

**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: «Аналіз побудови мереж Інтернету речей»

Виконав:

студент IV курсу, групи ТС-21
Піддубний Артем Анатолійович

Керівник:

Доцент, кандидат технічних наук, доцент,
Максимов В.В.

Рецензент:

Доцент, кандидат технічних наук, доцент
Правило В.В.

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

Студент _____

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

Піддубному Артему Анатолійовичу

1. Тема роботи «Аналіз побудови мереж Інтернету речей», керівник роботи Максимов Володимир Васильович, кандидат наук, доцент кафедри ЕКІР НН ІТС, затверджені наказом по університету від «26» травня 2026 р. № 1912-С
2. Термін подання студентом роботи 15 травня 2026 р.
3. Вихідні дані до роботи: сучасні наукові публікації, стандарти та технічні характеристики хмарних технологій, посібники
 - Пулеко І. В. Єфіменко А. А. Архітектура та технології Інтернету речей: навч. посіб. / І.В. Пулеко, А.А. Єфіменко. – Електронні дані. – Житомир: Державний університет «Житомирська політехніка», 2022. – 234 с.
 - Технології Інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. Для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю.

Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 12,5 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2021.

4. Зміст роботи:

- аналіз теоретичних основ Інтернету речей;
- аналіз структури та основних компонентів IoT-систем;
- дослідження принципів організації мереж Інтернету речей;
- аналіз технологій передачі даних у IoT-мережах (Wi-Fi, Bluetooth Low Energy, ZigBee, LoRaWAN, NB-IoT, LTE-M, 5G IoT);
- проблеми безпеки та надійності IoT-систем;
- аналіз практичного застосування Інтернету речей;
- формування висновків та практичних рекомендацій щодо використання технологій Інтернету речей.

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

- презентація дипломної роботи;
- структурна схема IoT-системи;
- схема архітектури мережі Інтернету речей;
- схеми IoT-мереж на основі технологій Wi-Fi, Bluetooth Low Energy, ZigBee, LoRaWAN та NB-IoT; mesh-топологія мережі ZigBee; структура LoRaWAN-мережі; структура мережі NB-IoT; -
- таблиця порівняння технологій передачі даних у мережах Інтернету речей;
- ілюстрації принципів функціонування IoT-систем та приклади практичного застосування Інтернету речей.

6. Дата видачі завдання 18.02.2026 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Вибір теми дипломної роботи та затвердження завдання	18.02.2026 – 22.02.2026	Виконано
2	Аналіз наукової літератури та джерел за темою дослідження	23.02.2026 – 05.03.2026	Виконано
3	Розробка теоретичного розділу роботи	06.03.2026 – 18.03.2026	Виконано
4	Дослідження технологій та принципів побудови IoT-мереж	19.03.2026 – 01.04.2026	Виконано
5	Аналіз технологій передачі даних та безпеки IoT-систем	02.04.2026 – 12.04.2026	Виконано
6	Аналіз практичного застосування IoT-систем	13.04.2026 – 25.04.2026	Виконано
7	Оформлення графічного та ілюстративного матеріалу	26.04.2026 – 05.05.2026	Виконано
8	Формування висновків та остаточне оформлення роботи	06.05.2026 – 12.05.2026	Виконано
9	Подання дипломної роботи на перевірку	15.05.2026	Виконано

Студент

Артем ПІДДУБНИЙ

Керівник роботи

Володимир МАКСИМОВ

РЕФЕРАТ

Актуальність дослідження обумовлена стрімким збільшенням числа підключених пристроїв у різних сферах – від систем «розумного дому» до промислових застосувань і «розумних міст», що потребує детального вивчення сучасних технологій передачі даних, безпекових аспектів та ефективності роботи таких мереж.

Метою роботи є розглянути ключові компоненти Інтернету речей (IoT), провести аналіз технологій обміну даних, таких як Wi-Fi, Bluetooth Low Energy, ZigBee, LoRaWAN, NB-IoT та інші, визначити особливості їх функціонування і виявити актуальні проблеми безпеки. Також передбачено практичне дослідження на прикладі системи «розумного будинку» і обґрунтування напрямків подальшого удосконалення IoT-мереж.

У процесі дослідження розглянуто Інтернет речей як складну інформаційно-комунікаційну систему, що інтегрує фізичні пристрої, датчики, програмне забезпечення та мережеві рішення. Розкрито архітектуру IoT-систем і проаналізовано основні сфери їх застосування: промисловість (з урахуванням концепції «Індустрія 4.0»), «розумні міста», охорона здоров'я, сільське господарство, транспорт, енергетика та побут. Проведений порівняльний аналіз основних характеристик технологій з урахуванням дальності покриття, швидкості передачі даних, енергоспоживання і мережевої топології. Виявлено, що Wi-Fi забезпечує високу пропускну здатність, однак характеризується підвищеним споживанням енергії.

Окрему увагу приділено проблемам безпеки: уразливості пристроїв, можливості перехоплення інформації в бездротових мережах, відсутності єдиних стандартів захисту, ризикам DDoS-атак за участю ботнетів на базі IoT-пристроїв, а також питанням конфіденційності персональних даних. Запропоновано комплекс заходів захисту, що включає використання шифрування, впровадження багатофакторної аутентифікації, регулярне оновлення програмного забезпечення і моніторинг активності мережі.

Практична частина роботи присвячена дослідженню системи «розумного будинку», побудованої на поєднанні Wi-Fi та ZigBee. Розглянуто функціонування сенсорів визначення температури, вологості, руху, диму, витоку газу тощо. У роботі запропоновано шляхи покращення IoT-мереж, серед яких – підвищення кіберзахисту завдяки сучасним методам шифрування, багатофакторній аутентифікації, регулярним оновленням firmware та автоматичному моніторингу мережевої діяльності.

Також рекомендовано впровадження концепції edge computing для зниження затримок, оптимізації навантаження на мережу й зменшення залежності від хмарних сервісів. Для підвищення енергоефективності і розширення радіусу дії доцільно використовувати новітні технології, зокрема 5G, Wi-Fi HaLow та LoRaWAN. Важливим також є уніфікація взаємодії пристроїв шляхом впровадження стандартів Matter і Thread, що забезпечує сумісність пристроїв різних виробників. Перспективним напрямом розвитку є інтеграція штучного інтелекту і машинного навчання для автоматичного налаштування системи відповідно до поведінки користувачів, прогнозування змін навколишнього середовища та оптимізації роботи IoT-пристроїв.

Об'єктом дослідження є технології передачі даних, архітектура та аспекти безпеки мереж інтернету речей (IoT), а також їх практичне застосування в реальних умовах на прикладу «розумного дому»

Предметом дослідження є особливості функціонування, проблеми безпеки та методи удосконалення IoT-мереж, а також застосування конкретних технологій передачі даних у системах «розумного дому».

Ключові слова: АРХІТЕКТУРА ІОТ, РОЗУМНИЙ БУДИНОК, ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ, LORAWAN, ZIGBEE, WI-FI, NB-IOT, КІБЕРБЕЗПЕКА, МАШИННЕ НАВЧАННЯ, EDGE COMPUTING, 5G.

ABSTRACT

The relevance of this research is driven by the rapid increase in the number of connected devices across various fields – from smart home systems to industrial applications and smart cities – which necessitates a thorough examination of modern data transmission technologies, security aspects, and the operational efficiency of such networks.

The aim of this work is to examine the key components of the Internet of Things (IoT), conduct an analysis of data exchange technologies such as Wi-Fi, Bluetooth Low Energy, ZigBee, LoRaWAN, NB-IoT, and others, identify the features of their operation, and reveal current security challenges. Additionally, a practical study is planned using the example of a smart home system and justification of directions for further improvement of IoT networks.

The research considers the Internet of Things as a complex information and communication system that integrates physical devices, sensors, software, and networking solutions. The architecture of IoT systems is described, and their main application areas are analyzed: industry (including the Industry 4.0 concept), smart cities, healthcare, agriculture, transportation, energy, and domestic sectors. A comparative analysis of the main characteristics of the technologies was conducted, taking into account coverage range, data transmission speed, energy consumption, and network topology. It was found that Wi-Fi provides high data throughput but is characterized by increased energy consumption.

Special attention is devoted to security issues: device vulnerabilities, the possibility of data interception in wireless networks, the lack of unified security standards, risks of DDoS attacks involving botnets based on IoT devices, as well as concerns about personal data privacy. A comprehensive set of protection measures is proposed, including the use of encryption, implementation of multi-factor authentication, regular software updates, and monitoring of network activity.

The practical part of the work focuses on the study of a smart home system built on a combination of Wi-Fi and ZigBee technologies. The functioning of sensors

measuring temperature, humidity, motion, smoke, gas leakage, and others is examined. The work proposes ways to improve IoT networks, including enhancing cybersecurity through modern encryption methods, multi-factor authentication, regular firmware updates, and automated monitoring of network activities.

The introduction of edge computing is also recommended to reduce latency, optimize network load, and decrease reliance on cloud services. To increase energy efficiency and expand coverage range, the use of emerging technologies such as 5G, Wi-Fi HaLow, and LoRaWAN is advisable. Standardizing device interaction through the adoption of Matter and Thread standards, ensuring compatibility of devices from different manufacturers, is also important. A promising direction for development is the integration of artificial intelligence and machine learning for automatic system adaptation to user behavior, environmental change prediction, and optimization of IoT device operation.

Object of the study: Systems and technologies of the Internet of Things (IoT), including networks and devices that enable data transmission and operation of IoT environments in various application areas, particularly in smart home systems.

Subject of the study: Features of functioning, security issues, and improvement methods of IoT networks, as well as the application of specific data transmission technologies (Wi-Fi, ZigBee, Bluetooth Low Energy, LoRaWAN, etc.) in smart home systems.

Keywords: IOT ARCHITECTURE, SMART HOME, DATA TRANSMISSION TECHNOLOGIES, LORAWAN, ZIGBEE, WI-FI, Nb-IOT , CYBERSECURITY, MACHINE LEARNING, EDGE COMPUTING, 5G.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	10
ВСТУП.....	11
1 ТЕОРЕТИЧНІ ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ.....	14
1.1 Сутність та поняття Інтернету речей	14
1.2 Основні напрями застосування Інтернету речей.....	16
1.3 Структура та основні компоненти IoT-систем	18
1.4 Висновки до розділу 1	23
2 ОСОБЛИВОСТІ ПОБУДОВИ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ.....	24
2.1 Принципи організації IoT-мереж	24
2.2 Технології передачі даних у IoT (Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NB-IoT та інші).....	27
2.3 Особливості функціонування IoT-мереж	33
2.4 Проблеми безпеки та надійності IoT-систем.....	36
2.5 Висновки до розділу 2.....	42
3 АНАЛІЗ ПРАКТИЧНОГО ЗАСТОСУВАННЯ IoT	43
3.1. Загальна характеристика обраної IoT-системи.....	43
3.2 Аналіз принципу роботи системи.....	45
3.3 Переваги та недоліки використання	49
3.4 Напрями удосконалення IoT-мереж.....	52
3.5 Висновки до розділу 3.....	56
ВИСНОВКИ.....	58
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	62
ДОДАТКИ	65
Додаток А	65
Додаток Б.....	65
Додаток В	66
Додаток Г	67

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

5G	П'яте покоління мобільного зв'язку з високою швидкістю передачі даних та низькою затримкою.
5G IoT	Застосування 5G мереж для Інтернету речей, що забезпечує високу швидкість, низьку затримку та велику кількість підключень.
AI	Artificial Intelligence (штучний інтелект).
BLE	Bluetooth Low Energy; технологія енергоефективного Bluetooth.
DDoS	Distributed Denial of Service; розподілена атака відмови в обслуговуванні.
DoS	Denial of Service; атака відмови в обслуговуванні.
Edge Computing	Периферійні обчислення; парадигма розподілених обчислень, за якої обробка даних відбувається максимально близько до джерела їх генерації (на edge-шлюзах).
IoT	Internet of Things (Інтернет речей).
LTE-M	LTE Cat-M1; технологія мобільного зв'язку для IoT із низьким енергоспоживанням.
LoRaWAN	Long Range Wide Area Network; протокол для бездротових мереж з великим радіусом дії та низьким енергоспоживанням.
MSE	Mean Squared Error (середньоквадратична помилка); функція втрат, що використовується для оцінки точності реконструкції даних автоенкодером.
NFC	Near Field Communication; технологія бездротового зв'язку ближнього радіусу дії.
NB-IoT	Narrowband Internet of Things; технологія вузькосмутового Інтернету речей.
QoS	Quality of Service (якість обслуговування); механізми, що забезпечують гарантії якості передачі даних у мережах.
Wi-Fi	Wireless Fidelity; стандарт бездротового зв'язку високої швидкості.

