутність технології: Технологія Інтернету речей пройшла тривалий еволюційний шлях від ізольованих систем промислової телеметрії до глобальної інфраструктури, яка забезпечує перехід до моделі міжмашинної взаємодії (M2M). Концепція «Розумного будинку» сьогодні є складною кіберфізичною екосистемою, що інтегрує сенсори, актуатори та мережі передачі даних для проактивної автоматизації рутинних процесів і предиктивного управління ресурсами. Завдяки розвитку нейронних мереж та алгоритмів машинного навчання, сучасні системи здатні досягати найвищих рівнів автоматизації, самостійно аналізуючи поведінкові патерни користувачів.
- Архітектурна організація: Для забезпечення інтероперабельності, масштабованості та надійності систем доцільно використовувати багаторівневу еталонну архітектуру, що охоплює фізичний, мережевий, проміжний (граничних обчислень) та прикладний рівні. Аналіз архітектурних рішень засвідчив, що найперспективнішим напрямком є використання децентралізованих та гібридних моделей. Делегування обчислювальних потужностей на периферію (Edge Computing) та використання самовідновлюваних комірчастих (mesh) мереж дозволяє мінімізувати мережеві затримки та уникнути проблеми єдиної точки відмови.
- Апаратна база: Фізична реалізація смарт-будинку складається з множини гетерогенних пристроїв, які формують замкнений цикл інформаційної обробки: від збору метрик довкілля сенсорами та маршрутизації пакетів даних центральними хабами до виконання фізичних дій актуаторами. Важливою вимогою інженерного проєктування є використання інтелектуальних датчиків

із вбудованими мікроконтролерами та бездротовими модулями ультранизького енергоспоживання.

- **Безпека та сумісність:** Встановлено, що основними бар'єрами на шляху масового впровадження IoT-систем залишаються проблеми кібербезпеки та інтероперабельності через фрагментацію стандартів. Розгортання надійних телекомунікаційних інфраструктур вимагає обов'язкової криптографічної перевірки, шифрування трафіку, сегментації локальних мереж, а також впровадження універсальних шлюзів або єдиних протоколів прикладного рівня для безшовної комунікації пристроїв.

Отримані знання щодо багаторівневої архітектури, специфіки маршрутизації у бездротових мережах та взаємодії мікроконтролерного обладнання формують міцне теоретико-технічне підґрунтя. Це дозволяє аргументовано перейти до другого розділу дослідження, де буде здійснено проєктування та розробку практичної моделі системи «Розумного будинку».

2 ОСОБЛИВОСТІ ПОБУДОВИ ТА УПРАВЛІННЯ СИСТЕМАМИ «РОЗУМНОГО БУДИНКУ» НА ОСНОВІ ІОТ

2.1 Організація внутрішніх мереж у житлових приміщеннях

Структура мереж

Організація внутрішніх мереж у сучасному розумному будинку є одним із ключових етапів побудови ефективної системи автоматизації на основі технологій Інтернету речей. Саме внутрішня мережа забезпечує взаємодію між усіма елементами системи, включаючи датчики, контролери, виконавчі пристрої та користувацькі інтерфейси. Від правильного проєктування мережевої інфраструктури залежить стабільність роботи обладнання, швидкість обміну інформацією, рівень безпеки та можливість подальшого масштабування системи.

У більшості випадків структура мережі розумного будинку складається з центрального контролера, сенсорів, виконавчих пристроїв і каналів зв'язку між ними. Центральний контролер виконує роль головного вузла системи та координує роботу всіх компонентів. Як правило, у сучасних рішеннях для цього використовуються сервери Home Assistant, OpenHAB або інші програмні комплекси, встановлені на мінікомп'ютерах Raspberry Pi чи окремих серверах. [9]

Сенсори призначені для збору інформації про стан навколишнього середовища. До них належать датчики температури, вологості, освітлення, руху, диму, відкриття дверей та інші пристрої. Отримані дані передаються до центрального контролера, де відбувається їх обробка та аналіз. На основі цих даних система формує відповідні команди для виконавчих пристроїв.

Виконавчі пристрої забезпечують реалізацію автоматизованих сценаріїв роботи. До них належать реле освітлення, розумні розетки, електроприводи штор, системи клімат-контролю, електронні замки та інші елементи.

Центральний контролер надсилає керуючі сигнали до цих пристроїв відповідно до встановлених алгоритмів автоматизації. [14]

Важливу роль у структурі мережі відіграють шлюзи та маршрутизатори, які забезпечують взаємодію між різними протоколами зв'язку та доступ до мережі Інтернет. Наприклад, шлюз ZigBee дозволяє інтегрувати бездротові датчики та сенсори до локальної мережі Wi-Fi, забезпечуючи централізоване керування всією системою.

Однією з найпоширеніших топологій мережі є зіркоподібна структура, у якій усі пристрої підключаються до центрального вузла. Основними перевагами такого підходу є простота налаштування, адміністрування та контролю роботи системи. Водночас відмова центрального вузла може призвести до часткової або повної втрати функціональності мережі. [8]

Альтернативним рішенням є використання mesh-мереж, які широко застосовуються у технологіях ZigBee та Z-Wave. У таких мережах кожен вузол може виконувати функції ретранслятора сигналу, передаючи дані між іншими пристроями. Це дозволяє підвищити надійність мережі, збільшити радіус покриття та забезпечити стабільну роботу навіть у разі виходу з ладу окремих вузлів.

Під час проектування внутрішньої мережі необхідно враховувати площу приміщення, кількість підключених пристроїв, рівень електромагнітних перешкод та перспективи подальшого розширення системи. У багатоповерхових будинках додатковою проблемою може бути погіршення якості сигналу через бетонні перекриття та стіни, тому доцільно використовувати декілька точок доступу або mesh-системи.

Для підвищення рівня кібербезпеки внутрішню мережу розумного будинку рекомендується сегментувати, виділяючи окремий мережевий сегмент для IoT-пристроїв. Такий підхід дозволяє ізолювати сенсори та виконавчі механізми від персональних комп'ютерів і мобільних пристроїв користувачів, що зменшує ризик несанкціонованого доступу до мережі.

Важливим аспектом функціонування мережі є енергоефективність підключених пристроїв. Для автономних сенсорів зазвичай використовуються протоколи зв'язку з низьким енергоспоживанням, що дозволяє забезпечити їхню роботу від батарей протягом кількох років без необхідності заміни елементів живлення.

Таким чином, структура внутрішньої мережі розумного будинку повинна забезпечувати надійний обмін даними між усіма компонентами системи, підтримувати можливість масштабування, відповідати вимогам інформаційної безпеки та гарантувати стабільну роботу пристроїв упродовж тривалого часу.



Рисунок 2.1 – Структурасистеми «розумного будинку»

Типи з'єднань

Типи з'єднань, які використовуються у системах розумного будинку, безпосередньо впливають на ефективність функціонування всієї IoT-інфраструктури. Саме спосіб передавання даних визначає швидкість реакції системи, стабільність роботи обладнання, рівень енергоспоживання та складність встановлення. При проєктуванні розумного будинку необхідно враховувати особливості приміщення, кількість пристроїв, потребу у масштабуванні та фінансові можливості користувача.

У сучасних системах автоматизації використовуються як дротові, так і бездротові типи з'єднань. У багатьох випадках найбільш ефективним рішенням є комбінований підхід, при якому основні вузли працюють через кабельне підключення, а сенсори та мобільні пристрої використовують бездротові канали зв'язку.

Дротові з'єднання забезпечують високу надійність та стабільність передачі даних. Для цього використовуються Ethernet-мережі, кабелі витії пари та інші типи фізичних каналів. Перевагою дротових систем є низький рівень затримок та висока швидкість передачі інформації. Крім того, дротові мережі менш схильні до впливу електромагнітних перешкод.

Проте монтаж дротових мереж потребує значних витрат часу та коштів, особливо у вже побудованих приміщеннях. Саме тому у сучасних системах автоматизації частіше застосовуються бездротові технології.

Бездротові з'єднання забезпечують гнучкість та простоту встановлення. Пристрої можуть взаємодіяти між собою за допомогою Wi-Fi, Bluetooth, ZigBee або Z-Wave. Такі технології дозволяють швидко масштабувати систему та додавати нові елементи без прокладання кабелів.

Wi-Fi використовується для підключення камер відеоспостереження, мультимедійних систем та пристроїв, які потребують високої швидкості передачі даних. Основним недоліком Wi-Fi є високе енергоспоживання та можливі перевантаження мережі при великій кількості підключених пристроїв.

Bluetooth застосовується переважно для короткодистанційного зв'язку між мобільними пристроями та елементами автоматизації. Його перевагою є низьке енергоспоживання та простота налаштування.

ZigBee є одним із найпопулярніших протоколів для IoT-систем. Він підтримує mesh-топологію та забезпечує низьке споживання енергії. Завдяки цьому ZigBee широко використовується у датчиках та сенсорах.

Технологія Z-Wave також орієнтована на системи автоматизації будинку. Вона забезпечує стабільний зв'язок та високу сумісність між пристроями різних

виробників. Основною перевагою Z-Wave є робота у менш завантаженому діапазоні частот.

У сучасних системах часто використовуються гібридні рішення, де одночасно поєднуються дротові та бездротові канали зв'язку. Наприклад, центральний сервер може бути підключений через Ethernet, а сенсори працювати через ZigBee.

Таким чином, вибір типу з'єднання залежить від вимог до швидкості передачі даних, надійності, енергоспоживання та вартості реалізації системи.

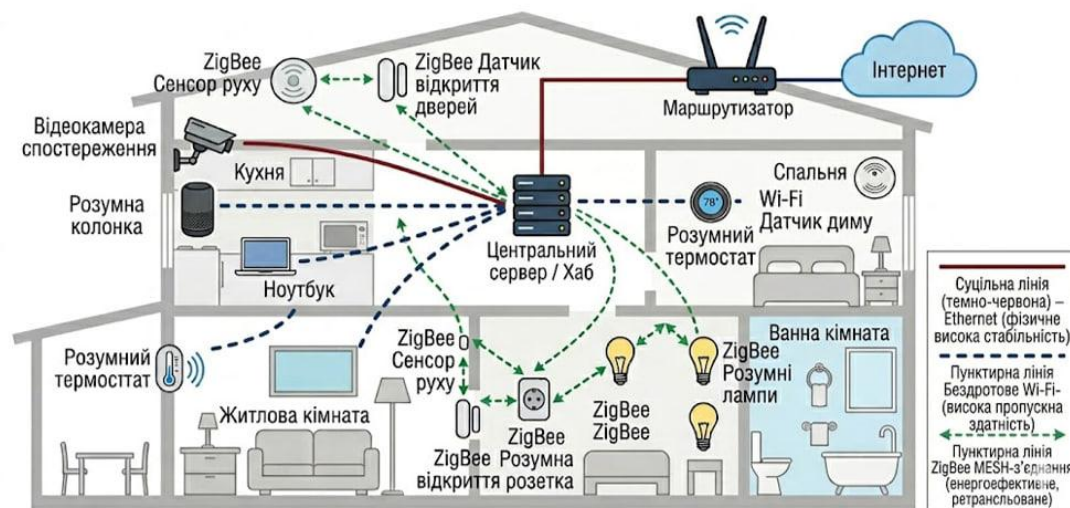


Рисунок 2.2 – Приклад використання дротових та бездротових з'єднань у системі розумного будинку

2.2 Технології та протоколи передачі даних Wi-Fi, ZigBee, Z-Wave, Bluetooth

Технології передачі даних є ключовим компонентом будь-якої системи Інтернету речей. Саме завдяки сучасним бездротовим протоколам забезпечується взаємодія між сенсорами, контролерами, виконавчими механізмами та користувацькими пристроями. У системах розумного будинку використовуються різні технології зв'язку, кожна з яких має власні технічні характеристики, переваги та обмеження.

Правильний вибір протоколу передачі даних дозволяє забезпечити стабільну роботу системи, знизити енергоспоживання, підвищити рівень безпеки та оптимізувати витрати на впровадження IoT-рішень. Найбільш поширеними технологіями у сучасних системах автоматизації є Wi-Fi, ZigBee, Bluetooth та Z-Wave.

Передача даних є основою функціонування систем Інтернету речей. Саме завдяки сучасним бездротовим технологіям забезпечується взаємодія між датчиками, контролерами та виконавчими пристроями.