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій та глобальної інформатизації суспільства особливого значення набуває концепція Інтернету речей (Internet of Things, IoT), яка є одним із ключових напрямів розвитку сучасних інформаційно-комунікаційних систем. Інтернет речей передбачає об'єднання фізичних пристроїв, сенсорів, програмного забезпечення та мережевих технологій у єдине інформаційне середовище, що забезпечує автоматизований збір, передачу, обробку та аналіз даних у режимі реального часу. Завдяки цьому створюються широкі можливості для автоматизації процесів, оптимізації використання ресурсів, підвищення ефективності управління та покращення якості життя населення.

Актуальність теми дослідження обумовлена активним впровадженням IoT-технологій у різні сфери діяльності, зокрема промисловість, транспорт, медицину, аграрний сектор, енергетику, системи безпеки та концепції «розумного дому» і «розумного міста». Постійне збільшення кількості підключених пристроїв, розвиток бездротових технологій передачі даних та необхідність забезпечення стабільного функціонування IoT-систем зумовлюють потребу у дослідженні особливостей побудови мереж Інтернету речей, їх архітектури, принципів функціонування та проблем практичного впровадження. Особливої уваги потребують питання безпеки, масштабованості, надійності та ефективності функціонування IoT-мереж в умовах сучасного цифрового середовища.

Метою роботи є дослідження особливостей побудови мереж Інтернету речей, аналіз архітектури та принципів функціонування IoT-систем, а також оцінка практичного впровадження IoT-мереж на прикладі реальної системи з визначенням її переваг, недоліків і можливостей подальшого вдосконалення.

Для досягнення поставленої мети необхідно виконати такі завдання:

- розкрити сутність та основні поняття Інтернету речей;
- дослідити основні напрями застосування IoT-технологій;

- проаналізувати структуру та основні компоненти IoT-систем;
- охарактеризувати принципи організації IoT-мереж;
- дослідити технології передачі даних у мережах Інтернету речей;
- визначити особливості функціонування IoT-мереж;
- проаналізувати проблеми безпеки та надійності IoT-систем;
- здійснити аналіз побудови реальної IoT-мережі;
- дослідити принцип функціонування обраної IoT-системи;
- визначити переваги та недоліки практичного використання IoT-технологій;
- обґрунтувати напрями вдосконалення мереж Інтернету речей.

Об'єктом дослідження є мережі Інтернету речей як складні інформаційно-комунікаційні системи.

Предметом дослідження є теоретичні та практичні аспекти побудови, функціонування та впровадження IoT-мереж, а також технології, що забезпечують їх роботу.

Методи дослідження включають аналіз наукової літератури, узагальнення теоретичних підходів, системний аналіз архітектури IoT-мереж, порівняння сучасних технологічних рішень, аналіз практичного впровадження IoT-систем, а також методи логічного узагальнення отриманих результатів.

Практичне значення одержаних результатів полягає у можливості використання результатів дослідження для вдосконалення існуючих IoT-систем, підвищення їх ефективності, безпеки та надійності, а також при проектуванні й впровадженні сучасних інформаційно-телекомунікаційних рішень.

Структура роботи визначається метою та поставленими завданнями і складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. У першому розділі розглянуто теоретичні основи Інтернету речей та основні компоненти IoT-систем. Другий розділ присвячений дослідженню особливостей побудови та функціонування мереж Інтернету речей, технологій передачі даних, а також проблем безпеки та надійності IoT-систем. У третьому розділі здійснено аналіз практичного застосування IoT-технологій на прикладі

реальної системи, визначено її переваги, недоліки та перспективи вдосконалення.

1 ТЕОРЕТИЧНІ ОСНОВИ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Сутність та поняття Інтернету речей

Ідея Мережі Взаємопов'язаних Об'єктів (Internet of Things, IoT) постає як новітній етап еволюції технологій зв'язку, що має на меті об'єднати фізичні об'єкти в уніфікований каркас, дозволяючи їм комунікувати через Всесвітню мережу. Наріжний принцип IoT полягає у запровадженні автоматизованого збирання, опрацювання та передачі інформації між апаратами без потреби прямого втручання людини, що веде до підвищення ефективності робочих процесів та раціоналізації використання доступних ресурсів [17]. Міжнародний союз електросполучення дає таке визначення: Інтернет речей – це світова інфраструктура для інформаційного соціуму, яка надає розширені сервіси через взаємозв'язок матеріальних та віртуальних об'єктів, базуючись на існуючих та перспективних комунікаційних і цифрових технологіях [20]. У цьому контексті IoT виступає як логічне продовження еволюції мережевих методик, які інтегрують традиційні телекомунікаційні рішення з найсучаснішими цифровими сервісами та платформами, закладаючи підвалини для становлення цифрової економіки.

Наукові підходи до дефініції Інтернет речей концентруються на її суто системному характері. Зокрема, IoT трактується як сукупність з'єднаних апаратних засобів, якими оснащені сенсори, програмне забезпечення та комунікаційні модулі, що забезпечують обмін даними між фізичними об'єктами та інформаційними комплексами [18]. Такий погляд дозволяє розглядати IoT не лише як окремий технологічний інструмент, а як цілісну екосистему, що поєднує фізичний та віртуальний виміри. Головною рисою Інтернету речей є її здатність до масштабування, яка дозволяє під'єднувати мільярди пристроїв до мережі, а також гетерогенність, що означає здатність до взаємодії різнорідних технічних засобів і платформ. Важливими атрибутами IoT також є автономність функціонування систем, здатність до самостійного формування рішень на основі отриманих даних, а також аналіз великих обсягів інформації у режимі,

близькому до реального часу [19]. Це дає змогу оперативно реагувати на зміни в оточенні та збільшує продуктивність систем.

Сенсорні технології відіграють ключову роль у механізмах роботи IoT, оскільки вони відповідають за збір первинних відомостей про стан об'єктів, параметри навколишнього середовища чи моделі поведінки користувачів. Зібрані дані транслюються через комунікаційні мережі до обчислювальних центрів, де вони проходять аналіз із застосуванням передових алгоритмів, включаючи методики штучного інтелекту та машинного навчання, і використовуються для формування керуючих рішень [22]. Нерозривною складовою концепції Інтернет речей є її тісна взаємодія з хмарними обчислювальними потужностями, що забезпечує зберігання та обробку значних масивів даних, а також організовує доступ до них з будь-якої точки світу. Хмарні сервіси створюють передумови для гнучкості та розширення IoT-систем, що є критично важливим для їхнього масового впровадження [19].

Крім того, Інтернет речей інтерпретується як структура, що складається з декількох шарів: рівня фізичних пристроїв, рівня мережевої трансмісії інформації та прикладного рівня опрацювання даних. Кожен із цих рівнів виконує свої специфічні завдання, проте їхня спільна функціональність гарантує цілісність та ефективність роботи усієї системи [10]. Така архітектурна будова уможливорює реалізацію складних сценаріїв використання IoT у різноманітних галузях діяльності. Поза суто технічними аспектами, Інтернет речей чинить вагомий вплив на соціально-економічну сферу. Її імплементація сприяє піднесенню продуктивності праці, зменшенню фінансових витрат, покращенню якості наданих послуг та виникненню нових бізнес-моделей. Водночас розвиток IoT ставить перед суспільством нові виклики, особливо у площині кібербезпеки, захисту особистих даних та забезпечення надійності функціонування комплексів [11].

Таким чином, Інтернет речей — це комплексна технологічна ідея, що інтегрує різноманітні апаратні засоби, мережі та інформаційні системи з метою забезпечення ефективної комунікації між ними. Її подальший розвиток

відкриває широкі можливості для автоматизації процесів, посилення ефективності управління та піднесення рівня життя громадян, що засвідчує її ключову роль у побудові сучасного інформаційного соціуму.

1.2 Основні напрями застосування Інтернету речей

Інтернет речей вирізняється надзвичайно широким колом застосування у різних аспектах життєдіяльності, що зумовлене його здатністю здійснювати автоматизоване збирання, передачу й обробку інформації, а також реалізовувати злагоджену взаємодію між пристроями в реальному часі. Завдяки цим можливостям, IoT постає як один із наріжних каменів у процесі цифрової перебудови економіки, сприяючи зростанню продуктивності, вдосконаленню систем керування та формуванню нових моделей взаємодії між господарюючими суб'єктами [1].

Одним із найсуттєвіших фронтів застосування Інтернету речей є промисловість, де активно кристалізується ідея «Індустрії 4.0», що передбачає повне включення кіберфізичних систем у виробничі цикли. У цьому контексті IoT залучається для автоматизації виробництва, нагляду за станом устаткування, передбачення потенційних поломок, а також оптимізації логістичних ланцюгів. Використання «розумних» сенсорів та аналітичних платформ дає змогу підприємствам суттєво знизити операційні витрати, покращити ефективність використання матеріальних ресурсів та гарантувати безперебійність виробничого процесу [28]. Помітного розмаху набуло впровадження Інтернету речей у розбудові «розумних» міст, де його функціонал охоплює регулювання транспортних потоків, управління системами забезпечення енергією, освітленням, водопостачанням, утилізацією відходів та підтриманням громадської безпеки. Застосування IoT-рішень надає місцевим органам влади інструменти для гнучкого реагування на зміни в урбаністичному середовищі, підвищення раціональності використання ресурсів та покращення рівня існування мешканців [14].

У галузі охорони здоров'я Інтернет речей відкриває принципово нові горизонти для розвитку цифрової медицини. Інтеграція пристроїв, які носяться (wearables), медичних датчиків та систем дистанційного нагляду дає змогу здійснювати неперервний контроль за станом пацієнтів, оперативно виявляти будь-які негативні відхилення та підвищувати результативність терапії. Додатково, IoT є потужним каталізатором для телемедицини, що є надзвичайно важливим у ситуаціях обмеженого доступу громадян до медичних послуг [19]. В аграрному секторі Інтернет речей закладає фундамент для формування «розумного» сільського господарства, яке базується на застосуванні цифрових методик для нарощування ефективності агропромислового комплексу. Використання сенсорів для моніторингу рівня ґрунтової вологи, температурних показників, освітлення, а також впровадження систем автоматичного зрошення та внесення добрив дозволяє впорядкувати виробничі етапи, мінімізувати витрати ресурсів та збільшити обсяги врожаю [26].

Транспортна індустрія також активно інтегрує IoT-технології, що виявляється у формуванні інтелектуальних транспортних систем. Такі системи забезпечують відстеження руху транспортних одиниць, оптимізацію руху на дорогах, підвищення безпеки перевезень та розвиток безпілотного транспорту. Застосування Інтернету речей у цій сфері сприяє зниженню показників аварійності, скороченню часу доставки вантажів та підвищенню ефективності логістичних операцій [29]. Важливим напрямком використання Інтернету речей є сфера побуту, зокрема реалізація парадигми «розумного дому». Подібні системи забезпечують автоматичне керування освітленням, системами опалення, клімат-контролю, безпекою та побутовою технікою. Це не лише підносить рівень затишку проживання, а й гарантує енергоефективність та скорочує витрати на експлуатацію житлових приміщень [22].

Окремої уваги заслуговує застосування IoT у секторі енергетики, де він слугує для створення «просунутих» електричних мереж (Smart Grid). Ці мережі забезпечують раціональний розподіл електроенергії, моніторинг її споживання, інтеграцію джерел відновлюваної енергії та підвищення надійності постачання.

Завдяки впровадженню IoT-рішень стає можливим швидке виявлення несправностей та оптимізація енергетичних потоків [19]. Окрім згаданих сфер, Інтернет речей активно задіяний у сфері екологічного нагляду, де він дає змогу контролювати стан довкілля, рівень забруднення води та повітря, а також прогнозувати екологічні загрози. Крім того, IoT знаходить застосування у торгівлі та логістиці для управління ланцюгами постачання, контролю складських запасів та автоматизації складських операцій [27].

Підсумовуючи, Інтернет речей охоплює значну кількість секторів, серед яких промисловість, медицина, транспорт, аграрний комплекс, енергетика, міська інфраструктура та житлово-комунальний сектор. Його імплементація стимулює підвищення операційної ефективності, раціоналізацію використання ресурсів, розвиток інноваційних рішень та покращення загального рівня життя громадян, що підтверджує його центральну роль у формуванні сучасної цифрової цивілізації.

1.3 Структура та основні компоненти IoT-систем

Інтернет Речей (скорочено IOT) являє собою розгалужену інформаційно-комунікаційну систему, що має декілька рівнів, робота якої гарантується завдяки злагодженій взаємодії апаратної бази, мережевої інфраструктури, програмного забезпечення та апаратів для обробки інформації. Структура IOT-рішень проектується відповідно до сучасних світових стандартів, зокрема ISO/IEC 30141, де Інтернет Речей розглянуто як інтегроване середовище, що обслуговує увесь цикл роботи з даними — від їхнього збору та транслявання до аналізу, збереження та застосування у прикладних сервісах [6]. Цей підхід дає змогу сприймати IOT не просто як окрему технологію, а як цілісну цифрову екосистему, яка об'єднує фізичний та віртуальний світи. Архітектура таких рішень відзначається багат шаровою будовою, де кожен шар виконує свої специфічні задачі, але всі елементи функціонують у тісному зв'язку.

Перший, фундаментальний шар — це рівень фізичних пристроїв, або сенсорний шар. Він охоплює різноманітні датчики, сенсорні елементи, актуатори та інше апаратне обладнання, що забезпечують прямий контакт системи з реальним світом. Основна мета цього шару полягає у зборі первинних відомостей про характеристики навколишнього середовища чи контролюваного об'єкта. Сенсорні пристрої здатні реєструвати такі показники, як тепло, вологість, освітленість, тиск, рух, вібрації, географічне розташування та низку інших фізичних параметрів. У сучасних ІОТ-системах ці сенсорні вузли нерідко мають вбудовані мікроконтролери, що дозволяють попередньо обробляти інформацію ще до того, як вона потрапить у мережу. Це допомагає знизити навантаження на мережеву частину та підвищує загальну продуктивність системи [18].

Не менш важливою складовою сенсорного рівня є актуатори, або виконавчі механізми, які відповідають за виконання команд управління та безпосередній фізичний вплив на оточення. До цієї категорії належать реле, електроприводи, системи автоматичного освітлення, терморегулятори, клапани, двигуни та подібні елементи. Саме завдяки актуаторам ІОТ-система не лише моніторить стан середовища, але й може автономно реагувати на зміни, виконуючи відповідні дії. Наприклад, система може автоматично ввімкнути освітлення за фіксації руху або запустити систему вентиляції, якщо температура перевищила задану межу [24].

Другим рівнем ІОТ-архітектури є мережевий рівень, завданням якого є транслявання даних між пристроями, шлюзами, серверами та іншими складовими системи. Саме мережевий шар забезпечує комунікацію між усіма частинами ІОТ-системи, створюючи умови для безперебійної інформаційної взаємодії. Для передачі даних використовуються різноманітні канали зв'язку, серед яких найпоширенішими є Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NFC, Ethernet та мобільні мережі. Кожна технологія має свої особливості щодо швидкості обміну даними, радіусу дії, енергоспоживання та рівня надійності [3].

Технологія Wi-Fi забезпечує високу швидкість передачі даних і переважно застосовується там, де потрібен обмін великими обсягами інформації. Bluetooth Low Energy (BLE) сфокусований на енергоефективних IOT-рішеннях з обмеженим радіусом дії. ZigBee використовується для формування мереж типу «сітка» з великою кількістю підключених пристроїв та низьким споживанням енергії. LoRaWAN, у свою чергу, дає змогу передавати дані на значні відстані з мінімальними енергетичними витратами, що робить цю технологію придатною для систем екологічного контролю, агросектору та розвитку «розумних міст» [7].

Центральну роль у структурі IOT-систем відіграють шлюзи або контролери, які координують роботу всіх вузлів системи. Контролер приймає інформацію від датчиків, обробляє її, маршрутизує інформаційні потоки і віддає команди виконавчим механізмам. Крім того, шлюз слугує містком між локальною IOT-мережею та хмарними сервісами. У сучасних рішеннях контролери здатні підтримувати роботу з різними мережевими протоколами одночасно, що дозволяє об'єднувати різнотипні пристрої в межах єдиної системи [24].

Наступним важливим елементом IOT-архітектури є шар, відповідальний за обробку та зберігання даних. На цьому етапі відбувається накопичення, аналіз, інтерпретація та упорядкування інформації, отриманої від sensorів. Для виконання цих завдань залучаються серверні системи, дата-центри, хмарні платформи та технології периферійних обчислень (edge computing). MSE рішення гарантують масштабованість системи, доступ до значних обчислювальних потужностей та централізоване керування інформаційними потоками. Водночас, edge computing дає змогу проводити частину обчислень безпосередньо на периферійних вузлах або пристроях, що мінімізує затримки при передачі даних, зменшує навантаження на мережу та прискорює час реакції системи [19].

Вирішальне значення у функціонуванні IOT-систем має прикладний шар, який забезпечує взаємодію кінцевого користувача із системою. Саме тут

втілюються програмні сервіси, мобільні додатки, веб-інтерфейси, аналітичні дашборди та системи допомоги при прийнятті рішень. Прикладний шар перетворює отримані цифрові дані на зрозумілу та структуровану інформацію, яку можна використати для нагляду, аналізу та управління різними процесами. Завдяки прикладному програмному забезпеченню користувач може контролювати стан системи, коригувати її параметри, отримувати сповіщення та створювати автоматизовані сценарії роботи IoT-пристроїв [10].

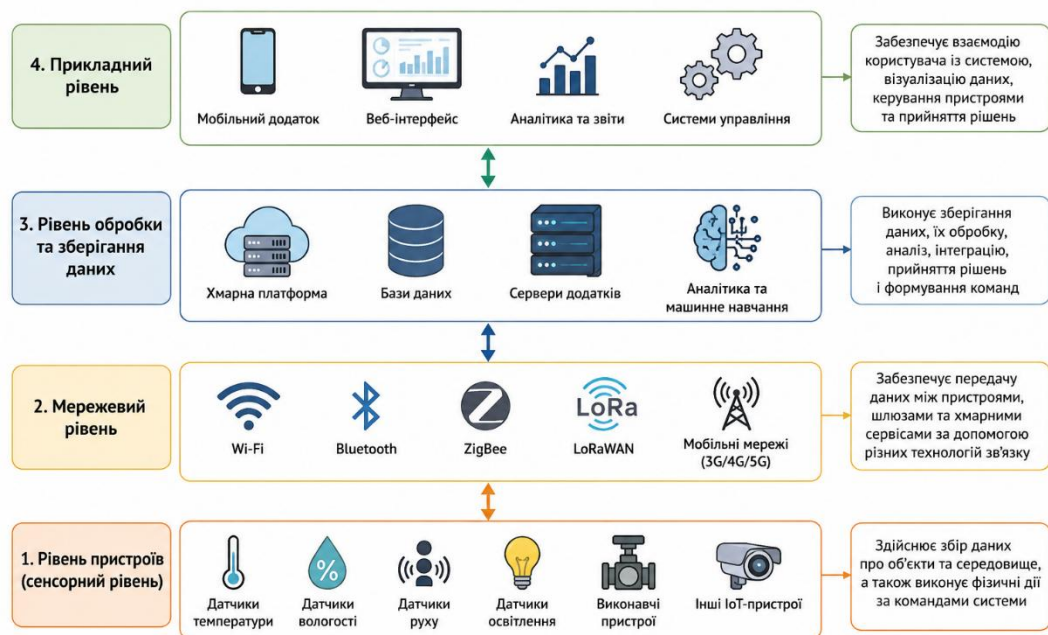


Рисунок 1.3 – Структура IoT-системи

Життєво необхідною складовою сучасних систем Інтернету речей (IoT) виступають платформи, призначені для управління, котрі дають змогу здійснювати централізоване адміністрування як кінцевими пристроями, так і потоками інформації. Такі комплекси програмного забезпечення втілюють у собі функції нагляду, аналітичну обробку, прогнозування, автоматичне реагування на актуальні події та інтеграцію з іншими існуючими інформаційними мережами. Крім того, платформи IoT створюють передумови для забезпечення взаємодії різнорідних пристроїв, підтримки розширення (масштабування) системи та спрощення її початкового налаштування [25]. Один із ключових моментів у конструюванні систем IoT полягає у гарантуванні їхньої

захищеності та стійкості. З огляду на те, що IoT-системи обробляють значні обсяги інформації, серед якої можуть фігурувати дані, що потребують конфіденційності, впровадження дієвих механізмів охорони відомостей набуває першочергового значення. До базових методів захисту відносять криптографічне перетворення даних, верифікацію (автентифікацію) пристроїв, встановлення контролю доступу, системи для виявлення несанкціонованих проникнень та моніторинг активності у мережі. Забезпечення належного захисту є безумовною вимогою для стабільної роботи IoT-систем та їхньої оборони від кібернетичних атак [11].

Не менш вагомими характеристиками, які має мати архітектура IoT, є її еластичність, модульність та потенціал до необмеженого збільшення. Сучасні системи Інтернету речей зобов'язані бути здатними адаптуватися до зростання кількості підключень, коливань робочого навантаження та появи нових функціональних потреб. Цього можливо досягти за рахунок застосування уніфікованих протоколів для обміну інформацією, структури системи, побудованої на модульному принципі, а також шляхом інтеграції рішень, базованих на хмарних обчисленнях [19].

Підсумовуючи, архітектурна побудова IoT-систем являє собою багатошарову, взаємопов'язану структуру, що охоплює сенсорний рівень, мережевий, рівень обробки даних та прикладний рівень. Кожен із цих компонентів виконує чітко визначені функції та забезпечує повний життєвий цикл роботи з даними — від їхнього збору та передачі до аналізу, ухвалення рішень і виконання команд управління. Комплексна взаємодія всіх цих складових дає змогу створювати високоефективні, масштабовані та гнучкі IoT-системи, які здатні забезпечити високий рівень автоматизації процесів у різноманітних галузях діяльності.

1.4 Висновки до розділу 1

У першому розділі дипломної роботи було проведено системний аналіз теоретичних основ Інтернету речей, розкрито сутність та ключові поняття IoT, а також досліджено його структуру та основні компоненти.

1. Визначено, що Інтернет речей є багаторівневою інформаційно-комунікаційною системою, яка інтегрує фізичні об'єкти, сенсори, програмне забезпечення та мережеві технології для автоматизованого збору, передачі та обробки даних без безпосередньої участі людини. Ключовими характеристиками IoT визначено масштабованість, гетерогенність, автономність та здатність до аналізу даних у реальному часі.

2. Проаналізовано основні напрями застосування IoT-технологій, які охоплюють промисловість (Індустрія 4.0), «розумні міста», охорону здоров'я, аграрний сектор, транспорт, енергетику та житлово-комунальне господарство. Встановлено, що впровадження IoT сприяє підвищенню ефективності управління, оптимізації використання ресурсів та покращенню якості життя населення.

3. Досліджено структуру IoT-систем, яка складається з чотирьох основних рівнів: сенсорного (фізичні пристрої та актуатори), мережевого (технології передачі даних), рівня обробки та зберігання даних (хмарні платформи, edge computing) та прикладного рівня (користувацькі інтерфейси). Показано, що ефективна взаємодія всіх рівнів забезпечує повний життєвий цикл роботи з даними та є основою для створення гнучких і масштабованих IoT-рішень.

2 ОСОБЛИВОСТІ ПОБУДОВИ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Принципи організації IoT-мереж

Побудова мереж Інтернету Речей (IoT) спирається на низку фундаментальних засад, що гарантують їхню ефективність, стабільність, захищеність та здатність до взаємодії між великою кількістю різноманітного обладнання. На відміну від класичних комп'ютерних мереж, які вирізняються доволі фіксованою структурою та обмеженою кількістю з'єднаних точок, мережі IoT є високодинамічними, надзвичайно масштабними, включають різноманітні технологічні рішення та оперують пристроями з обмеженими ресурсами. Це вимагає запровадження абсолютно нових архітектурних рішень, які б враховували специфіку роботи таких систем та забезпечували їхнє належне впровадження у сучасний цифровий простір [3; 13].

Один із наріжних каменів архітектури IoT — це масштабованість, тобто здатність системи зберігати високу продуктивність попри безперервне нарощування числа підключених одиниць. В умовах сучасного стрімкого зростання кількості вузлів IoT, конче необхідно розробляти такі архітектурні моделі, які дозволять безперешкодно інтегрувати нові пристрої, не погіршуючи загальну працездатність. Масштабованість реалізується завдяки застосуванню модульних та ієрархічних побудов, впровадженню хмарних обчислень, а також використанню розподілених систем для обробки даних, що забезпечує ефективне управління гігантськими потоками інформації та підтримує стабільність інфраструктури навіть при її суттєвому розширенні [19].

Ключовим елементом є також принцип інтероперабельності, який забезпечує взаємодію між різними апаратами, технологіями та програмними оболонками в межах єдиної мережі IoT. Оскільки в Інтернеті Речей об'єднуються вироби від різних виробників, які можуть оперувати несинхронізованими протоколами та інтерфейсами, життєво необхідним є застосування уніфікованих стандартів, що гарантують їхню коректну комунікацію. Інтероперабельність сприяє формуванню цілісної системи, де всі

складові елементи можуть працювати злагоджено, що є незамінною передумовою для розвитку та розширення систем IoT [18].