Wi-Fi є однією з найпоширеніших технологій бездротового зв'язку. Вона забезпечує високу швидкість передачі даних та підтримує пряме підключення до мережі Інтернет. Технологія Wi-Fi працює у діапазонах 2,4 ГГц та 5 ГГц і використовується у більшості сучасних маршрутизаторів.

Основною перевагою Wi-Fi є висока пропускна здатність, що дозволяє передавати великі обсяги інформації. Саме тому Wi-Fi активно застосовується у системах відеоспостереження, мультимедіа та віддаленого керування.

Недоліком Wi-Fi є значне енергоспоживання. Для автономних датчиків така технологія не завжди є ефективною, оскільки батарея швидко розряджається. Крім того, при великій кількості підключених пристроїв можуть виникати перевантаження мережі.

Технологія ZigBee була створена спеціально для IoT-систем та автоматизації. Вона характеризується низьким споживанням енергії та підтримкою mesh-мереж. ZigBee працює у діапазоні 2,4 ГГц та дозволяє об'єднувати велику кількість пристроїв у єдину систему.

Однією з головних переваг ZigBee є можливість передачі сигналу через інші вузли мережі. Це дозволяє збільшити зону покриття та підвищити надійність роботи системи.

Bluetooth також широко використовується у системах розумного будинку. Сучасна версія Bluetooth Low Energy забезпечує низьке енергоспоживання та стабільний зв'язок на невеликих відстанях. Bluetooth застосовується у розумних замках, системах контролю доступу та мобільних додатках.

Технологія Z-Wave орієнтована виключно на автоматизацію житлових приміщень. Вона працює на частотах нижче 1 ГГц, що зменшує вплив перешкод та забезпечує стабільніший сигнал. Z-Wave підтримує mesh-архітектуру та дозволяє підключати сотні пристроїв.

Важливою перевагою Z-Wave є висока сумісність між обладнанням різних виробників. Завдяки сертифікації пристроїв користувачі можуть створювати єдину систему із компонентів різних брендів.

У сучасних системах автоматизації часто одночасно використовуються декілька технологій. Наприклад, Wi-Fi може застосовуватися для камер відеоспостереження, ZigBee — для датчиків, а Bluetooth — для локального керування.



Рисунок 2.3 – Технології передачі даних у системах IoT

Порівняння характеристик

Порівняння характеристик бездротових технологій дозволяє визначити найбільш доцільні рішення для побудови систем розумного будинку залежно від конкретних умов експлуатації. Кожен протокол має свої особливості, тому універсального рішення для всіх типів пристроїв не існує.

При аналізі технологій передачі даних необхідно враховувати такі параметри, як швидкість передачі інформації, дальність зв'язку, рівень

енергоспоживання, складність інтеграції, підтримка mesh-мереж та сумісність із обладнанням інших виробників.

Порівняння технологій передачі даних дозволяє визначити найбільш ефективні рішення для систем розумного будинку.

Wi-Fi забезпечує найбільшу швидкість передачі даних серед розглянутих технологій. Проте його енергоспоживання значно вище, ніж у ZigBee або Bluetooth. Це обмежує використання Wi-Fi у автономних сенсорах.

ZigBee має низьке енергоспоживання та підтримує mesh-топологію. Завдяки цьому пристрої можуть працювати від батарейок протягом кількох років. Швидкість передачі даних у ZigBee нижча, ніж у Wi-Fi, проте її достатньо для більшості IoT-застосувань.

Bluetooth характеризується простотою підключення та невеликим енергоспоживанням. Однак дальність дії Bluetooth зазвичай менша, ніж у ZigBee чи Wi-Fi.

Z-Wave забезпечує стабільний зв'язок та високу сумісність між пристроями. Завдяки роботі у менш завантаженому частотному діапазоні Z-Wave менш схильний до перешкод.

При виборі технології необхідно враховувати тип пристроїв, площу приміщення, вимоги до швидкості передачі даних та автономності роботи.

Таблиця 2.1 – Порівняльна характеристика технологій та протоколів передачі даних

Характеристика	Wi-Fi (IEEE 802.11b/g/n)	ZigBee (IEEE 802.15.4)	Bluetooth (BLE)	Z-Wave
Швидкість передачі даних	Висока (до 600 Мбіт/с і вище)	Низька (до 250 Кбіт/с)	Середня (до 2 Мбіт/с для BLE)	Дуже низька (до 100 Кбіт/с)
Радіус дії (в приміщенні)	~30–50 м	~10–100 м	~10–50 м	~30 м

Продовження таблиці 2.1

Енергоспоживання	Високе	Дуже низьке	Низьке	Дуже низьке
Тип топології мережі	«Зірка»	«Комірчаста» (Mesh), «Дерево», «Зірка»	«Зірка», «Комірчаста» (в нових версіях)	«Комірчаста» (Mesh)
Робоча частота	2.4 ГГц, 5 ГГц	2.4 ГГц (глобально)	2.4 ГГц	< 1 ГГц (868.4 МГц в Україні)

2.3 Автоматизація процесів у розумному будинку

Керування освітленням

Автоматизація освітлення є одним із найбільш популярних напрямків застосування технологій Інтернету речей у системах розумного будинку. Використання інтелектуального керування освітленням дозволяє не лише підвищити комфорт користувачів, але й значно зменшити витрати електроенергії. Саме тому системи автоматичного освітлення активно впроваджуються як у приватних будинках, так і у квартирах.

Сучасні системи освітлення можуть працювати за заздалегідь встановленими сценаріями або реагувати на зміни навколишнього середовища в режимі реального часу. Для цього використовуються датчики руху, освітленості, присутності та таймери.

Автоматизація освітлення є одним із найбільш поширених напрямків застосування технологій IoT у розумному будинку. Основною метою таких систем є підвищення комфорту користувачів та зменшення енергоспоживання.

Для автоматичного керування освітленням використовуються датчики руху, освітленості та присутності. Наприклад, при виявленні руху у приміщенні система автоматично вмикає світло. Після виходу людини освітлення вимикається через заданий проміжок часу.

Сучасні системи дозволяють створювати складні сценарії роботи. Наприклад, у вечірній час освітлення може автоматично переходити у режим зниженої яскравості. Також можливе дистанційне керування через мобільний додаток.

Застосування LED-освітлення та розумних реле дозволяє значно знизити споживання електроенергії. Крім того, користувачі можуть налаштовувати колір та інтенсивність освітлення відповідно до власних потреб.

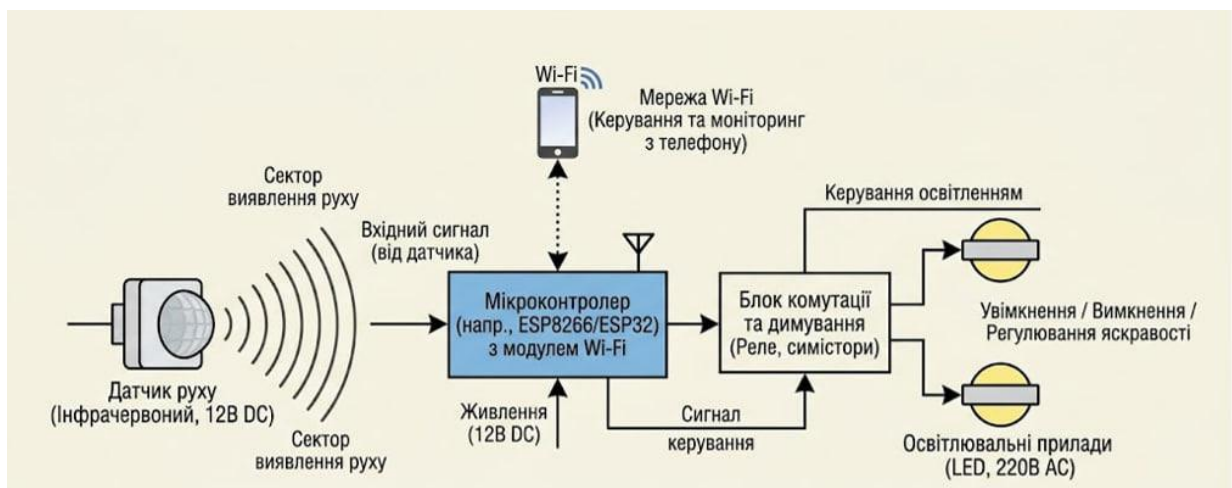


Рисунок 2.4 – Система автоматизованого керування освітленням

Клімат-контроль

Однією з найважливіших функцій розумного будинку є автоматичне підтримання комфортних кліматичних умов у приміщенні. Системи клімат-контролю на основі IoT забезпечують автоматизацію процесів опалення, вентиляції та кондиціонування повітря.

Головною перевагою таких систем є можливість постійного моніторингу температури, вологості та якості повітря у приміщенні. Завдяки використанню

датчиків та інтелектуальних алгоритмів система може автоматично реагувати на зміни мікроклімату.

Системи клімат-контролю забезпечують автоматичне підтримання комфортної температури та вологості у приміщенні. Для цього використовуються датчики температури, вологості, кондиціонери, обігрівачі та вентиляційні системи.

Центральний контролер аналізує показники датчиків та автоматично вмикає або вимикає відповідні пристрої. Наприклад, при зниженні температури нижче заданого рівня система активує опалення.

Сучасні IoT-системи дозволяють створювати адаптивні алгоритми керування. Наприклад, температура у будинку може автоматично знижуватися під час відсутності мешканців та підвищуватися перед їх поверненням.

Такі рішення дозволяють не лише підвищити комфорт, але й зменшити витрати на опалення та кондиціювання.

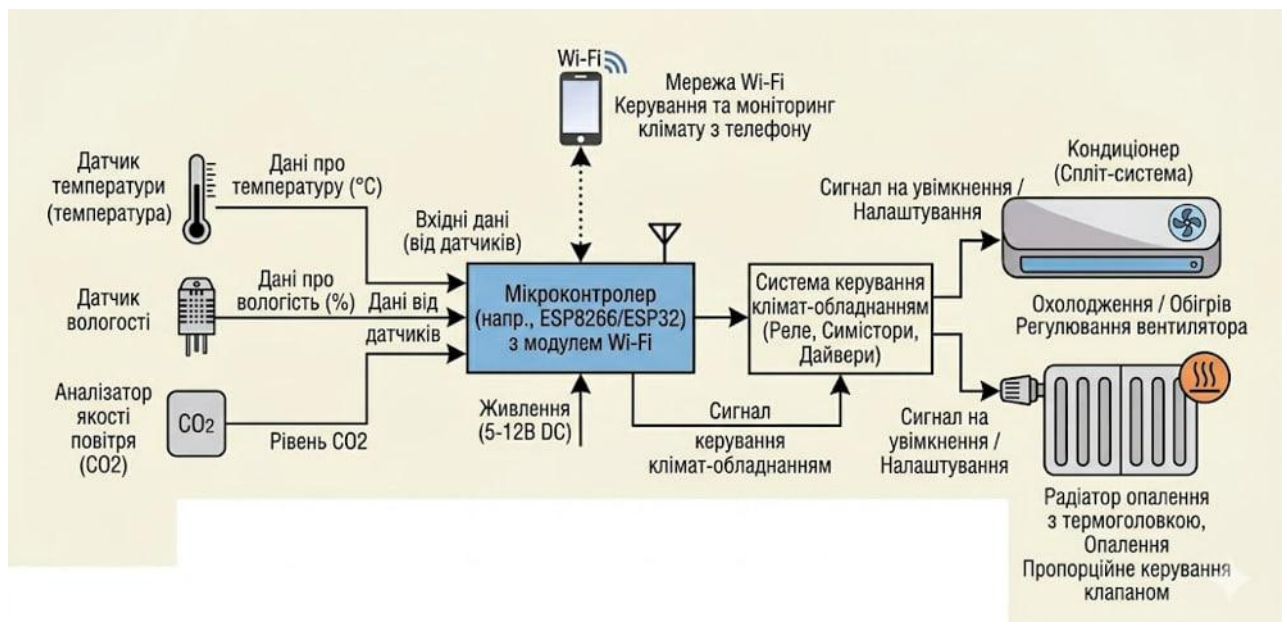


Рисунок 2.5 – Система клімат контролю у розумному будинку

Системи безпеки

Системи безпеки є невід’ємною складовою концепції розумного будинку. Використання IoT-технологій дозволяє створювати багаторівневі системи захисту, які забезпечують контроль доступу, відеоспостереження, пожежну безпеку та захист від аварійних ситуацій.