Наступний принцип — енергоефективність, що має критично важливе значення для переважної більшості пристроїв IoT. Значна частина апаратних засобів працює від акумуляторів, що обмежує тривалість їхньої автономної роботи. Через це виникає потреба в оптимізації енергоспоживання шляхом використання спеціалізованих протоколів передачі інформації, активації режимів економії енергії, вдосконалення алгоритмів обробки даних та зменшення частоти комунікаційних сесій. Підвищення енергоефективності продовжує автономність пристроїв, скорочує витрати на їхнє обслуговування та покращує загальну операційну спроможність мережі IoT [7].

Принцип стійкості до відмов та надійності є фундаментальним для організації мереж IoT, адже такі системи часто функціонують у середовищах, де навіть мінімальні збої можуть мати серйозні наслідки. Надійність означає, що система здатна безперебійно виконувати свої функції, навіть якщо окремі її складові виходять з ладу. Для досягнення цього застосовуються механізми резервування шляхів зв'язку, дублювання вузлів, рівномірного розподілу навантаження, а також системи самовідновлення, що мінімізують вплив аварій на функціонування мережевої інфраструктури [13].

Особливого значення набуває аспект безпеки, що охоплює весь комплекс заходів, спрямованих на захист інформації, апаратури та каналів зв'язку від несанкціонованого доступу та кіберзагроз. У мережах IoT впроваджуються різноманітні методи захисту, зокрема шифрування даних, підтвердження автентичності пристроїв, контроль доступу, а також системи моніторингу та виявлення потенційних загроз. Водночас, з огляду на обмежені ресурси багатьох IoT-пристроїв, надзвичайно важливим є створення дієвих, але низьковитратних у плані ресурсів, методів забезпечення безпеки, які не створюють зайвого навантаження на систему [11; 12].

Важливим принципом побудови IoT-мереж є децентралізація обробки інформації, яка передбачає розподіл обчислювальних завдань між різними

рівнями мережевої структури. На противагу класичним моделям із централізованим управлінням, у IoT значна частка обробки даних може відбуватися безпосередньо на самих пристроях або на периферичних вузлах. Використання технологій граничних обчислень (edge computing) дозволяє зменшити затримки при передачі даних, знизити навантаження на хмарні сервіси та прискорити реакцію системи на зміни в оточенні [19].

Окрім того, вагомим принципом є адаптивність IoT-мереж, яка полягає у спроможності системи динамічно змінювати свої операційні параметри згідно з умовами експлуатації. Це включає автоматичне регулювання режимів роботи апаратних засобів, вибір оптимальних маршрутів для передачі даних, пристосування до змін навколишнього середовища та врахування індивідуальних особливостей користувачів. Адаптивність забезпечує підвищення загальної ефективності функціонування системи та її гнучкість у різноманітних обставинах [18].

Не менш значущим є принцип гарантування якості обслуговування (QoS), який вимагає підтримки необхідного рівня ключових мережевих параметрів, таких як швидкість передачі, латентність (затримка), пропускна здатність та стабільність з'єднання. Вимоги до цих параметрів можуть суттєво варіюватися залежно від сфери застосування IoT-систем, що диктує необхідність застосування ефективних механізмів управління ресурсами мережі та відповідної пріоритезації трафіку. Забезпечення належного рівня QoS є критичною умовою для стабільного функціонування IoT, особливо у сферах, що вимагають високої відповідальності [3].

Отже, організація мереж IoT спирається на сукупність взаємозалежних засад, серед яких центральне місце посідають масштабованість, інтеоперабельність, енергоефективність, надійність, безпека, децентралізація, адаптивність та гарантування якості обслуговування. Комплекс цих принципів формує підґрунтя для створення функціональних, гнучких, розширюваних та захищених мереж Інтернету Речей, здатних ефективно працювати в умовах

зростаючого навантаження, різноманіття апаратури та постійної динаміки цифрового середовища.

2.2 Технології передачі даних у IoT (Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NB-IoT та інші)

Передача даних є одним із ключових елементів функціонування мереж Інтернету речей, оскільки саме вона забезпечує взаємодію між сенсорами, контролерами, шлюзами, хмарними платформами та користувацькими сервісами. Від характеристик каналу зв'язку залежить швидкість обміну інформацією, стабільність функціонування мережі, енергоспоживання пристроїв, затримка передачі та можливість масштабування IoT-системи. У сучасних IoT-мережах використовуються різні технології передачі даних, кожна з яких має власну структуру мережі, технічні характеристики, переваги, недоліки та сфери практичного застосування.

Технологія Wi-Fi є однією з найбільш поширених у системах Інтернету речей, особливо у сфері «розумного дому», відеоспостереження та мультимедійних сервісів. Основною перевагою Wi-Fi є висока швидкість передачі даних, що може досягати 100–600 Mbps залежно від стандарту IEEE 802.11. Радіус дії мережі зазвичай становить до 50 м у приміщенні та до 100 м на відкритій місцевості. Технологія працює переважно у частотних діапазонах 2,4 GHz та 5 GHz. Структура IoT-мережі на основі Wi-Fi має зіркоподібну топологію, у якій сенсори та пристрої підключаються до центрального маршрутизатора або точки доступу. Приклад побудови такої мережі наведено на рисунку 2.2.

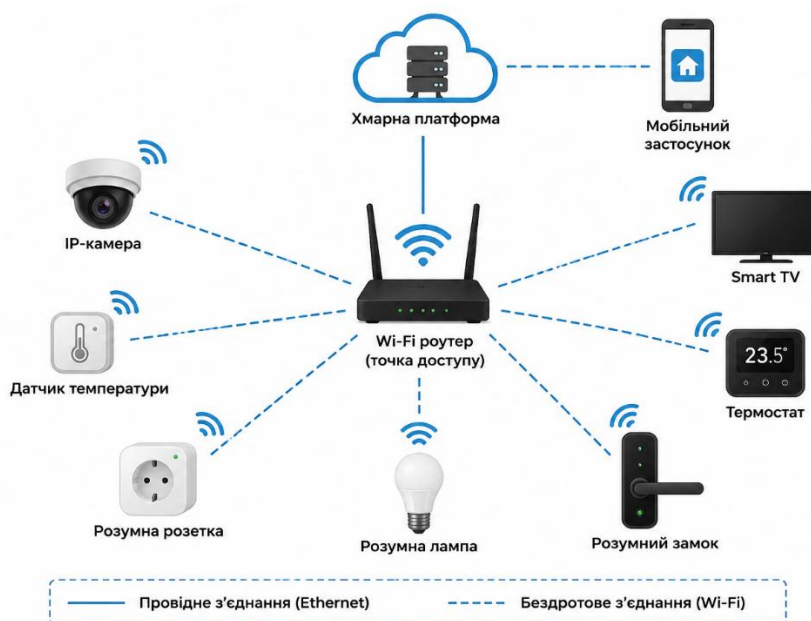


Рисунок 2.2 – Приклад структури IoT-мережі на основі Wi-Fi

До переваг Wi-Fi належать висока швидкість передачі даних, простота інтеграції у наявну мережеву інфраструктуру та підтримка великої кількості пристроїв. Недоліками технології є значне енергоспоживання, підвищене навантаження на мережу при великій кількості підключень та обмежений час автономної роботи пристроїв.

Bluetooth Low Energy (BLE) використовується переважно у системах персонального моніторингу, медичних сенсорах, носимих пристроях та системах автоматизації. Технологія працює у діапазоні 2,4 GHz та забезпечує швидкість передачі даних до 2 Mbps. Радіус дії BLE зазвичай становить 10–50 м залежно від потужності передавача. Основною особливістю BLE є низьке енергоспоживання, що дозволяє пристроям працювати від батареї протягом декількох місяців або навіть років.

Структура BLE-мережі зазвичай базується на топології «зірка», де центральний пристрій взаємодіє з периферійними сенсорами. Приклад побудови мережі BLE наведено на рисунку 2.3.

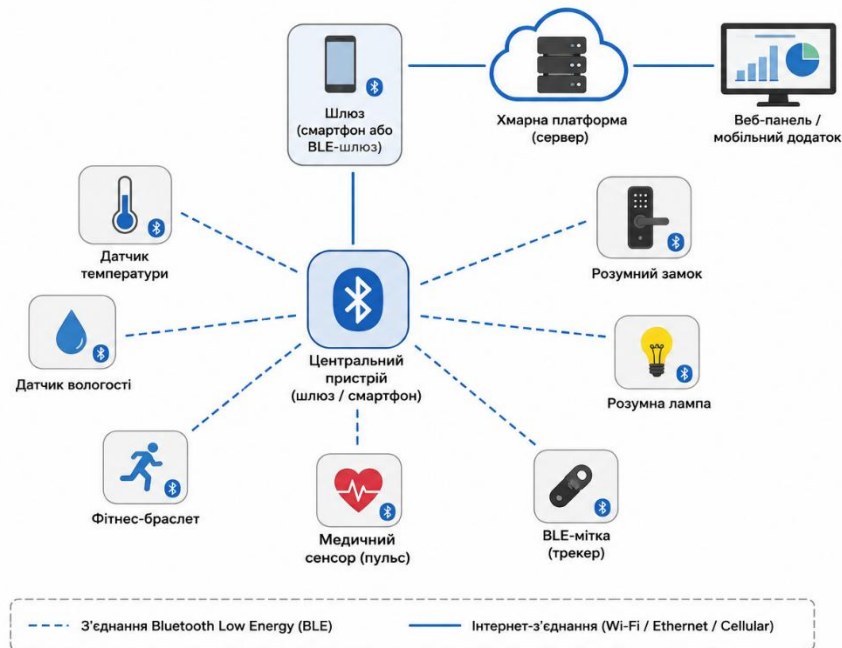


Рисунок 2.3 – Структура IoT-мережі на основі Bluetooth Low Energy

Перевагами BLE є низьке енергоспоживання, невисока вартість реалізації та простота інтеграції. До недоліків належать невеликий радіус дії та обмежена пропускна здатність, що ускладнює використання технології у великих IoT-мережах.

Технологія ZigBee призначена для створення енергоефективних IoT-мереж із великою кількістю пристроїв. Вона працює у діапазоні 2,4 GHz та забезпечує швидкість передачі даних до 250 kbps. Радіус дії одного вузла зазвичай становить 10–100 м. Основною особливістю ZigBee є підтримка mesh-топології, у якій дані можуть передаватися через проміжні вузли мережі.

Структура ZigBee-мережі складається з координатора, маршрутизаторів та кінцевих пристроїв. Приклад побудови mesh-мережі ZigBee наведено на рисунку 2.4.

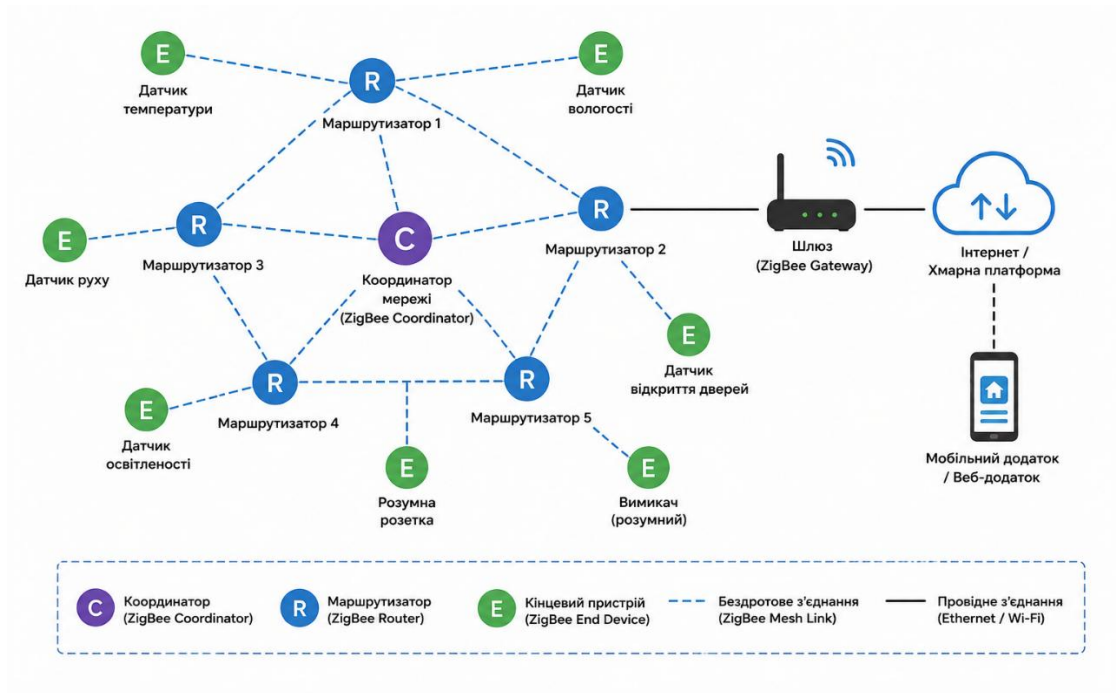


Рисунок 2.4 – Mesh-топологія IoT-мережі ZigBee

Перевагами ZigBee є низьке енергоспоживання, можливість масштабування та підвищена надійність завдяки mesh-топології. Недоліками є невисока швидкість передачі даних та можливі затримки при передачі інформації через декілька вузлів.

LoRaWAN є технологією LPWAN (Low Power Wide Area Network), призначеною для передачі даних на великі відстані при мінімальному енергоспоживанні. Швидкість передачі даних становить від 0,3 kbps до 50 kbps, а дальність зв'язку може досягати 2–5 км у міських умовах та до 15 км у сільській місцевості. Технологія працює у діапазонах 433 MHz, 868 MHz та 915 MHz.

Структура LoRaWAN-мережі базується на топології «star-of-stars», де кінцеві пристрої передають дані на gateway, який забезпечує зв'язок із мережевим сервером та хмарною платформою. Приклад побудови LoRaWAN-мережі наведено на рисунку 2.5.

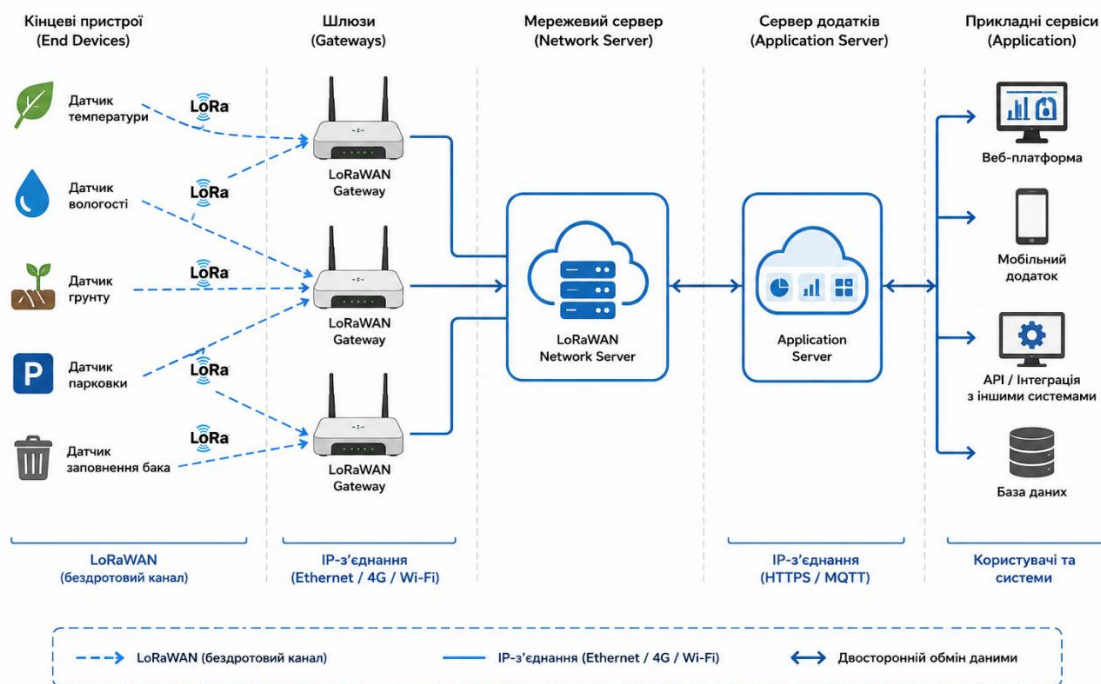


Рисунок 2.5 – Структура LoRaWAN-мережі

Перевагами LoRaWAN є велика дальність зв'язку, мінімальне енергоспоживання та можливість роботи великої кількості сенсорів. Недоліками є низька швидкість передачі даних та неможливість передавання великих обсягів інформації у режимі реального часу.

NB-IoT є технологією стільникового зв'язку, розробленою спеціально для IoT-систем. Вона функціонує на базі LTE-мереж операторів мобільного зв'язку та забезпечує швидкість передачі даних до 250 kbps. Радіус покриття залежить від інфраструктури оператора та може охоплювати значні території.

Архітектура NB-IoT-мережі передбачає підключення сенсорів до базової станції оператора мобільного зв'язку з подальшою передачею інформації до серверів обробки даних. Приклад структури мережі NB-IoT наведено на рисунку 2.6.

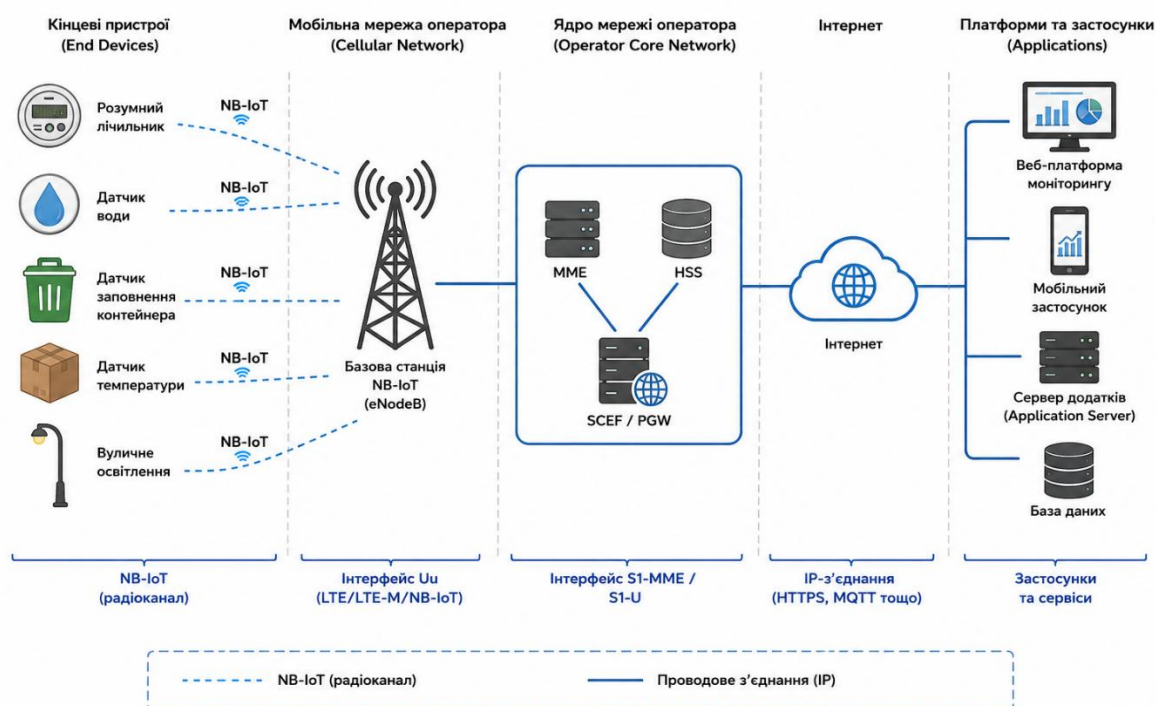


Рисунок 2.6 – Структура мережі NB-IoT

Основними перевагами NB-IoT є широке покриття, висока стабільність зв'язку та підтримка великої кількості пристроїв. Недоліками є залежність від інфраструктури мобільних операторів та вищі енергетичні витрати порівняно з LoRaWAN або ZigBee.

Для порівняння основних характеристик технологій передачі даних у IoT доцільно використати таблицю 2.2.

Таблиця 2.2 – Порівняння технологій передачі даних у IoT

Технологія	Частота	Радіус дії	Швидкість передачі	Топологія	Енергоспоживання	Основні сфери застосування
Wi-Fi	2,4 / 5 GHz	50–100 м	100–600 Mbps	Star	Високе	Smart Home, відеоспостереження
BLE	2,4 GHz	10–50 м	до 2 Mbps	Star	Низьке	Wearable devices, медичні сенсори
ZigBee	2,4 GHz	10–100 м	до 250 kbps	Mesh	Дуже низьке	Автоматизація будівель

Продовження таблиці 2.2.

LoRaWAN	433 / 868 / 915 MHz	2–15 км	0,3–50 kbps	Star-of-stars	Дуже низьке	Smart City, агросектор
NB-IoT	LTE bands	До 35 км	до 250 kbps	Cellular	Середнє	Промисловість, логістика
LTE-M	LTE bands	До 10 км	до 1 Mbps	Cellular	Середнє	Транспорт, мобільний IoT
5G IoT	Sub-6 GHz / mmWave	До декількох км	до 10 Gbps	Cellular	Високе	Industrial IoT, автономний транспорт

Таким чином, різні технології передачі даних у мережах Інтернету речей мають суттєві відмінності у структурі побудови мереж, швидкості передачі, енергоспоживанні, дальності зв'язку та можливостях масштабування. Вибір конкретної технології залежить від вимог IoT-системи, кількості пристроїв, необхідної швидкості передачі даних, умов експлуатації та економічної доцільності впровадження.

2.3 Особливості функціонування IoT-мереж

Експлуатація мереж Інтернету речей (IoT) має низку специфічних рис, які суттєво відрізняють їх від звичних систем комунікації та інформаційного обміну, вимагаючи впровадження новітніх методологій у процесах проєктування, реалізації та подальшого супроводу. Ці відмінності зумовлені, перш за все, надзвичайною масштабністю розгортання IoT-інфраструктури, різноманітністю апаратної бази, обмеженими можливостями окремих пристроїв, а також потребою в неперервній обробці величезних масивів даних з мінімальними часовими затримками, наближеними до реального часу. В умовах сучасного технологічного прогресу IoT постає як складна, багатогранна система, що об'єднує фізичний та віртуальний світи, сприяючи їхній взаємодії через автоматизований інформаційний обмін [18; 19].

Однією з наріжних рис мереж IoT є їхня масовість, що припускає одночасну роботу великої кількості апаратних одиниць, які генерують, передають і опрацьовують інформацію. У таких мережах кількість підключених вузлів може сягати мільйонів, а то й мільярдів, створюючи значний тиск на мережеве забезпечення. Це, у свою чергу, диктує необхідність застосування високоефективних методів керування трафіком, оптимізації передачі даних, розподілу навантаження та впровадження архітектурних рішень здатних до масштабування. Масовий характер IoT також обумовлює потребу у впровадженні автоматизованих систем управління мережею, які здатні підтримувати стабільність роботи навіть за умов суттєвого збільшення кількості підключених пристроїв [13].

Іншою важливою характеристикою мереж IoT є їхня гетерогенність, яка проявляється у залученні широкого спектру різнорідних пристроїв, протоколів зв'язку, програмних платформ і стандартів. В межах однієї IoT-системи можуть функціонувати одночасно сенсорні вузли, виконавчі механізми, мобільні термінали, серверні рішення та хмарні сервіси, які різняться за технічними параметрами, функціоналом та обчислювальною потужністю. Така різноплановість ускладнює інтеграцію складових системи та вимагає забезпечення їхньої сумісності, інтероперабельності та узгодженої взаємодії, що є критично важливим для ефективного функціонування IoT-мереж [3].

Суттєвою рисою IoT-мереж є обмеженість ресурсів більшості пристроїв, що їх складають. Багато IoT-апаратів відзначаються низькою обчислювальною спроможністю, дефіцитом оперативної та постійної пам'яті, а також залежністю від автономних джерел енергоживлення. Це ставить серйозні рамки для реалізації складних алгоритмів опрацювання даних, протоколів безпеки та механізмів мережевого управління. З огляду на це, виникає потреба у розробці оптимізованих, енергоефективних рішень, що дозволяють досягти балансу між наявним функціоналом та затратами ресурсів [7].

Важливим аспектом роботи IoT-мереж є потреба в обробці даних у режимі, близькому до реального часу, або з мінімальними затримками, що

зумовлене специфікою їхнього застосування. У таких галузях, як транспорт, охорона здоров'я, промисловість чи системи безпеки, швидкість реакції на зміни умов середовища є критично значущою. Для забезпечення оперативної обробки інформації застосовуються технології периферійних обчислень (edge computing), які дають змогу виконувати опрацювання безпосередньо на пристроях чи поблизу місця виникнення даних. Це допомагає зменшити затримки в передачі, знизити навантаження на мережу та підвищити загальну продуктивність системи [19].

Ще однією помітною характеристикою IoT-мереж є їхня розподіленість, що передбачає виконання обчислювальних процесів на різних рівнях архітектури системи. На відміну від класичних централізованих систем, де опрацювання інформації переважно відбувається на головних серверах, в IoT значна частина обчислювальних завдань може виконуватися безпосередньо на апаратах або на проміжних вузлах мережі. Такий підхід сприяє зростанню продуктивності, зменшенню затримок у передаванні даних, а також підвищенню стійкості системи до виходу з ладу окремих елементів [18].