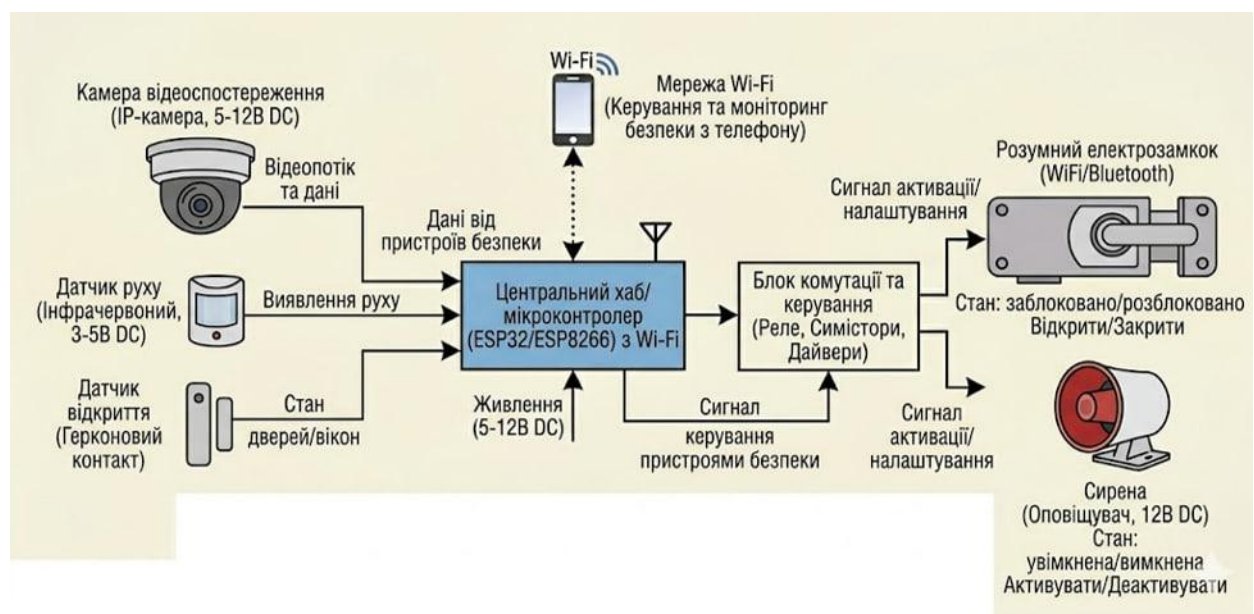
Основною перевагою сучасних систем безпеки є можливість цілодобового моніторингу стану житла та оперативного інформування власника про потенційні загрози.

Безпека є одним із найважливіших компонентів розумного будинку. IoT-технології дозволяють створювати комплексні системи захисту житла.

До складу систем безпеки входять камери відеоспостереження, датчики руху, датчики відкриття дверей та вікон, датчики диму та витoku газу.

При виявленні небезпечної ситуації система автоматично надсилає повідомлення власнику на смартфон. Також можливе автоматичне ввімкнення сирени або виклик охоронної служби.

Сучасні камери відеоспостереження підтримують функції розпізнавання облич та запису відео у хмарне сховище. Це дозволяє забезпечити високий рівень контролю та безпеки.



Рисunek 2.6 – Структура системи безпеки розумного будинку

2.4 Віддалене керування та моніторинг системи

Хмарні сервіси

Розвиток хмарних технологій значно вплинув на функціонування сучасних систем розумного будинку. Хмарні сервіси забезпечують централізоване зберігання інформації, синхронізацію даних та віддалений доступ до IoT-пристроїв.

Завдяки використанню хмарних платформ користувач отримує можливість контролювати систему розумного будинку з будь-якої точки світу, де є доступ до мережі Інтернет. [4]

Хмарні технології відіграють важливу роль у роботі сучасних систем розумного будинку. Завдяки хмарним сервісам користувач може отримати доступ до системи з будь-якої точки світу. [6]

Хмарні платформи забезпечують зберігання даних, синхронізацію налаштувань та дистанційне керування пристроями. Вони також дозволяють реалізовувати аналітичні функції та автоматичне резервне копіювання.

Однією з переваг хмарних сервісів є можливість централізованого оновлення програмного забезпечення. Це дозволяє швидко усувати вразливості та додавати нові функції.

Проте використання хмарних сервісів створює додаткові ризики, пов'язані із конфіденційністю даних та залежністю від доступу до Інтернету.

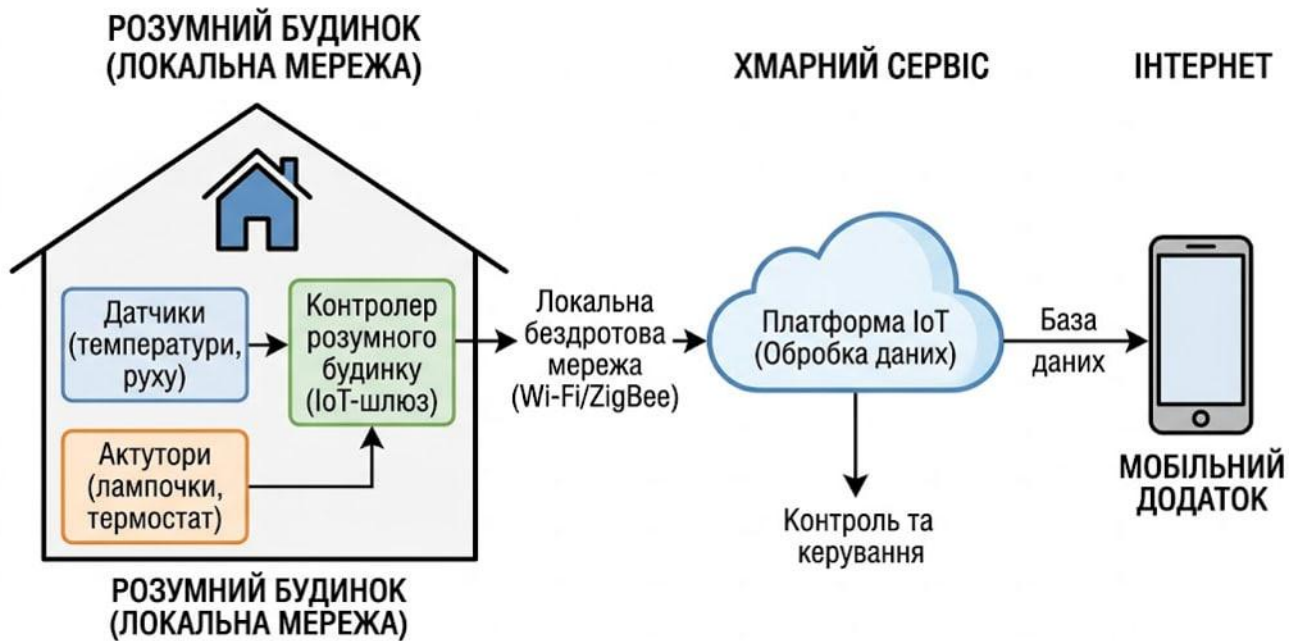


Рисунок 2.7 – Взаємодія хмарного сервісу із системою розумного будинку

Мобільні додатки

Мобільні додатки є одним із головних елементів взаємодії користувача із системою розумного будинку. Саме через смартфон або планшет власник житла може отримувати інформацію про стан системи, змінювати налаштування та керувати пристроями у режимі реального часу.

Сучасні мобільні додатки мають інтуїтивно зрозумілий інтерфейс та підтримують інтеграцію великої кількості IoT-пристроїв. [3]

Мобільні додатки є основним інструментом взаємодії користувача із системою розумного будинку. За допомогою смартфона можна керувати освітленням, клімат-контролем, системами безпеки та іншими пристроями.

Сучасні додатки мають зручний інтерфейс та підтримують створення автоматичних сценаріїв. Наприклад, користувач може налаштувати режим «Відпустка», при якому система автоматично імітує присутність людей у будинку.

Мобільні додатки також дозволяють отримувати сповіщення про події у реальному часі. Це підвищує рівень безпеки та забезпечує оперативне реагування на надзвичайні ситуації.

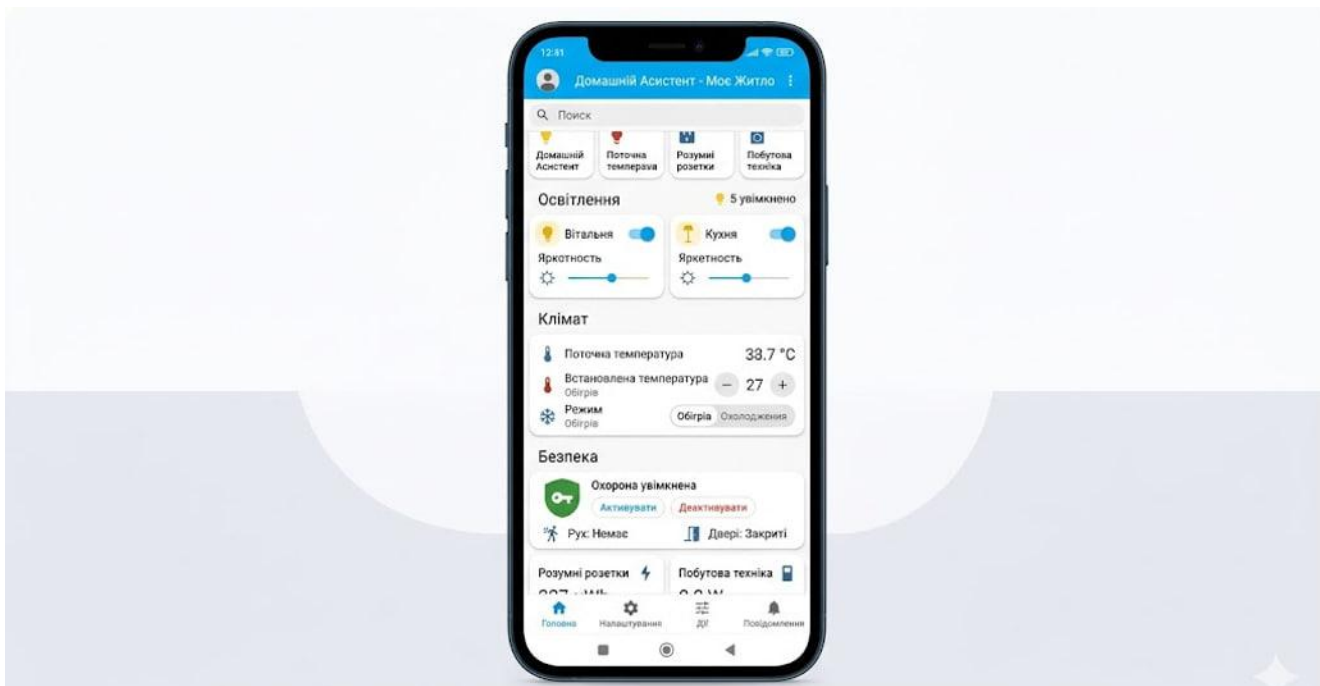


Рисунок 2.8 – Інтерфейс мобільного додатка для керування розумним будинком

Голосові помічники

Інтеграція голосових помічників є одним із найбільш перспективних напрямків розвитку систем розумного будинку. Голосове керування дозволяє зробити взаємодію користувача із системою максимально простою та зручною.

Сучасні голосові помічники здатні розпізнавати природну мову та виконувати складні команди користувача.

Одним із сучасних напрямків розвитку IoT-систем є інтеграція голосових помічників. Найбільш популярними рішеннями є Google Assistant, Amazon Alexa та Apple Siri.

Голосові помічники дозволяють керувати пристроями за допомогою голосових команд. Наприклад, користувач може увімкнути світло, змінити температуру або запустити музичну систему без використання смартфона.

Інтеграція голосових сервісів підвищує зручність користування системою та робить взаємодію більш природною.

Проте використання голосових помічників створює додаткові ризики для конфіденційності, оскільки голосові дані можуть передаватися на віддалені сервери.



Рисунок 2.9 – Використання голосового помічника у системі «розумного будинку»

2.5 Проблеми безпеки та захисту даних

Кіберзагрози

Стрімкий розвиток Інтернету речей призводить не лише до розширення функціональних можливостей розумного будинку, але й до появи нових кіберзагроз. Велика кількість підключених до мережі пристроїв створює додаткові ризики для безпеки інформації та конфіденційності користувачів.