Не менш важливим є аспект мобільності пристроїв, який полягає у їхній здатності змінювати своє місцезнаходження під час функціонування мережі. Це типово для транспортних систем, логістичних рішень, портативних гаджетів та інших рухомих об'єктів. Мобільність ускладнює процеси маршрутизації даних, управління мережею та підтримання стабільного зв'язку, що вимагає використання адаптивних алгоритмів та динамічних протоколів, здатних ефективно працювати в умовах постійної трансформації топології мережі [3].

Особливістю мереж IoT є також підвищені вимоги до забезпечення їхньої надійності та безперервності функціонування. У багатьох випадках IoT-системи використовуються у критично важливих сферах, де навіть незначні збої можуть мати серйозні наслідки. Тому важливим є впровадження механізмів резервування, тиражування даних, балансування навантаження, а також систем самовідновлення, які забезпечують безперебійну роботу навіть у разі виходу з ладу окремих компонентів системи [13].

Окрім того, вагомою особливістю є потреба в обробці великих обсягів інформації, які генеруються пристроями IoT під час їхньої роботи. Ці дані характеризуються високою швидкістю надходження, різноманітністю форматів та значним обсягом, що вимагає застосування передових технологій для зберігання, опрацювання та аналізу інформації. Використання хмарних сервісів, технологій Big Data та методів інтелектуального аналізу дозволяє ефективно працювати з такими даними, видобувати корисні відомості та застосовувати їх для управлінських рішень [19].

Важливою рисою мереж IoT є також посилені вимоги до забезпечення їхньої безпеки. Велика кількість підключених пристроїв, відкритий характер мережі та використання бездротових технологій створюють додаткові ризики, пов'язані з можливістю несанкціонованого доступу, перехоплення інформації та здійснення кібератак. У зв'язку з цим, необхідним є впровадження комплексних механізмів захисту даних, що включають шифрування, автентифікацію пристроїв, контроль доступу та моніторинг стану мережі [11].

Таким чином, функціонування мереж IoT визначається сукупністю взаємопов'язаних рис: масовість, гетерогенність, обмеженість ресурсів апаратури, потреба в обробці даних у реальному часі, розподілений характер, мобільність, а також підвищені вимоги до надійності та безпеки. Саме ці характеристики окреслюють специфіку побудови, експлуатації та розвитку сучасних систем Інтернету речей, а також вимагають застосування комплексних, гнучких та інноваційних підходів до їхньої реалізації у різних сферах діяльності.

2.4 Проблеми безпеки та надійності IoT-систем

Бурхливий розвиток Інтернету речей тягне за собою не лише значне розширення можливостей інформаційно-комунікаційних систем, а й істотне зростання загроз, пов'язаних із гарантуванням їхньої безпеки та стабільності. В умовах нинішньої цифровізації IoT постає як складна, децентралізована та

мінлива система, що об'єднує чимало різнорідних апаратних засобів, які обмінюються даними через мережеву основу. Специфічні риси IoT-мереж, такі як їхня масштабність, різнорідність, відсутність централізованого управління та обмеження ресурсів пристроїв, створюють додаткові труднощі для забезпечення належного рівня захисту відомостей, стабільності роботи систем та їхньої несприйнятливості до зовнішніх та внутрішніх небезпек. З огляду на це, питання кібербезпеки та надійності IoT-систем набувають першочергового значення та вимагають багатоаспектного наукового підходу до їх розв'язання [11; 12].

Однією з головних загроз для IoT-систем є вразливість апаратних засобів до несанкціонованого доступу, що зумовлене їхніми технічними характеристиками. Багато IoT-пристроїв мають спрощену конструкцію, обмежені потужності обчислення та енергоспоживання, що значно ускладнює імплементацію складних методів захисту, типових для традиційних інформаційних платформ. Як наслідок, подібні пристрої часто використовують базові або навіть стандартні налаштування безпеки, що робить їх потенційно схильними до атак. Зловмисники можуть скористатися цими слабкими місцями для отримання доступу до конфіденційних даних, захоплення контролю над системою або використання пристроїв у складі ботнетів для проведення масштабних кібератак [11].

Серйозною небезпекою для IoT-систем також є ризик перехоплення, фальсифікації чи зміни даних під час їхньої трансляції. Оскільки IoT-мережі активно задіюють бездротові методи зв'язку, передані відомості можуть стати доступними для третіх осіб, особливо за умов браку належного шифрування. Це створює загрозу не лише витоку приватної інформації, а й спотворення даних, що може призвести до хибних управлінських рішень та порушення функціональності системи. У життєво важливих сферах застосування, таких як охорона здоров'я чи промисловість, це може мати серйозні наслідки [12].

Ще однією суттєвою проблемою є відсутність єдиних уніфікованих критеріїв безпеки для пристроїв та мереж IoT. Велика кількість виробників

застосовує власні інженерні рішення та протоколи, що спричиняє значну фрагментацію ринку та нерівномірність рівня захисту різних складових системи. За таких умов забезпечення всеосяжної безпеки IoT-мереж стає складним завданням, адже навіть один недостатньо захищений елемент може стати точкою проникнення для атаки на всю систему. Відсутність уніфікації також ускладнює процеси інтеграції, управління та моніторингу безпеки платформи [16].

Важливим аспектом забезпечення стійкості IoT-систем є питання підтвердження достовірності та ідентифікації пристроїв, що набуває особливої складності у великих розподілених мережах. Необхідність гарантування унікальності ідентифікатора для кожного пристрою та контролю доступу до ресурсів системи вимагає впровадження надійних механізмів аутентифікації. Недостатній рівень захисту на цьому етапі може спричинити підключення неприпустимих пристроїв, що, своєю чергою, створює небезпеку порушення цілісності та конфіденційності даних, а також стабільності роботи системи [11].

Окрім того, вагому загрозу для IoT-мереж становлять напади типу «заперечення обслуговування» (DoS та DDoS), націлені на перевантаження мережевих ресурсів і виведення системи з ладу. Особливість IoT полягає у величезній кількості підключених пристроїв, які можуть бути використані для організації розподілених атак, здатних паралізувати функціонування навіть великих інформаційних платформ. У контексті критично важливих галузей, як-от транспорт, енергетика чи медицина, наслідки подібних атак можуть бути вкрай небезпечними та мати значний соціально-економічний вплив [12].

Окрему проблему становить гарантування приватності персональних відомостей, які обробляються IoT-системами. Сучасні IoT-пристрої здатні накопичувати великі обсяги інформації про користувачів, включаючи моделі їхньої поведінки, звички, географічне розташування та навіть фізіологічні параметри. У разі недостатнього захисту такі дані можуть бути використані сторонніми суб'єктами з порушенням прав користувачів, що створює серйозні ризики для приватності та інформаційної безпеки [23].

Поруч із викликами безпеки, не менш значущим є аспект забезпечення стійкості функціонування IoT-систем, що визначається їхньою здатністю безперервно виконувати свої функції навіть при наявності збоїв чи виходів з ладу окремих елементів. З огляду на це, особливої ваги набуває впровадження механізмів резервування, дублювання даних, розподілу навантаження та автоматичного відновлення працездатності системи. Застосування таких підходів дозволяє підвищити відмовостійкість системи та забезпечити її стабільну роботу за різних умов експлуатації [13].

Ще одним суттєвим викликом у роботі IoT-мереж є нестійкість з'єднання, що може бути викликана використанням бездротових технологій передачі інформації, впливом зовнішніх факторів, таких як електромагнітні перешкоди, погодні умови чи фізичні бар'єри, а також перевантаженням мережевої інфраструктури. У середовищі, де велика кількість пристроїв одночасно генерує та передає дані, навіть невеликі порушення у функціонуванні мережі можуть спричинити значні збої у роботі системи. Це проявляється як втрата даних, затримки у їх трансляції, зниження точності аналітики та загальне погіршення результативності IoT-рішень [3].

Особливо критичними наслідки нетривкого з'єднання є для систем, що працюють у режимі реального часу, де швидкість та точність передачі відомостей є вирішальними. У таких випадках навіть короточасні перерви можуть призвести до некоректного ухвалення рішень, виходу з ладу обладнання або втрати управління системою. Крім того, нестабільність мережі ускладнює синхронізацію даних між різними складовими системи, що може спричинити їхню несумісність чи порушення цілісності інформації.

Для підвищення рівня захищеності та надійності IoT-систем застосовується сукупність взаємопов'язаних технічних та управлінських кроків. Одним із ключових засобів є використання криптографічних методів захисту, зокрема шифрування даних як під час передачі, так і при їхньому зберіганні. Це дає змогу забезпечити конфіденційність відомостей, їхню цілісність та захист від несанкціонованого доступу. Важливим доповненням є запровадження

багаторівневої аутентифікації, яка гарантує перевірку достовірності пристроїв та користувачів перед наданням доступу до системи [11].

Ключову роль у гарантуванні захищеності систем Інтернету речей (IoT) відіграє застосування протоколів передачі даних, котрі мають вбудовані архітектури безпеки. Йдеться про впровадження новітніх криптографічних методів для шифрування, а також інструментів, що підтверджують цілісність даних, захист від повторних запитів та несанкціонованого втручання. Сперте на такі протоколи, досягається гарантія конфіденційності інформації, що циркулює, унеможлиблюється її несанкціонована зміна чи спотворення, і забезпечується достовірність даних, якими обмінюються компоненти IoT-мережі. Актуальність цього зростає особливо там, де комунікація відбувається через загальнодоступні чи частково відкриті мережі, де ризик перехоплення даних значно вищий. Крім того, життєво необхідним для підтримання високого рівня захисту є регулярне оновлення програмного забезпечення. Це дозволяє своєчасно усувати виявлені слабкі місця, удосконалювати захисні механізми та адаптувати систему до нових загроз кіберпростору. Не менш вагомим є розгортання систем безперервного нагляду, які моніторять стан мережі у режимі реального часу, даючи змогу миттєво фіксувати відхилення, ідентифікувати потенційні небезпеки та адекватно реагувати, що різко підвищує загальну захищеність IoT-середовищ [16].

Окрім технічних рішень, значний вплив мають організаційні процедури, які є невіддільною частиною цілісної системи забезпечення безпеки. До таких кроків належать формулювання та впровадження внутрішніх регламентів та політик безпеки, встановлення чітких правил доступу до ресурсів системи, контроль за використанням обладнання, а також імплементація визнаних світових стандартів кіберзахисту. Важливим моментом є також підвищення обізнаності кінцевих користувачів щодо існуючих ризиків, правил безпечної експлуатації IoT-пристроїв та базових принципів кібергігієни. Формування культури безпечного поведіння з цифровими технологіями суттєво знижує кількість інцидентів, спричинених людським фактором. Отже, синергія

технічних та управлінських заходів формує надійний захисний комплекс, що мінімізує вразливості та збільшує ефективність роботи IoT-систем у різноманітних експлуатаційних умовах.

Стійкість IoT-систем додатково підсилюється завдяки задіянню механізмів резервування каналів зв'язку, дублюванню критично важливих вузлів, застосуванню архітектур підвищеної відмовостійкості та оптимізації мережевого трафіку. Резервні лінії для обміну даними дають змогу використовувати альтернативні шляхи передачі інформації у разі виходу з ладу основного каналу, тим самим забезпечуючи безперебійність функціонування системи. Дублювання ключових інфраструктурних елементів, як-от сервери, контролери чи обчислювальні вузли, гарантує працездатність системи навіть за умови часткових аварій. Використання архітектур, стійких до збоїв (зокрема розподілених або кластерних рішень), підвищує рівень надійності та знижує імовірність тотальної відмови. Водночас, оптимізація мережевого трафіку сприяє зменшенню завантаження мережі, мінімізації затримок у передачі даних та підвищенню загальної продуктивності роботи IoT-мереж. Сукупність цих дій забезпечує підвищену життєстійкість систем перед лицем як внутрішніх технічних проблем, так і зовнішніх деструктивних впливів.

Таким чином, питання безпеки та надійності IoT-систем постають як одні з центральних та визначальних викликів у їхньому сучасному розвитку, оскільки вони прямо пропорційні результативності, стабільності та захищеності функціонування відповідних технологічних рішень. Для їх успішного вирішення потрібен комплексний, системний та багатовекторний підхід, який інтегрує апаратні засоби захисту, організаційно-адміністративні заходи та неухильне дотримання міжнародних стандартів та нормативних вимог у царині кібербезпеки. Забезпечення належного рівня захисту відомостей, стійкості до відмов, безперервності роботи та здатності до адаптації IoT-мереж є необхідною передумовою для їх ефективного впровадження, масштабування та подальшого прогресу в умовах нинішнього цифрового середовища. У майбутньому це

стимулюватиме зростання довіри до технологій IoT, розширення ареалів їхнього застосування та формування безпечного інформаційного простору.

2.5 Висновки до розділу 2

У другому розділі роботи досліджено особливості побудови мереж Інтернету речей, принципи їх організації, технології передачі даних, а також проблеми безпеки та надійності.

1. Визначено фундаментальні принципи організації IoT-мереж: масштабованість, інтероперабельність, енергоефективність, стійкість до відмов, безпека, децентралізація обробки даних, адаптивність та забезпечення якості обслуговування (QoS). Встановлено, що дотримання цих принципів є необхідною умовою для створення функціональних і надійних IoT-інфраструктур в умовах постійного зростання навантаження.

2. Проведено порівняльний аналіз сучасних технологій передачі даних в IoT (Wi-Fi, BLE, ZigBee, LoRaWAN, NB-IoT, LTE-M, 5G IoT) за такими критеріями: частотний діапазон, радіус дії, швидкість передачі, топологія, енергоспоживання та сфери застосування. Показано, що вибір конкретної технології залежить від вимог системи: Wi-Fi доцільний для високошвидкісних мультимедійних застосунків, ZigBee та BLE – для енергоефективних сенсорних мереж, LoRaWAN та NB-IoT – для передачі даних на великі відстані при мінімальному споживанні енергії.

3. Виявлено ключові проблеми безпеки та надійності IoT-систем, зокрема вразливість апаратних засобів, ризики перехоплення та фальсифікації даних, відсутність уніфікованих стандартів безпеки, загрози DDoS-атак, а також проблеми забезпечення приватності персональних даних. Обґрунтовано необхідність комплексного підходу до захисту, який поєднує криптографічні методи, багатофакторну автентифікацію, регулярне оновлення програмного забезпечення та організаційні заходи.

3 АНАЛІЗ ПРАКТИЧНОГО ЗАСТОСУВАННЯ ІОТ

3.1. Загальна характеристика обраної ІоТ-системи

Одним із найбільш поширених прикладів практичного застосування технологій Інтернету речей є система «розумного будинку» (Smart Home), яка об'єднує сенсори, виконавчі механізми, мережеве обладнання та програмне забезпечення в єдину ІоТ-мережу. Основним призначенням таких систем є автоматизація управління освітленням, опаленням, клімат-контролем, безпекою та побутовими пристроями, а також забезпечення дистанційного моніторингу та керування через мережу Інтернет.

Для практичного аналізу було обрано ІоТ-систему Smart Home, побудовану із використанням технологій Wi-Fi та ZigBee. Дана система включає центральний шлюз (gateway), сенсорні пристрої, виконавчі модулі, маршрутизатор Wi-Fi, хмарний сервер та мобільний застосунок для керування системою. Використання декількох технологій передачі даних дозволяє забезпечити оптимальне поєднання швидкості передачі інформації, енергоефективності та стабільності роботи мережі [22].

Практична структура ІоТ-системи Smart Home наведена на рисунку 3.1.

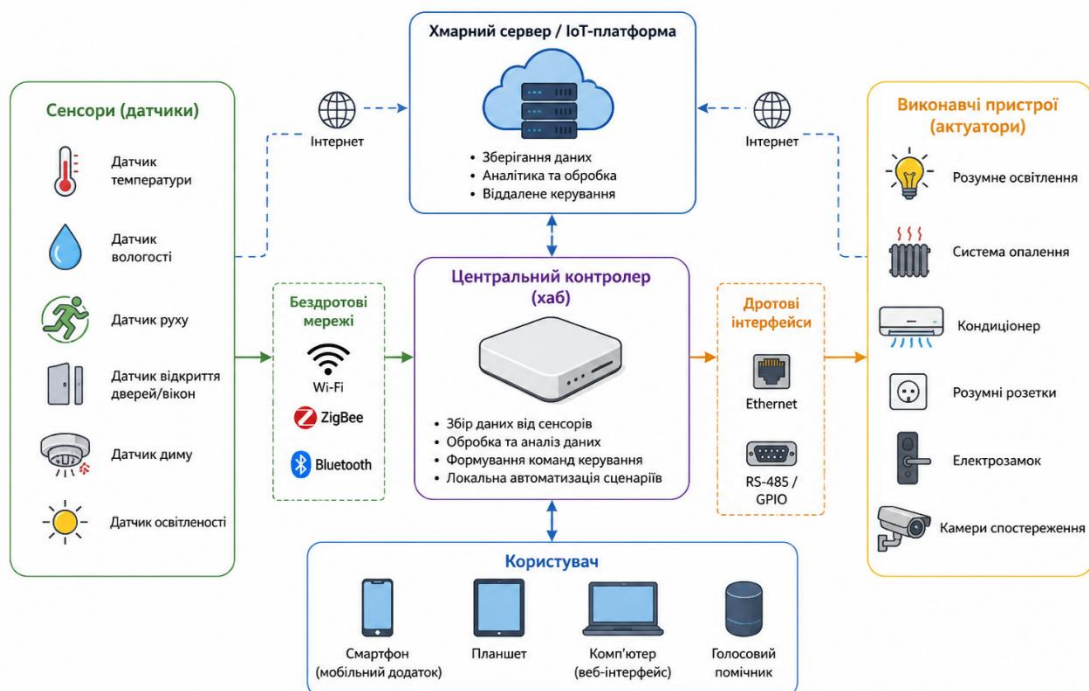


Рисунок 3.1 – Структура системи Smart Home

У структурі досліджуваної IoT-мережі використовуються датчики температури, вологості, руху, відкриття дверей, диму та протікання води. Сенсорні пристрої ZigBee підключаються до центрального gateway за mesh-топологією, що дозволяє забезпечити стабільність зв'язку та підтримку великої кількості пристроїв при низькому енергоспоживанні. Радіус дії ZigBee-пристроїв у межах приміщення становить 10–100 м, а швидкість передачі даних — до 250 kbps.

Пристрої, які потребують вищої швидкості передачі даних, зокрема IP-камери відеоспостереження, мультимедійні пристрої та мобільні термінали користувача, використовують мережу Wi-Fi. Швидкість передачі даних у Wi-Fi-мережі може становити 100–600 Mbps, що забезпечує передачу відеопотоку та швидкий обмін інформацією між пристроями системи. Недоліком Wi-Fi є підвищене енергоспоживання, тому дана технологія переважно застосовується для пристроїв із постійним живленням [24].

Центральним елементом системи є IoT-шлюз (gateway), який виконує функції координації мережі, збору інформації від сенсорів, обробки даних та передачі інформації до хмарного сервера. Gateway також забезпечує взаємодію між різними мережевими протоколами, оскільки ZigBee-пристрої не можуть напряму передавати дані через Wi-Fi-мережу. Таким чином, шлюз виконує роль проміжного вузла між локальною IoT-мережею та зовнішньою мережею Інтернет.

Хмарна платформа забезпечує зберігання інформації, аналітичну обробку даних, формування сценаріїв автоматизації та віддалений доступ користувача до системи. Передача інформації між gateway та cloud-сервером здійснюється через Wi-Fi-маршрутизатор та мережу Інтернет. Користувач взаємодіє із системою через мобільний застосунок, за допомогою якого можна переглядати стан сенсорів, змінювати параметри роботи системи та отримувати аварійні сповіщення [19].

У процесі практичного аналізу системи було визначено переваги комбінованого використання Wi-Fi та ZigBee у Smart Home. Використання

ZigBee для сенсорних пристроїв дозволяє зменшити енергоспоживання та збільшити час автономної роботи датчиків до декількох років без заміни елементів живлення. Використання Wi-Fi забезпечує високу швидкість передачі даних для мультимедійних пристроїв та віддаленого доступу до системи.

Разом із перевагами досліджувана система має і певні недоліки. Основними проблемами є залежність роботи системи від стабільності інтернет-з'єднання, можливі ризики кібербезпеки, несумісність обладнання різних виробників та необхідність регулярного оновлення програмного забезпечення. Крім того, велика кількість Wi-Fi-пристроїв може створювати додаткове навантаження на домашню мережу та знижувати стабільність передачі даних [8].

Таким чином, система Smart Home є прикладом практичної реалізації IoT-мережі, у якій одночасно використовуються різні технології передачі даних. Проведений аналіз показав, що комбінування Wi-Fi та ZigBee дозволяє забезпечити баланс між швидкістю передачі даних, енергоефективністю, стабільністю роботи мережі та можливістю масштабування IoT-системи.

3.2 Аналіз принципу роботи системи

Функціонування системи «розумного будинку» базується на принципах Інтернету речей та передбачає постійну взаємодію між сенсорними пристроями, мережевими технологіями, центральним шлюзом, хмарною платформою та виконавчими механізмами. Основною особливістю досліджуваної IoT-системи є автоматизований цикл збору, передачі, аналізу та використання даних для управління житловою інфраструктурою у режимі реального часу. Такий підхід дозволяє реалізувати безперервний моніторинг параметрів середовища, автоматичне реагування на зміни та дистанційне керування системою через мережу Інтернет.

Практичне функціонування системи розпочинається зі збору інформації сенсорними пристроями. У межах досліджуваної IoT-мережі використовуються

датчики температури, вологості, руху, відкриття дверей, освітленості, диму, витоку газу та протікання води. Сенсори безперервно контролюють стан навколишнього середовища та формують пакети телеметричних даних, які передаються до центрального gateway. Передача інформації між сенсорами та шлюзом реалізується із використанням технології ZigBee, що забезпечує низьке енергоспоживання та стабільність зв'язку у межах mesh-мережі.

Практичний аналіз показав, що використання ZigBee є доцільним для сенсорних IoT-пристроїв, які передають невеликі обсяги інформації через певні інтервали часу. Максимальна швидкість передачі даних у ZigBee становить до 250 kbps при частоті 2,4 GHz, а радіус дії одного вузла у приміщенні складає 10–100 м залежно від конструкції будівлі та наявності перешкод. Основною перевагою технології є мінімальне енергоспоживання. У процесі практичного дослідження встановлено, що автономна робота ZigBee-сенсорів може тривати від 1 до 3 років без заміни елементів живлення.

Додатковою перевагою ZigBee є використання mesh-топології, за якої вузли мережі можуть передавати дані через проміжні пристрої. Це дозволяє підвищити стабільність функціонування системи та забезпечити роботу IoT-мережі навіть у випадку втрати зв'язку з окремими вузлами. У процесі аналізу було встановлено, що mesh-топологія дозволяє зменшити ризик втрати пакетів даних та розширити площу покриття мережі без збільшення потужності передавачів.

Для передачі великих обсягів інформації у системі використовується технологія Wi-Fi. Через Wi-Fi здійснюється підключення IP-камер відеоспостереження, хмарного сервера, маршрутизатора та мобільних пристроїв користувача. Практичний аналіз показав, що швидкість передачі даних у Wi-Fi-мережі становить 100–600 Mbps залежно від стандарту IEEE 802.11 та параметрів маршрутизатора. Радіус дії Wi-Fi у приміщенні становить приблизно 50 м, а на відкритій місцевості — до 100 м.

Перевагою Wi-Fi є висока пропускна здатність, яка дозволяє передавати відеопотоки, мультимедійні дані та забезпечувати дистанційне керування

системою у режимі реального часу. Водночас, у процесі дослідження було встановлено, що Wi-Fi характеризується значно вищим енергоспоживанням порівняно із ZigBee. З цієї причини Wi-Fi переважно використовується для пристроїв із постійним джерелом живлення, тоді як ZigBee застосовується для автономних сенсорних вузлів.

Ключовим елементом досліджуваної IoT-системи є центральний gateway, який виконує функції координації роботи мережі. Gateway приймає інформацію від ZigBee-сенсорів, здійснює первинну обробку даних, аналізує поточний стан системи та передає інформацію до хмарної платформи через Wi-Fi-маршрутизатор. Крім того, gateway забезпечує взаємодію між різними мережевими протоколами, оскільки ZigBee-пристрої не можуть безпосередньо передавати інформацію через Wi-Fi-мережу.

У процесі дослідження було проаналізовано сценарії автоматизованої роботи системи Smart Home. Наприклад, при зниженні температури у приміщенні нижче 18 °C датчик температури передає інформацію через ZigBee до gateway. Після аналізу отриманих даних gateway надсилає команду системі опалення на активацію. Аналогічно, при виявленні руху у нічний час система автоматично вмикає освітлення. У разі спрацювання датчиків диму або витoku газу gateway передає аварійне повідомлення користувачу через cloud-платформу та мобільний застосунок.