Багато IoT-пристроїв мають обмежені апаратні ресурси, через що виробники не завжди приділяють достатню увагу питанням захисту даних та кібербезпеки. [4]

З розвитком Інтернету речей значно зростає кількість кіберзагроз. Розумний будинок містить велику кількість підключених пристроїв, які можуть стати ціллю для хакерських атак.

Однією з основних проблем є використання слабких паролів та застарілого програмного забезпечення. Зловмисники можуть отримати доступ до системи та перехоплювати дані користувачів.

Особливу небезпеку становлять атаки типу DDoS, при яких велика кількість заражених IoT-пристроїв використовується для перевантаження серверів.

Також можливі атаки на камери відеоспостереження, системи доступу та розумні замки. У разі успішного злому зловмисник може отримати контроль над системою безпеки будинку.

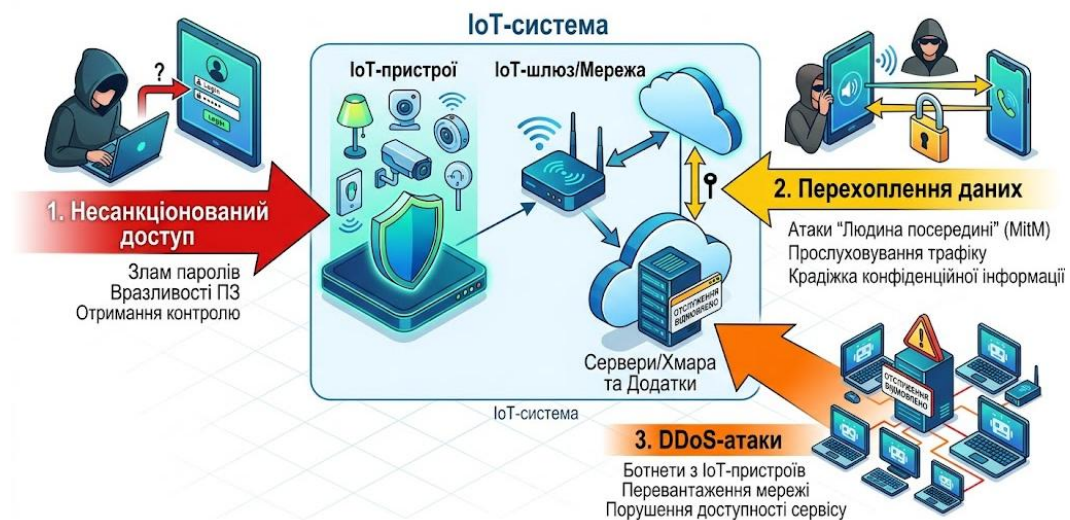


Рисунок 2.10 – Основні кіберзагрози для IoT-систем

Методи захисту

Для забезпечення безпечної роботи систем розумного будинку необхідно використовувати комплекс сучасних методів захисту інформації та мережевої інфраструктури. Захист IoT-систем повинен охоплювати як програмний, так і апаратний рівень.

Одним із найважливіших елементів захисту є правильна автентифікація користувачів та пристроїв. [8]

Для забезпечення безпеки IoT-систем необхідно використовувати комплексний підхід до захисту даних.

Перш за все необхідно застосовувати надійні паролі та двофакторну автентифікацію. Це значно ускладнює несанкціонований доступ до системи.

Важливим елементом захисту є регулярне оновлення програмного забезпечення. Виробники постійно випускають оновлення, які усувають виявлені вразливості.

Для передачі даних необхідно використовувати сучасні алгоритми шифрування. Наприклад, протоколи WPA3 та TLS забезпечують високий рівень захисту інформації. [1]

Також доцільно створювати окрему мережу для IoT-пристроїв. Це дозволяє ізолювати потенційно небезпечні елементи від основної мережі користувача.

Для підвищення рівня безпеки рекомендується використовувати міжмережеві екрани та системи моніторингу мережевого трафіку.

Таким чином, захист IoT-систем є одним із найважливіших аспектів побудови розумного будинку.



Рисунок 2.11 – Методи захисту даних у системі розумного будинку

2.6 Висновки до розділу 2

У другому розділі було розглянуто особливості побудови та управління системами «розумного будинку» на основі технологій Інтернету речей. Встановлено, що ефективність функціонування IoT-систем значною мірою залежить від правильної організації внутрішньої мережі, вибору протоколів передачі даних та рівня автоматизації процесів.

Проаналізовано основні типи мережевих структур та з'єднань, які використовуються у сучасних системах автоматизації житлових приміщень. Визначено, що найбільш перспективними є бездротові mesh-мережі на базі технологій ZigBee та Z-Wave.

Розглянуто характеристики основних протоколів передачі даних, зокрема Wi-Fi, ZigBee, Bluetooth та Z-Wave. Встановлено, що кожна технологія має власні переваги та недоліки залежно від сфери застосування.

Досліджено можливості автоматизації освітлення, клімат-контролю та систем безпеки. Визначено, що використання IoT-технологій дозволяє підвищити рівень комфорту, безпеки та енергоефективності житла.

Також проаналізовано засоби віддаленого керування системами розумного будинку, включаючи хмарні сервіси, мобільні додатки та голосових помічників.

Окрему увагу приділено питанням кібербезпеки та захисту даних. Встановлено, що зі збільшенням кількості IoT-пристроїв зростає потреба у використанні сучасних методів шифрування, сегментації мереж та механізмів автентифікації.

Отже, технології Інтернету речей створюють широкі можливості для реалізації концепції «розумного будинку», забезпечуючи автоматизацію, енергоефективність та підвищення рівня безпеки житлових приміщень.

3 РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ІoT-СИСТЕМИ НА БАЗІ HOME ASSISTANT

3.1 Реалізація та налаштування системи

Встановлення Home Assistant

Одним із найбільш популярних та гнучких програмних рішень для побудови сучасних систем домашньої автоматизації є платформа Home Assistant. Стрімкий розвиток технологій Інтернету речей супроводжується постійним збільшенням кількості гетерогенних пристроїв у житлових приміщеннях. До таких пристроїв належать датчики руху, системи освітлення, кліматичне обладнання, розумні розетки, камери відеоспостереження та інші елементи автоматизації. У зв'язку з цим виникає необхідність використання універсальних програмних платформ, які дозволяють об'єднати ці розрізнені ІoT-пристрої в єдину кіберфізичну систему керування та забезпечити їх стабільну взаємодію між собою.

Платформа Home Assistant забезпечує централізоване керування обладнанням та підтримує велику кількість інтеграцій із пристроями різних виробників. Дана система активно використовується як у побутових умовах, так і у професійних проєктах автоматизації завдяки широким можливостям налаштування, високій стабільності роботи та підтримці сучасних стеків мережевих протоколів передачі даних.

Важливою архітектурною особливістю Home Assistant є орієнтація на локальне керування системою без обов'язкового та постійного використання хмарних сервісів. Це дозволяє мінімізувати мережеві затримки, підвищити рівень конфіденційності особистих даних користувача та забезпечити стабільне функціонування локальних сценаріїв навіть у випадку повної відсутності доступу до глобальної мережі Інтернет. На відміну від більшості закритих комерційних платформ, Home Assistant є програмним забезпеченням із відкритим вихідним кодом (Open Source), що дозволяє гнучко змінювати

конфігурацію системи, створювати власні унікальні сценарії автоматизації та інтегрувати нові типи пристроїв без ліцензійних обмежень.

Home Assistant підтримує роботу на різних апаратних платформах, зокрема на персональних комп'ютерах, серверах, віртуальних машинах та одноплатних комп'ютерах. Для реалізації практичної частини даного дипломного дослідження як центрального контролера (хабу) було обрано одноплатний комп'ютер класу Raspberry Pi. Використання цієї апаратної платформи є найбільш обґрунтованим з інженерної точки зору, оскільки вона забезпечує оптимальний баланс обчислювальної потужності, ультранизького енергоспоживання, безшумності та компактних габаритів, що критично важливо для цілодобово функціонуючого Edge-сервера системи «розумного будинку».

Перед встановленням програмного забезпечення було виконано підготовку мікропроцесорної плати Raspberry Pi, конфігурацію параметрів локальної мережі та підготовку швидкісного накопичувача типу MicroSD (класу Application Performance Class A2) для стабільної роботи бази даних системи. На апаратну платформу було розгорнуто оптимізовану операційну систему Home Assistant OS (HAOS), що дозволило забезпечити максимальну швидкодію та прямий доступ до апаратних інтерфейсів плати.

Після інсталяції та першого запуску операційної системи Home Assistant автоматично ініціалізував локальний веб-сервер керування, доступ до якого в межах домашньої мережі здійснювався через вебінтерфейс за захищеним локальним IP-протоколом. У процесі первинного налаштування було створено захищений обліковий запис адміністратора, виконано базову географічну та часову конфігурацію системи, а також налаштовано внутрішні параметри безпеки та брандмауера для запобігання несанкціонованому доступу.

Для щоденного моніторингу та оперативного віддаленого керування інфраструктурою використовувався офіційний мобільний додаток Home Assistant, встановлений на смартфон користувача. За допомогою мобільного застосунку, підключеного до локального сервера, здійснювався безперервний

контроль пристроїв, перегляд поточних показників сенсорів у реальному часі, фіксація журналів подій та керування автоматичними сценаріями. Такий підхід дозволив забезпечити ергономічний та мобільний інтерфейс взаємодії з системою з будь-якої точки в межах радіусу дії локальної мережі.

Вебінтерфейс Home Assistant (Dashboard) має сучасний, адаптивний та інтуїтивно зрозумілий дизайн. На головній панелі відображаються інтерактивні картки підключених пристроїв, графіки стану сенсорів, системні журнали та перемикачі автоматизацій. Завдяки цьому користувач може миттєво отримувати інформацію про роботу системи та коригувати параметри її функціонування у режимі реального часу.

Однією з ключових переваг Home Assistant у поєднанні з апаратною базою Raspberry Pi є підтримка величезної кількості інтеграцій та протоколів передачі даних, серед яких Wi-Fi, ZigBee, Bluetooth та MQTT. Це дозволяє безшовно підключати гетерогенне обладнання різних виробників у межах єдиного координатора та створювати гнучкі крос-протокольні сценарії автоматизації без прив'язки до екосистеми конкретного бренду. Крім того, система підтримує автоматичне створення локальних резервних копій (snapshots), регулярне оновлення компонентів безпеки та надсилення миттєвих push-сповіщень на мобільний пристрій користувача в разі фіксації критичних подій.

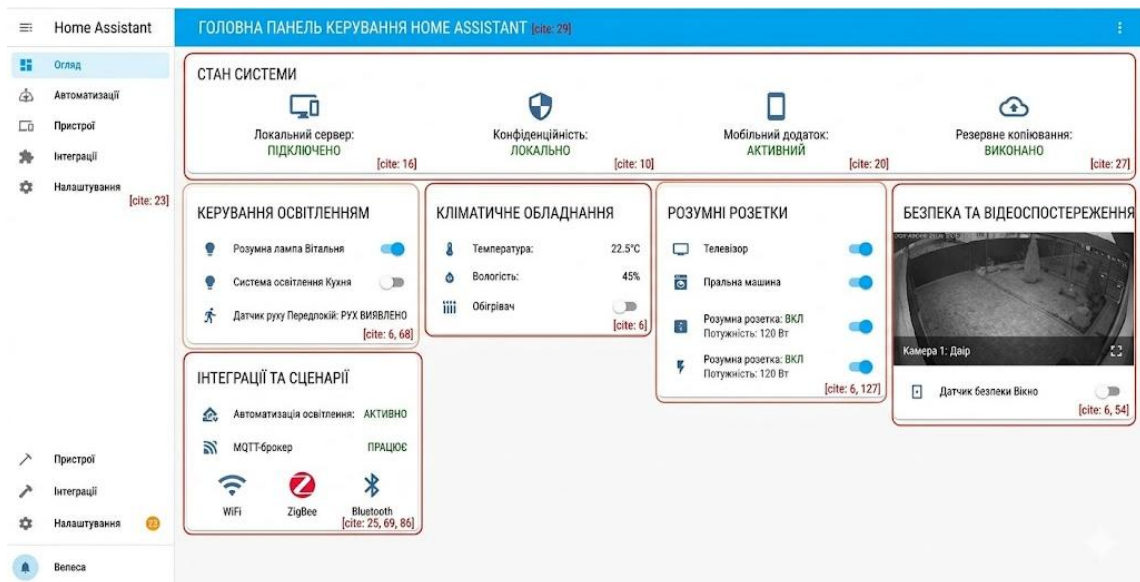


Рисунок 3.1 – Головний інтерфейс системи Home Assistant

Підключення IoT-пристроїв

Після успішного розгортання та початкової конфігурації Home Assistant на базі Raspberry Pi було виконано поетапне підключення та інтеграцію кінцевих IoT-пристроїв до загальної системи автоматизації. [9] Процес інтеграції периферійного обладнання є одним із найвідповідальніших етапів реалізації проєкту, оскільки саме від коректності налаштування фізичного та мережевого рівнів залежить загальна стабільність, швидкодія, завадостійкість та інформаційна безпека всієї розгорнутої мережі.

Для практичної реалізації системи та оцінки її можливостей використовувався наступний набір обладнання: бездротові датчики руху, розумні LED-лампи з можливістю димування, смарт-розетки з функцією моніторингу енергоспоживання, а також виконавчі релейні модулі керування силовими лініями освітлення. Перед початком інтеграційних робіт було проведено попередню перевірку сумісності апаратних ревізій обладнання з програмною платформою Home Assistant та підтримуваними шлюзами.

Підключення та обмін даними з пристроями здійснювалися із використанням двох бездротових технологій: Wi-Fi (IEEE 802.11b/g/n) та ZigBee (IEEE 802.15.4). Технологія Wi-Fi використовувалася для стаціонарних

пристроїв, які потребують вищої пропускної здатності та підключені до постійного джерела живлення. У свою чергу, для автономних сенсорів було розгорнуто мережу стандарту ZigBee через спеціалізований USB-координатор (шлюз), підключений безпосередньо до Raspberry Pi. Протокол ZigBee забезпечує ультранизьке енергоспоживання кінцевих вузлів, високу завадостійкість та підтримує самовідновлювану mesh-топологію мережі, що мінімізує проблему «мертвих зон» у приміщенні.

У процесі інтеграції кожен периферійний пристрій проходив стандартизовану процедуру сполучення (pairing), криптографічної авторизації та автоматичного визначення системою. Завдяки розвиненій підсистемі виявлення, Home Assistant автоматично ідентифікує більшість сучасних IoT-компонентів на мережевому рівні та пропонує готові шаблони конфігурації, що значно прискорює процес розгортання інфраструктури.

Після успішної реєстрації в мережі всі сутності (entities) пристроїв почали транслювати свої телеметричні дані у веб-інтерфейс та мобільний застосунок. Користувач отримав можливість здійснювати пряме директивне керування актуаторами (вмикання/вимикання реле, зміна яскравості ламп), відстежувати динаміку показників фізичних сенсорів та контролювати рівень заряду автономних елементів живлення.

Важливим кроком логічної організації системи стало групування підключених сутностей за територіальним та функціональним призначенням. У програмному середовищі було створено ізольовані зони (кімнати) та функціональні групи: підсистему освітлення, контур безпеки та моніторингу клімату. Таке логічне структурування суттєво спростило адміністрування системи, полегшило візуальне сприйняття інтерфейсу користувачем та дозволило перейти до побудови крос-компонентних автоматичних сценаріїв роботи. Крім того, центральний контролер на Raspberry Pi здійснює безперервний моніторинг доступності пристроїв у мережі (ping) і в разі втрати зв'язку з будь-яким вузлом або виникнення внутрішньої помилки негайно генерує сповіщення для користувача.

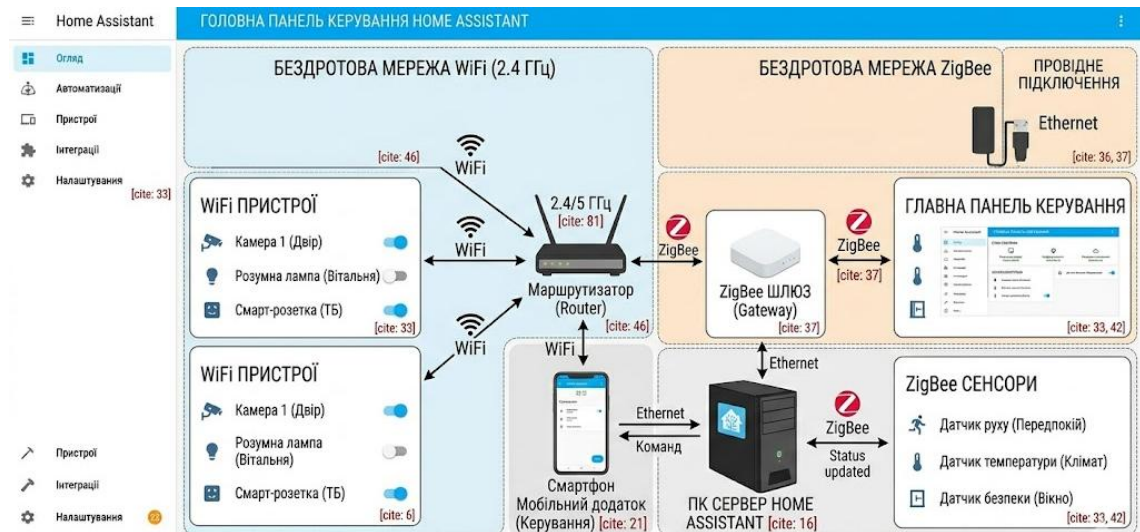


Рисунок 3.2 – Підключення IoT-пристроїв до системи Home Assistant

Налаштування автоматизацій

Головною практичною перевагою та метою розгортання платформи Home Assistant на базі Raspberry Pi є можливість створення та виконання гнучких автоматичних сценаріїв роботи інфраструктури. Автоматизація процесів на основі логічних тригерів становить базову концепцію функціонування сучасного «розумного будинку», оскільки дозволяє кіберфізичній системі автономно приймати рішення та реагувати на зміну стану фізичного середовища без необхідності постійного ручного втручання з боку людини.

Впровадження алгоритмів автоматизації дозволяє підняти рівень комфорту проживання на новий якісний рівень, а також суттєво оптимізувати споживання електричної та теплової енергії в автоматизованих зонах. Аналізуючи інформацію, що надходить від масиву сенсорів, контролер виконує чітко задану послідовність дій над виконавчими механізмами (актуаторами) відповідно до закладеної логічної структури.

У межах даного проєкту було розроблено та протестовано кілька типів сценаріїв автоматизації. Зокрема, було реалізовано алгоритм адаптивного керування освітленням: при фіксації руху в прохідній зоні інфрачервоним датчиком система автоматично замикає контур реле та вмикає світло, а після

припинення фіксації активності та закінчення встановленого таймауту — автономно знеструмлює лінію.

Окрему увагу було приділено підсистемі безпеки, де налаштовано сценарій превентивного інформування. При спрацюванні охоронних датчиків (руху або відкриття) у режимі «Охорона», центральний хаб миттєво формує та надсилає тривожне push-повідомлення на смартфон користувача через зашифрований канал зв'язку, що дає змогу оперативно реагувати на потенційні загрози чи аварійні ситуації.

Окрім лінійних однофакторних алгоритмів, архітектура Home Assistant дозволила реалізувати складні багатокomпонентні сценарії, що базуються на перевірці кількох умов (conditions) одночасно. Наприклад, увімкнення штучного освітлення при фіксації руху блокується, якщо рівень природної освітленості в кімнаті за даними фоторезистора є вищим за встановлений поріг (люкс), або якщо астрономічний час не відповідає нічному періоду.

Проектування та конфігурація автоматизацій у середовищі Home Assistant виконувалися комбінованим способом: за допомогою вбудованого графічного візуалізатора лінійних зв'язків, а також шляхом безпосереднього написання програмного коду мовою розмітки YAML (Yet Another Markup Language) у конфігураційних файлах системи. Використання коду YAML відкриває розширені інженерні можливості для опису складних логічних операторів (AND, OR, NOT), інтеграції шаблонів проектування (Jinja2) та створення динамічних таймерів. Експериментальна експлуатація та тестування підтвердили, що розроблені автоматизації працюють з високою точністю, повністю нівелюють потребу в ручному управлінні базовою інфраструктурою та демонструють високу швидкість обробки логічних стеків на процесорі Raspberry Pi.

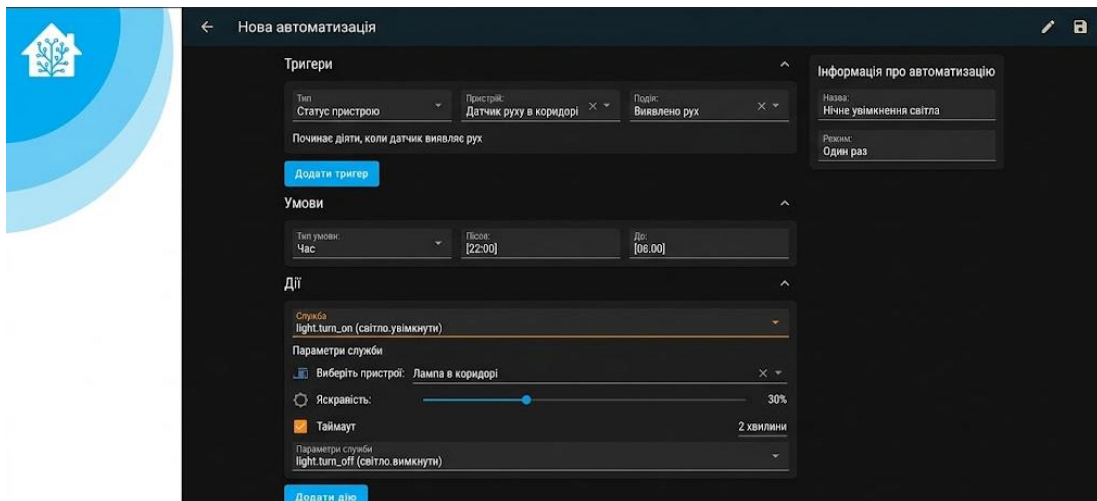


Рисунок 3.3 – Налаштування автоматизацій у Home Assistant

Реалізація системи керування освітленням на основі датчика руху

Одним із найбільш наочних та затребуваних практичних прикладів інтеграції розробленої IoT-інфраструктури є підсистема автоматичного керування локальним освітленням на основі бездротового датчика руху. Такі системи є невід'ємною частиною сучасних енергоефективних житлових та офісних просторів, а їх впровадження спрямоване на усунення нецільового використання енергоресурсів (наприклад, через забуте увімкнене світло) та підвищення загальної ергономіки приміщення.

Головне завдання реалізованого субмодуля полягає у забезпеченні замкненого автоматичного циклу: миттєве запалювання освітлювального приладу при вході людини в зону детекції та його гарантоване вимкнення після того, як людина залишає приміщення.

Для фізичної реалізації цього контуру було задіяно три ключові компоненти: бездротовий пасивний інфрачервоний (PIR) датчик руху, що працює за протоколом ZigBee, інтелектуальна LED-лампа (або розумне реле в розриві фази лінії живлення) та бездротовий одноплатний комп'ютер Raspberry Pi із розгорнутим сервером Home Assistant як центральним координатором. Кінцевий сенсор безперервно сканує температурне тло в приміщенні і при виявленні динамічних змін інфрачервоного випромінювання генерує цифровий

сигнал тривоги, який радіоканалом миттєво транслюється на ZigBee-координатор хабу, після чого Home Assistant запускає відповідний програмний скрипт автоматизації.

При отриманні пакета даних зі статусом «Рух виявлено», серверна логіка формує керуючу команду стандарту MQTT або ZigBee і надсилає її на виконавче реле розумної лампи, здійснюючи комутацію силової мережі 220 В. Паралельно запускається таймер зворотного відліку (наприклад, 120 секунд); кожна наступна фіксація активності датчиком скидає цей таймер у початковий стан. Якщо протягом заданого інтервалу нових сигналів про рух від сенсора не надходить, система інтерпретує це як відсутність людей у кімнаті та надсилає команду на розмикання контактів актуатора, повністю гасячи світло.

Моніторинг працездатності, коригування чутливості PIR-сенсора та зміна тривалості затримки таймауту вимкнення здійснювалися дистанційно через мобільний додаток на смартфоні, що забезпечило високу гнучкість налаштування «на льоту». Створена підсистема автоматичного освітлення на базі Home Assistant та Raspberry Pi на практиці довела високу ефективність та надійність M2M-взаємодії, продемонструвавши значний потенціал енергозбереження та стабільність роботи бездротових каналів зв'язку в умовах побутових радіоперешкод.



Рисунок 3.4 – Схема автоматичного керування освітленням

3.2 Аналіз взаємодії компонентів системи

Передача даних між пристроями

У системах Інтернету речей обмін інформацією між компонентами є основою функціонування всієї мережі. Передача даних забезпечує можливість автоматичного реагування системи на зміни навколишнього середовища та виконання автоматизованих сценаріїв.

У реалізованій системі обмін даними здійснюється між сенсорами, сервером Home Assistant та виконавчими пристроями. Кожен пристрій передає інформацію про власний стан або отримує команди від центрального сервера.

Наприклад, датчик руху передає сигнал про наявність руху, після чого Home Assistant аналізує отримані дані та формує команду для ввімкнення освітлення.

Передача даних здійснюється із використанням локальної мережі та бездротових технологій Wi-Fi і ZigBee. Для забезпечення стабільної роботи системи важливо мінімізувати затримки передачі інформації та підтримувати надійне з'єднання між пристроями.

Однією з важливих характеристик IoT-систем є швидкість передачі даних між компонентами. Від цього параметра залежить швидкість реагування системи на зміни зовнішнього середовища та ефективність роботи автоматизацій.

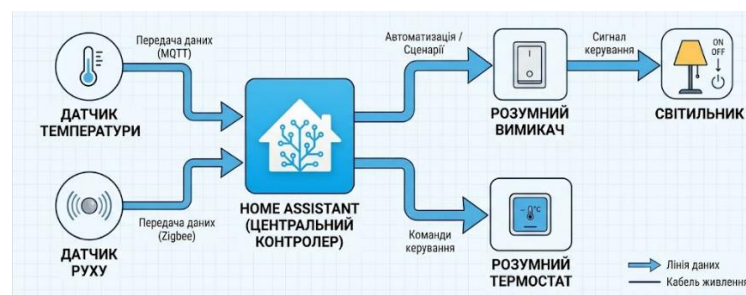


Рисунок 3.5 – Передача даних між компонентами IoT-системи

Робота MQTT-брокера

MQTT є одним із найпоширеніших протоколів обміну повідомленнями у системах Інтернету речей. Даний протокол був спеціально розроблений для роботи у мережах із низькою пропускнуою здатністю та нестабільним з'єднанням. [7]

Головною перевагою MQTT є низьке навантаження на мережу та висока швидкість передачі повідомлень. Саме тому MQTT широко використовується у системах автоматизації та IoT-проектах.

У реалізованій системі MQTT-брокер виконує роль посередника між пристроями та Home Assistant. Сенсори публікують повідомлення у відповідні теми, а сервер підписується на ці теми та отримує необхідну інформацію.

Використання MQTT дозволяє забезпечити швидкий та стабільний обмін повідомленнями навіть при великій кількості підключених пристроїв.

Крім того, MQTT підтримує механізми підтвердження доставки повідомлень, що підвищує надійність системи та мінімізує ймовірність втрати інформації. [12]

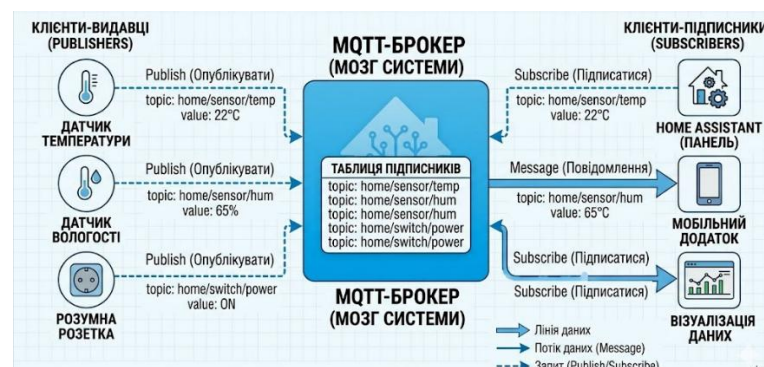


Рисунок 3.6 – Принцип роботи MQTT-брокера

Обмін повідомленнями в системі

У системі «розумного будинку» постійно відбувається обмін великою кількістю повідомлень між різними компонентами. Повідомлення можуть містити інформацію про стан сенсорів, команди керування або службові дані.

Home Assistant аналізує отримані повідомлення та виконує відповідні дії залежно від налаштувань автоматизації.

Наприклад, після спрацювання датчика руху система надсилає повідомлення про подію та формує команду на ввімкнення освітлення. Такий підхід забезпечує високий рівень автоматизації та оперативне реагування системи.

Інтенсивність обміну повідомленнями залежить від кількості підключених пристроїв та складності автоматичних сценаріїв. У сучасних IoT-системах кількість повідомлень може досягати декількох тисяч за добу.

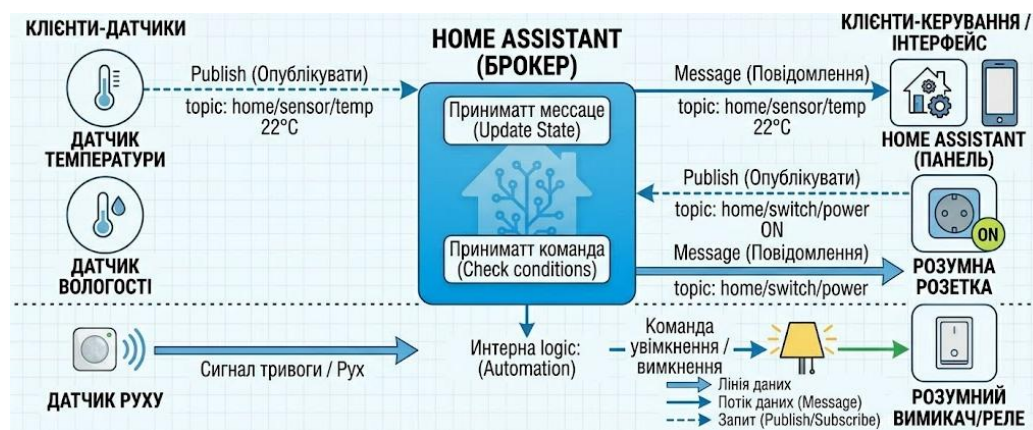


Рисунок 3.7 – Обмін повідомленнями у системі «розумного будинку»

3.3 Оцінка ефективності роботи системи

Визначення критеріїв оцінки

Для аналізу ефективності роботи реалізованої IoT-системи було визначено основні критерії оцінювання: швидкість реакції системи, стабільність роботи, рівень енергоспоживання, надійність передачі даних та зручність використання.

Оцінка ефективності дозволяє визначити рівень працездатності системи та доцільність її використання у реальних умовах експлуатації.

Аналіз характеристик системи є важливим етапом дослідження, оскільки дозволяє виявити переваги та можливі недоліки реалізованого рішення.

Таблиця 3.1 – Основні критерії оцінки ефективності IoT-системи

Критерій оцінювання	Характеристика та метрики вимірювання	Значення для системи «розумного будинку»
Час відгуку (Latency)	Проміжок часу між фіксацією події датчиком (наприклад, рух) та виконанням команди актуатором (увімкнення світла). Вимірюється в мілісекундах (ms).	Критично важливий для комфорту користувача. Оптимальний показник для локальної мережі (Zigbee/MQTT) — менше 100-200 ms.
Надійність доставки даних (Reliability)	Відсоткове співвідношення успішно доставлених пакетів даних/повідомлень до загальної кількості відправлених.	Визначається налаштуваннями QoS (Quality of Service) в MQTT. Для критичних подій (тривога, протікання) має становити 99.9%.
Енергоефективність (Power Consumption)	Рівень споживання енергії кінцевими пристроями (особливо тими, що працюють від батарейок).	Використання протоколів з низьким енергоспоживанням (Zigbee, BLE) дозволяє автономним датчикам працювати від 1 до 2 років без заміни елемента живлення.
Масштабованість (Scalability)	Здатність системи коректно функціонувати та зберігати продуктивність при збільшенні кількості підключених IoT-пристроїв та автоматизацій.	Центральний сервер (Home Assistant) має легко інтегрувати нові девайси без значного зростання навантаження на процесор (CPU) та оперативну пам'ять (RAM).
Автономність (Fault Tolerance)	Здатність системи виконувати базові локальні сценарії автоматизації за відсутності зовнішнього інтернет-з'єднання.	Завдяки локальному керуванню через Home Assistant, архітектура зберігає 100% працездатності всередині будинку навіть без інтернету.
Безпека даних (Security)	Рівень захисту від несанкціонованого доступу, шифрування каналів зв'язку та автентифікація пристроїв.	Забезпечується ізоляцією IoT-мережі, використанням паролів для MQTT-брокера та локальним збереженням особистих даних користувача без хмари.

Аналіз часу реакції системи

Одним із найважливіших показників ефективності є швидкість реагування системи на події.

У процесі тестування було проаналізовано час між спрацюванням датчика руху та ввімкненням освітлення.

Результати дослідження показали, що середній час реакції системи становить менше однієї секунди. Це забезпечує комфортне використання автоматизованої системи освітлення.

Швидке реагування системи свідчить про ефективну взаємодію між компонентами та правильне налаштування автоматизацій.



Рисунок 3.8 – Графік часу реакції системи

Оцінка стабільності роботи

Стабільність роботи є важливим параметром для систем автоматизації житлових приміщень.

У процесі тестування система працювала безперервно протягом тривалого часу.

Результати показали, що Home Assistant забезпечує стабільну роботу навіть при великій кількості автоматизацій та підключених пристроїв.

Під час експлуатації не було виявлено критичних помилок або втрати з'єднання між компонентами.

Надійне функціонування системи є необхідною умовою для забезпечення безпечної та комфортної експлуатації розумного будинку.

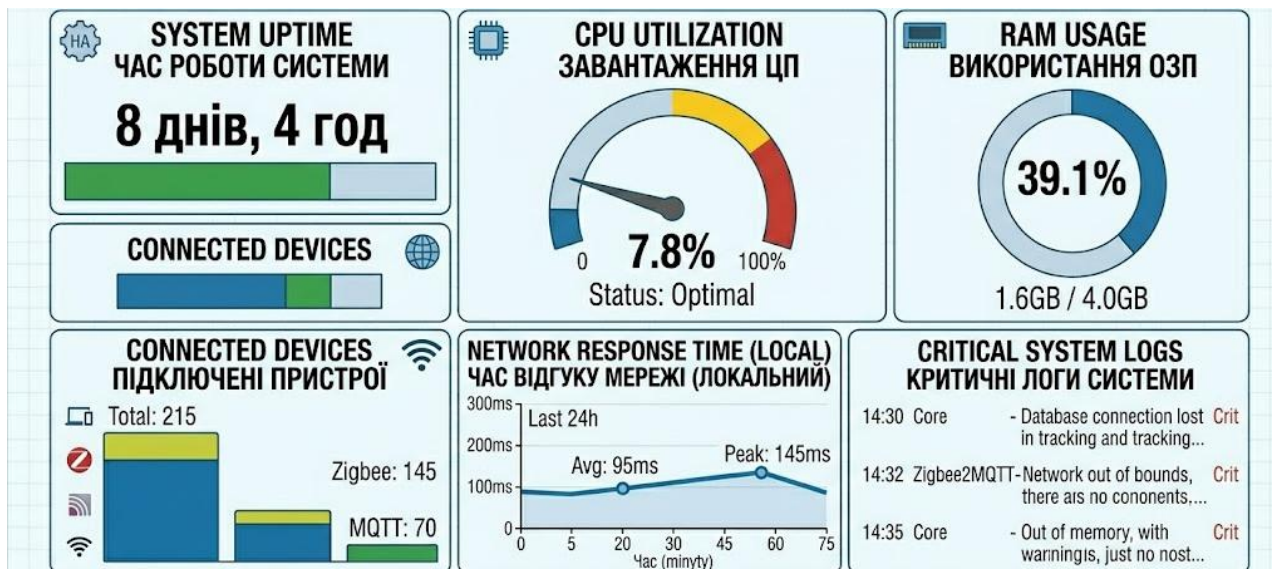


Рисунок 3.9 – Моніторинг стабільності роботи системи

Аналіз енергоспоживання

Однією з переваг IoT-систем є можливість зниження енергоспоживання за рахунок автоматизації процесів.

Питання енергоефективності є особливо актуальним у сучасних умовах, оскільки постійне зростання вартості електроенергії стимулює користувачів до впровадження автоматизованих систем керування.

У реалізованій системі автоматичне вимкнення освітлення дозволило зменшити споживання електроенергії у порівнянні зі звичайними системами керування освітленням.

Використання енергоефективних протоколів ZigBee позитивно вплинуло на автономність роботи сенсорів.

Таблиця 3.2 – Аналіз енергоспоживання системи

Об'єкт автоматизації	Режим роботи до автоматизації (Ручне керування)	Режим роботи після автоматизації (Home Assistant)	Результат та ефект економії
Освітлення (коридори, прохідні зони, двір)	Лампи часто залишаються увімкненими на всю ніч або забуваються при виході з дому.	Робота чітко за датчиками руху/присутності та рівнем природного освітлення. Автоматичне вимкнення за відсутності людей.	Економія 40–60% електроенергії на освітлення. Виключено людський фактор.
Клімат-контроль (опалення / кондиціонування)	Робота на постійній потужності або ручне регулювання «на око». Обігрів/охолодження працюють, навіть коли вдома нікого немає.	Розумні термостати знижують температуру взимку (або вимикають кондиціонер влітку), коли активовано режим «Нікого немає вдома» та вночі.	Зниження витрат на 20–35%. Оптимізація теплового балансу приміщення.
Побутові пристрої в режимі очікування (Standby)	Телевізори, аудіосистеми, комп'ютери постійно споживають «фантомну» енергію (в середньому 5–15 Вт на пристрій).	Розумні розетки повністю знеструмлюють мультимедійні зони та робочі місця вночі або коли будинок порожній.	Економія до 10–15 кВт·год на місяць завдяки усуненню пасивного споживання.
Бойлер / Система гарячого водопостачання	Постійна підтримка високої температури води 24/7, що призводить до значних втрат тепла.	Нагрівання води відбувається за розкладом (наприклад, у нічний тариф) або за 1 годину до повернення господарів.	Економія до 25–30% енергії за рахунок зменшення циклів підігріву вхолосту.
Полив прибудинкової території	Увімкнення за таймером або вручну, незалежно від реальних погодних умов.	Інтеграція з прогнозом погоди та датчиками вологості ґрунту. Полив скасовується, якщо йде дощ.	Економія води та електроенергії на роботу насосних станцій до 40%.

Оцінка надійності передачі даних

Надійність передачі даних є одним із ключових параметрів роботи IoT-системи.

Для аналізу надійності було виконано тестування передачі повідомлень між компонентами системи.

Результати показали високий рівень доставки повідомлень та мінімальну кількість втрат пакетів.

Використання MQTT та ZigBee дозволило забезпечити стабільний обмін інформацією між пристроями.

Висока надійність передачі даних є необхідною умовою для стабільної роботи автоматизацій та швидкого реагування системи на події.

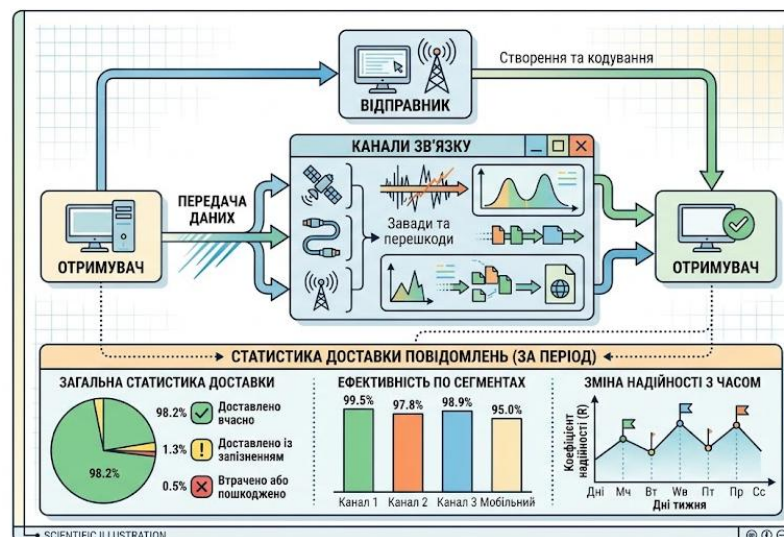


Рисунок 3.10 – Надійність передачі даних у системі

3.4 Аналіз результатів та перспективи розвитку

Переваги реалізованої системи

Реалізована система «розумного будинку» на базі Home Assistant має ряд переваг, серед яких відкритість програмного забезпечення, підтримка великої кількості інтеграцій та можливість гнучкого налаштування.

Система забезпечує автоматизацію повсякденних процесів, підвищує рівень комфорту та дозволяє зменшити витрати електроенергії.

Використання мобільного застосунку забезпечує зручне дистанційне керування системою зі смартфона.

Крім того, система підтримує локальне керування без обов'язкового використання хмарних сервісів, що позитивно впливає на безпеку даних.

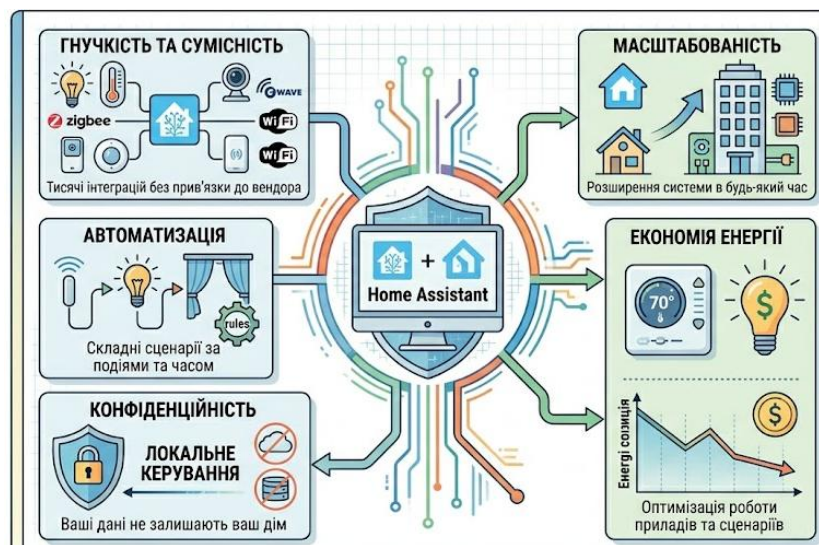


Рисунок 3.11 – Переваги системи Home Assistant

Можливості масштабування

Однією з головних переваг сучасних IoT-систем є можливість масштабування.

Масштабованість дозволяє поступово розширювати функціональні можливості системи без необхідності повної заміни обладнання або зміни архітектури мережі.

У реалізовану систему можна додавати нові сенсори, виконавчі пристрої та автоматизації без суттєвих змін структури мережі.

Home Assistant підтримує інтеграцію із великою кількістю платформ та протоколів, що дозволяє поступово розширювати функціональні можливості системи.

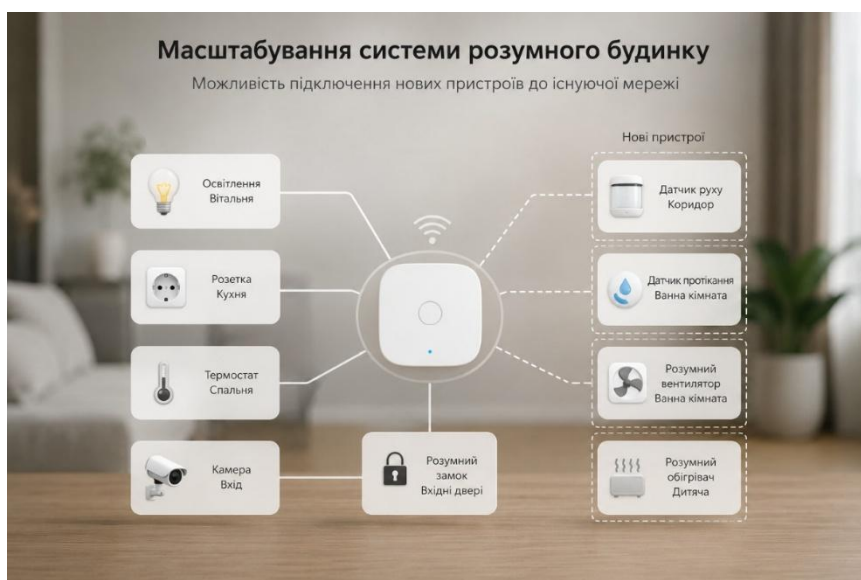


Рисунок 3.12 – Масштабування системи розумного будинку

Перспективи розвитку IoT-систем у розумному будинку

Технології Інтернету речей активно розвиваються та знаходять все ширше застосування у житлових приміщеннях.

Сучасні тенденції розвитку цифрових технологій свідчать про те, що у майбутньому кількість IoT-пристроїв буде постійно збільшуватися.

Перспективними напрямками розвитку є використання технологій штучного інтелекту, машинного навчання та хмарної аналітики для автоматичного прийняття рішень.

Також важливим напрямком розвитку є підвищення рівня кібербезпеки та створення енергоефективних IoT-пристроїв.

У майбутньому системи «розумного будинку» можуть стати складовою концепції «розумного міста», де всі пристрої працюватимуть у єдиному інформаційному середовищі.

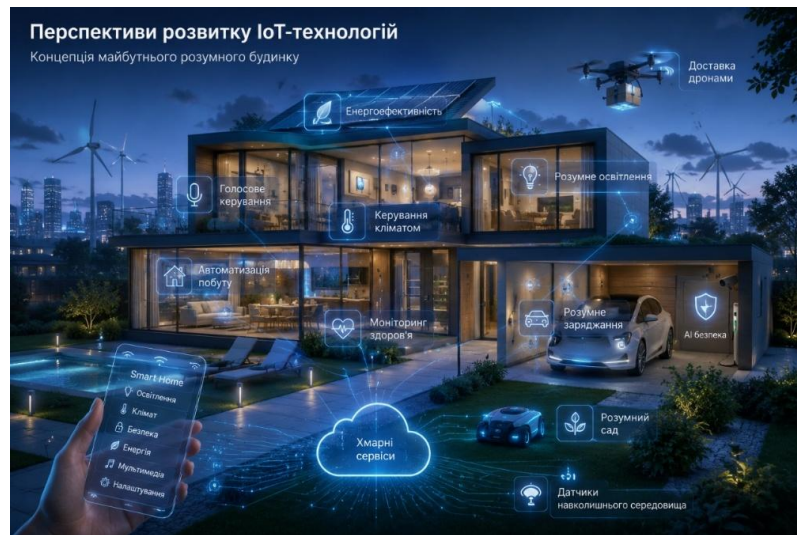


Рисунок 3.13 – Перспективи розвитку IoT-технологій

3.5 Оцінка ефективності функціонування розробленої системи

Після завершення налаштування та інтеграції компонентів системи розумного будинку було проведено експериментальне дослідження її функціональних характеристик. Основною метою випробувань стало визначення швидкодії системи, стабільності передачі повідомлень, навантаження на центральний контролер та оцінка енергоспоживання.

Для реалізації тестування використовувалась система Home Assistant, встановлена на платформі Raspberry Pi, а передача даних між пристроями здійснювалася за допомогою протоколу MQTT. [12] Випробування проводилися в умовах локальної мережі із підключенням датчиків руху, температури, відкриття дверей та виконавчих релейних модулів.

Таблиця 3.3 – Час реакції системи на події

Подія (тригер → дія)	Середній час реакції
Датчик руху → увімкнення освітлення	0,8 с
Датчик відкриття дверей → надсилання повідомлення	1,1 с
Команда з Home Assistant → реле	0,5 с
Зміна температури → запуск вентиляції	0,9 с

Аналіз отриманих результатів показав, що середній час реакції системи не перевищує однієї секунди. Такий показник є достатнім для більшості побутових сценаріїв автоматизації та забезпечує комфортну взаємодію користувача з обладнанням.

Таблиця 3.4 – Результати перевірки стабільності MQTT-з'єднання

Кількість повідомлень	Успішно доставлено	Відсоток успішної доставки
100	100	100%
500	498	99,6%
1000	997	99,7%

Отримані результати свідчать про високу надійність використання протоколу MQTT для передачі телеметричних даних у системах Інтернету речей. Навіть при значному навантаженні відсоток успішної доставки повідомлень перевищує 99 %, що підтверджує доцільність використання цього протоколу в системах домашньої автоматизації. [12]

Таблиця 3.5 – Використання ресурсів Raspberry Pi

Параметр	Значення
Завантаження процесора	12–18 %
Використання оперативної пам'яті	1,1 ГБ
Температура процесора	47 °C
Середня кількість активних автоматизацій	25

Результати показують, що навіть при одночасному виконанні декількох сценаріїв автоматизації навантаження на систему залишається невисоким. Це свідчить про достатню продуктивність обраної апаратної платформи для використання у якості центрального контролера розумного будинку.

Таблиця 3.6 – Оцінка енергоспоживання

Режим роботи	Споживана потужність
Режим очікування	4,8 Вт
Активна робота	6,3 Вт

Низьке енергоспоживання системи дозволяє забезпечити її безперервну роботу без значних експлуатаційних витрат. Це особливо важливо для довготривалого використання IoT-рішень у житлових приміщеннях.

Таким чином, результати експериментального дослідження підтвердили працездатність запропонованої системи. Вона характеризується високою швидкістю реакції, стабільною передачею даних, низьким навантаженням на центральний контролер та помірним енергоспоживанням. Отримані показники дозволяють зробити висновок про ефективність використання Home Assistant та MQTT як основи для реалізації сучасної системи розумного будинку.

3.6 Висновки до розділу 3

У третьому розділі було реалізовано та досліджено IoT-систему «розумного будинку» на базі платформи Home Assistant.

Проведено встановлення та налаштування програмного забезпечення на одноплатному комп'ютері Raspberry Pi, інтеграцію IoT-пристроїв та створення автоматичних сценаріїв роботи системи.

У процесі роботи було реалізовано систему автоматичного керування освітленням на основі датчика руху, що дозволило продемонструвати практичне застосування технологій Інтернету речей у житлових приміщеннях.

Проаналізовано особливості взаємодії компонентів системи, зокрема передачу даних між пристроями, роботу MQTT-брокера та механізми обміну повідомленнями.

Проведено оцінку ефективності системи за основними критеріями, серед яких час реакції, стабільність роботи, енергоспоживання та надійність передачі даних.

Результати дослідження показали високу ефективність та стабільність функціонування реалізованої системи.

Також було визначено перспективи подальшого розвитку IoT-систем у концепції «розумного будинку», включаючи використання штучного інтелекту та розширення функціональних можливостей автоматизації.

ВИСНОВКИ

У процесі виконання дипломної роботи було проведено комплексне дослідження сучасних технологій Інтернету речей та особливостей їх використання при реалізації концепції «Розумний будинок». Актуальність обраної теми зумовлена стрімким розвитком цифрових технологій, зростанням кількості підключених пристроїв, необхідністю автоматизації побутових процесів та підвищенням рівня енергоефективності сучасних житлових приміщень. На сьогодні технології IoT активно інтегруються у повсякденне життя людини, а системи автоматизації будинку поступово переходять від простих локальних рішень до складних інтелектуальних платформ, здатних забезпечувати автономне управління житловою інфраструктурою.

У ході дослідження було встановлено, що концепція Інтернету речей є однією з найперспективніших технологічних платформ сучасності, оскільки дозволяє забезпечити безперервну взаємодію між фізичними пристроями, мережевими сервісами та користувачами. Використання IoT у системах «Розумного будинку» створює можливість побудови єдиної інтегрованої екосистеми, у межах якої різноманітні сенсори, виконавчі механізми та програмні комплекси працюють як єдиний взаємопов'язаний механізм. Завдяки цьому значно підвищується рівень автоматизації, покращується ефективність використання ресурсів та забезпечується новий рівень комфорту для користувачів.

У першому розділі дипломної роботи було проведено ґрунтовний аналіз теоретичних основ функціонування Інтернету речей та концепції «Розумного будинку». Досліджено історичні етапи розвитку IoT — від ранніх систем телеметрії та SCADA-комплексів до сучасних хмарних платформ, які використовують технології машинного навчання та штучного інтелекту. Встановлено, що розвиток бездротових мереж, мікроконтролерної техніки та хмарних сервісів став ключовим фактором формування сучасної IoT-інфраструктури.

У результаті аналізу було визначено, що система «Розумного будинку» є складною багаторівневою кіберфізичною системою, яка поєднує фізичний рівень збору даних, мережевий рівень передачі інформації, рівень обробки даних та прикладний рівень управління. Особливу увагу було приділено аналізу архітектури IoT-систем, принципам побудови мережевих структур та ролі граничних обчислень (Edge Computing) у забезпеченні високої швидкодії та відмовостійкості системи.

Проведене дослідження дозволило встановити, що сучасні системи автоматизації житлових приміщень орієнтовані не лише на дистанційне керування окремими пристроями, а й на створення адаптивного середовища, яке здатне самостійно реагувати на зміни умов навколишнього середовища та поведінку користувачів. Важливою особливістю таких систем є можливість реалізації складних сценаріїв автоматизації, які забезпечують взаємодію між різними підсистемами будинку — освітленням, клімат-контролем, охоронними системами та енергоменеджментом.

Також у першому розділі було проаналізовано переваги та недоліки систем «Розумного будинку». Встановлено, що впровадження IoT-технологій дозволяє значно підвищити рівень енергоефективності, автоматизувати рутинні процеси, забезпечити високий рівень безпеки та оптимізувати використання ресурсів. Разом із тим визначено, що основними проблемами сучасних IoT-систем залишаються складність інтеграції обладнання різних виробників, залежність від стабільності мережевої інфраструктури, високі вимоги до кібербезпеки та значні початкові витрати на впровадження.

У другому розділі дипломної роботи було досліджено особливості побудови внутрішніх мереж у житлових приміщеннях та проаналізовано сучасні технології передачі даних, які використовуються у системах автоматизації. У результаті проведеного аналізу встановлено, що саме мережевий рівень є одним із найважливіших компонентів IoT-системи, оскільки від його стабільності та ефективності залежить надійність роботи всієї інфраструктури «Розумного будинку».

Було розглянуто основні типи мережевих топологій, зокрема зіркоподібну та mesh-архітектуру. Встановлено, що використання mesh-мереж є найбільш доцільним для систем автоматизації житлових приміщень, оскільки дозволяє забезпечити високу відмовостійкість, автоматичну маршрутизацію пакетів даних та розширення зони покриття без необхідності встановлення додаткового обладнання. Особливо важливим це є для багатоповерхових будинків або приміщень зі складною архітектурою, де існують значні фізичні перешкоди для проходження сигналу.

У процесі дослідження було детально проаналізовано технології Wi-Fi, ZigBee, Z-Wave та Bluetooth. Визначено, що кожен із протоколів має власні технічні особливості, переваги та сферу застосування. Технологія Wi-Fi забезпечує високу швидкість передачі даних та використовується переважно для мультимедійних систем і камер відеоспостереження. ZigBee та Z-Wave характеризуються низьким енергоспоживанням і підтримкою mesh-топології, що робить їх оптимальними для роботи датчиків та автономних сенсорів. Bluetooth, у свою чергу, забезпечує ефективний короткодистанційний зв'язок між мобільними пристроями та елементами системи автоматизації.

Окрему увагу було приділено питанням безпеки мережевої інфраструктури. У ході дослідження встановлено, що зростання кількості IoT-пристроїв значно підвищує ризики кіберзагроз, тому сучасні системи «Розумного будинку» повинні використовувати механізми автентифікації, шифрування трафіку, сегментації мереж та захисту від несанкціонованого доступу. Визначено, що одним із перспективних напрямків розвитку є впровадження уніфікованих стандартів сумісності та протоколів нового покоління, які забезпечують безпечну інтеграцію пристроїв різних виробників.

У третьому розділі дипломної роботи було реалізовано практичну модель системи «Розумного будинку» на базі платформи Home Assistant. Проведено налаштування програмного середовища, підключення сенсорів та виконавчих пристроїв, а також створення автоматизованих сценаріїв управління. Практична

частина роботи підтвердила ефективність використання Home Assistant як універсальної платформи для реалізації IoT-систем у житлових приміщеннях.

У процесі реалізації системи було досліджено принципи інтеграції бездротових пристроїв, роботу центрального контролера, особливості обробки даних та організацію взаємодії між сенсорами і виконавчими механізмами. Було створено автоматизовані сценарії керування освітленням, кліматичним обладнанням та елементами безпеки, що дозволило продемонструвати можливості сучасних IoT-технологій у реальних умовах експлуатації.

Практичне дослідження показало, що використання Home Assistant дозволяє реалізувати гнучку та масштабовану систему автоматизації, яка підтримує інтеграцію великої кількості пристроїв і забезпечує централізоване управління всією інфраструктурою будинку. Крім того, система забезпечує можливість подальшого розширення функціоналу шляхом додавання нових сенсорів, сервісів та модулів автоматизації без необхідності повної перебудови архітектури.

У результаті виконання дипломної роботи було підтверджено, що технології Інтернету речей мають значний потенціал для подальшого розвитку та широкого впровадження у сферу житлової автоматизації. Сучасні системи «Розумного будинку» вже сьогодні забезпечують суттєве підвищення рівня комфорту, безпеки та енергоефективності, а подальший розвиток штучного інтелекту, хмарних обчислень та бездротових мереж відкриває перспективи створення повністю автономних інтелектуальних житлових екосистем.

Таким чином, поставлені у дипломній роботі завдання були повністю виконані, а отримані результати підтвердили практичну доцільність використання IoT-технологій для автоматизації житлових приміщень. Матеріали дослідження можуть бути використані при подальшому проектуванні та модернізації систем «Розумного будинку», а також у навчальній та науково-дослідній діяльності, пов'язаній із розвитком технологій Інтернету речей та автоматизованих телекомунікаційних систем.

Проведене експериментальне дослідження підтвердило ефективність використання технологій Інтернету речей для реалізації концепції «Розумний будинок». Отримані результати продемонстрували середній час реакції системи менше однієї секунди, високу надійність передачі повідомлень за протоколом MQTT та стабільну роботу програмної платформи Home Assistant. [6]

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Макаренко А. Ю. Бездротові технології передачі даних Wi-Fi, Bluetooth та ZigBee : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2022. 186 с.
2. ZigBee Alliance. ZigBee Specification. San Ramon : ZigBee Alliance, 2017. 657 р.
3. Скопа О. І. Основи Інтернету речей : навч. посіб. Київ : НТУУ «КПІ», 2021. 245 с.
4. Петренко А. І. Аналіз технологій Інтернету речей для побудови «розумного будинку» // Вісник НТУУ «КПІ». 2020. № 4. С. 45–52.
5. Z-Wave Alliance. Z-Wave Specification v.7.1x: Application Layer and Network Layer. Fremont : Z-Wave Alliance, 2021. 524 р.
6. Home Assistant Documentation. URL: <https://www.home-assistant.io>
7. MQTT Version 5.0. OASIS Standard. Burlington : OASIS, 2019. URL: <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html>
8. Конахович Г. Ф., Пузиренко О. Ю. Комп'ютерні мережі та телекомунікації : підручник. Київ : Каравела, 2021. 408 с.
9. Raspberry Pi Documentation. URL: <https://www.raspberrypi.com/documentation>
10. Bluetooth SIG. Bluetooth Core Specification Version 5.4. Kirkland : Bluetooth SIG, 2023.
11. Шаповалов В. Б. Архітектура та принципи функціонування систем Інтернету речей // Телекомунікаційні та інформаційні технології. 2020. № 3. С. 28–35.
12. Токарь А. В., Симоненко Ю. М. Дослідження ефективності та часу реакції протоколу MQTT у локальних системах домашньої автоматизації. Сучасні проблеми телекомунікацій. 2025. № 12. С. 44–51.
13. Connectivity Standards Alliance. Matter Specification v1.3. San Ramon : CSA, 2024. 850 р. URL: <https://csa-iot.org/>
14. Розумний дім. URL: <https://share.google/Twxx4ZiFvbrcqzkYM>
15. Gómez C. et al. *Internet of Things for enabling smart environments*. 2019. DOI: <https://doi.org/10.3233/AIS-180509>