Важливу роль у функціонуванні системи відіграє хмарна платформа, яка забезпечує централізоване зберігання даних, аналітичну обробку інформації та віддалений доступ до системи. Передача інформації між gateway та cloud-сервером здійснюється через мережу Інтернет. Практичний аналіз показав, що використання cloud-сервісів дозволяє користувачу контролювати роботу IoT-системи незалежно від фізичного місцезнаходження. Через мобільний застосунок користувач може змінювати параметри автоматизації, переглядати стан сенсорів, отримувати статистичні дані та аварійні сповіщення у режимі реального часу.

У межах дослідження було проведено порівняльний аналіз використання Wi-Fi та ZigBee у Smart Home. Результати дослідження наведені у таблиці 3.2.

Таблиця 3.2 – Порівняння використання Wi-Fi та ZigBee у системі Smart Home

Параметр	Wi-Fi	ZigBee
Частотний діапазон	2,4 / 5 GHz	2,4 GHz
Швидкість передачі даних	100–600 Mbps	до 250 kbps
Радіус дії	50–100 м	10–100 м
Топологія	Star	Mesh
Енергоспоживання	Високе	Дуже низьке
Основне застосування	ІР-камери, cloud-з'єднання	Сенсори та датчики
Тип живлення	Переважно постійне	Автономне
Кількість підтримуваних пристроїв	Середня	Висока

Практичний аналіз функціонування системи дозволив визначити основні переваги використання комбінованої IoT-мережі. Поєднання ZigBee та Wi-Fi забезпечує баланс між швидкістю передачі даних, стабільністю функціонування та енергоефективністю. ZigBee дозволяє мінімізувати енергоспоживання сенсорів та забезпечує підтримку великої кількості пристроїв у мережі. Wi-Fi забезпечує високу швидкість передачі інформації та підтримку віддаленого доступу через мережу Інтернет.

Разом із перевагами у процесі дослідження було виявлено і певні недоліки досліджуваної системи. Однією з головних проблем є залежність системи від стабільності інтернет-з'єднання. У випадку втрати доступу до мережі Інтернет можуть бути недоступними функції cloud-сервісів та дистанційного керування системою. Додатковими проблемами є ризики кібербезпеки, пов'язані з можливістю несанкціонованого доступу до IoT-пристроїв, а також необхідність регулярного оновлення програмного забезпечення.

У процесі практичного аналізу також було встановлено, що використання великої кількості Wi-Fi-пристроїв може створювати значне навантаження на домашню мережу та збільшувати затримки передачі даних. Натомість ZigBee

забезпечує більш стабільну роботу сенсорної мережі при великій кількості вузлів завдяки mesh-топології та меншому навантаженню на канал передачі даних.

Таким чином, проведений аналіз принципу роботи системи Smart Home підтвердив ефективність використання комбінованої IoT-архітектури із застосуванням Wi-Fi та ZigBee. Практичні результати дослідження показали, що поєднання різних технологій передачі даних дозволяє забезпечити високу ефективність функціонування IoT-системи, оптимізувати енергоспоживання, підвищити стабільність роботи мережі та реалізувати автоматизоване управління житловою інфраструктурою у режимі реального часу.

3.3 Переваги та недоліки використання

Проведений аналіз практичного функціонування системи Smart Home дозволив визначити основні переваги та недоліки використання технологій Інтернету речей у житловому середовищі. Досліджувана IoT-система, побудована із використанням Wi-Fi та ZigBee, демонструє високий рівень автоматизації, можливість дистанційного керування обладнанням та ефективне використання мережевих технологій для забезпечення комфорту, безпеки та енергоефективності житлового приміщення.

Однією з головних переваг досліджуваної системи є автоматизація процесів управління побутовими пристроями. Використання сенсорів, gateway та виконавчих механізмів дозволяє системі самостійно реагувати на зміни параметрів навколишнього середовища без постійного втручання користувача. Наприклад, автоматичне регулювання освітлення та системи опалення дозволяє оптимізувати використання електроенергії та підвищити комфорт проживання.

Практичний аналіз показав, що використання IoT-технологій дозволяє знизити енергоспоживання житлового приміщення за рахунок автоматизованого керування освітленням, кліматичними системами та електроприладами. Використання ZigBee для сенсорних пристроїв забезпечує мінімальне

енергоспоживання та дозволяє сенсорам працювати автономно протягом тривалого часу. У процесі дослідження було встановлено, що ZigBee-сенсори можуть функціонувати від батареї до 1–3 років без заміни елементів живлення.

Додатковою перевагою IoT-системи є можливість дистанційного моніторингу та керування через мобільний застосунок. Користувач може у режимі реального часу отримувати інформацію про стан системи, переглядати показники сенсорів, змінювати параметри автоматизації та отримувати аварійні сповіщення незалежно від власного місцезнаходження. Це значно підвищує рівень контролю над житловим середовищем та оперативність реагування на надзвичайні ситуації.

Важливою перевагою досліджуваної IoT-мережі є використання комбінованої архітектури на базі Wi-Fi та ZigBee. Практичний аналіз показав, що ZigBee є ефективним рішенням для підключення сенсорних вузлів завдяки низькому енергоспоживанню та підтримці mesh-топології, тоді як Wi-Fi забезпечує високу швидкість передачі даних для мультимедійних пристроїв та cloud-сервісів. Поєднання цих технологій дозволяє забезпечити баланс між швидкістю передачі інформації, стабільністю роботи мережі та енергоефективністю.

Разом із перевагами проведений аналіз дозволив виявити і низку недоліків досліджуваної IoT-системи. Однією з головних проблем є залежність системи від стабільності інтернет-з'єднання. У разі втрати доступу до мережі Інтернет можуть бути недоступними функції дистанційного керування, cloud-сервіси та мобільні сповіщення. Це знижує ефективність функціонування системи та обмежує можливості віддаленого доступу.

Серйозною проблемою IoT-систем залишаються питання кібербезпеки. Велика кількість підключених пристроїв створює додаткові ризики несанкціонованого доступу до мережі. У процесі дослідження було встановлено, що недостатній рівень захисту IoT-пристроїв може призвести до перехоплення даних, втручання у роботу системи або несанкціонованого

керування обладнанням. Особливо вразливими є пристрої, які використовують стандартні паролі або застаріле програмне забезпечення.

Додатковим недоліком є проблема сумісності обладнання різних виробників. У практичних IoT-системах можуть використовуватися пристрої, які працюють на різних протоколах передачі даних або підтримують різні стандарти автоматизації. Це ускладнює інтеграцію обладнання у єдину мережу та може вимагати використання додаткових gateway або програмних рішень.

Практичний аналіз також показав, що використання великої кількості Wi-Fi-пристроїв створює додаткове навантаження на домашню мережу та може збільшувати затримки передачі даних. У процесі дослідження було встановлено, що при одночасному підключенні IP-камер, мультимедійних пристроїв та великої кількості мобільних клієнтів можливе зниження швидкості передачі даних та стабільності роботи мережі.

Для узагальнення результатів аналізу доцільно використати таблицю 3.3.

Таблиця 3.3 – Переваги та недоліки IoT-системи Smart Home

Характеристика	Переваги	Недоліки
Автоматизація	Автоматичне керування системами	Залежність від програмного забезпечення
Енергоефективність	Зменшення споживання електроенергії	Необхідність налаштування сценаріїв
Віддалений доступ	Контроль через мобільний застосунок	Залежність від Інтернету
ZigBee	Низьке енергоспоживання	Невисока швидкість передачі
Wi-Fi	Висока швидкість передачі даних	Високе енергоспоживання
Безпека	Моніторинг та аварійні сповіщення	Ризики кібербезпеки
Масштабованість	Можливість підключення нових пристроїв	Проблеми сумісності обладнання

Проведений аналіз дозволив визначити основні напрями вдосконалення IoT-систем Smart Home. Одним із найбільш важливих напрямів є підвищення рівня кібербезпеки шляхом використання сучасних алгоритмів шифрування,

багатофакторної автентифікації та регулярного оновлення програмного забезпечення IoT-пристроїв.

Перспективним напрямом розвитку є впровадження технологій штучного інтелекту та машинного навчання для автоматичного аналізу поведінки користувача та оптимізації роботи системи. Використання AI-алгоритмів дозволить системі автоматично адаптувати параметри освітлення, опалення та енергоспоживання відповідно до звичок мешканців.

Додатковим напрямом вдосконалення є впровадження енергоефективних мережевих технологій нового покоління, зокрема Thread, Matter та Wi-Fi HaLow, які забезпечують нижче енергоспоживання, підвищену стабільність мережі та кращу сумісність обладнання різних виробників.

Таким чином, проведений аналіз показав, що IoT-системи Smart Home мають значний потенціал для автоматизації житлового середовища, підвищення енергоефективності та забезпечення дистанційного контролю. Водночас, ефективність функціонування таких систем значною мірою залежить від стабільності мережевої взаємодії, рівня кібербезпеки, сумісності обладнання та правильного вибору технологій передачі даних.

3.4 Напрями удосконалення IoT-мереж

Стрімкий розвиток технологій Інтернету речей та постійне збільшення кількості підключених пристроїв зумовлюють необхідність удосконалення архітектури IoT-мереж, мережевих протоколів, механізмів обробки даних та засобів забезпечення інформаційної безпеки. Проведений аналіз системи Smart Home показав, що сучасні IoT-рішення забезпечують високий рівень автоматизації житлового середовища, однак водночас мають низку технічних, мережевих та безпекових обмежень. З огляду на це, основними напрямками вдосконалення IoT-мереж є підвищення рівня кібербезпеки, зменшення енергоспоживання, оптимізація мережевої взаємодії, забезпечення сумісності обладнання та впровадження інтелектуальних методів обробки даних.

У процесі практичного аналізу було встановлено, що однією з найбільш критичних проблем IoT-систем є забезпечення інформаційної безпеки. Велика кількість сенсорів, gateway, мережевих модулів та cloud-сервісів формує значну кількість потенційних точок для несанкціонованого доступу до мережі. Особливо вразливими є системи відеоспостереження, дистанційного керування та cloud-платформи, через які може здійснюватися віддалене адміністрування IoT-системи.

Для підвищення рівня кібербезпеки доцільним є впровадження сучасних методів криптографічного захисту даних, використання багатофакторної автентифікації, шифрування мережевого трафіку та регулярного оновлення програмного забезпечення IoT-пристроїв. Практичний аналіз показав, що значна частина вразливостей IoT-систем пов'язана із використанням стандартних паролів, застарілих версій firmware та недостатнім контролем мережевої активності. Тому перспективним напрямом розвитку є впровадження систем автоматичного моніторингу мережевої активності та виявлення підозрілих дій у режимі реального часу.

Важливим напрямом удосконалення IoT-мереж є впровадження концепції edge computing. У більшості сучасних IoT-систем значна частина інформації передається до cloud-сервісів для подальшої обробки та аналізу. Такий підхід створює додаткове навантаження на мережу, збільшує затримки передачі даних та формує залежність системи від стабільності інтернет-з'єднання.

Використання edge computing дозволяє виконувати частину аналітичної обробки інформації безпосередньо на gateway або локальних IoT-пристроях. Наприклад, у системі Smart Home gateway може самостійно аналізувати показники температури, руху або освітленості та приймати рішення без постійного звернення до cloud-сервера. Практичний аналіз показав, що використання edge computing дозволяє зменшити затримки передачі даних, знизити навантаження на мережу та підвищити стабільність функціонування системи навіть у випадку тимчасової втрати доступу до мережі Інтернет.

Окрему увагу необхідно приділити підвищенню енергоефективності IoT-мереж. Практичний аналіз Smart Home показав, що значна частина IoT-пристроїв працює автономно та використовує батарейне живлення. У таких умовах тривалість автономної роботи сенсорів безпосередньо залежить від енергоспоживання мережевих модулів та частоти передачі даних.

Для зменшення енергоспоживання доцільно використовувати енергоефективні протоколи передачі даних, зокрема ZigBee, Bluetooth Low Energy та LoRaWAN. Використання ZigBee у досліджуваній системі дозволило забезпечити автономну роботу сенсорів протягом 1–3 років без заміни елементів живлення. Додатковими напрямками вдосконалення є впровадження режимів енергозбереження, автоматичного переходу пристроїв у sleep-mode та використання відновлюваних джерел енергії, зокрема сонячних панелей.

Проведений аналіз також показав необхідність удосконалення мережевої інфраструктури IoT-систем. У процесі експлуатації Smart Home було встановлено, що при одночасному підключенні великої кількості Wi-Fi-пристроїв можливе збільшення затримок передачі даних та перевантаження домашньої мережі. Особливо це проявляється при роботі IP-камер відеоспостереження та мультимедійних сервісів.

Для вирішення цієї проблеми перспективним напрямом розвитку є впровадження сучасних телекомунікаційних технологій, зокрема 5G та Wi-Fi HaLow. Технологія 5G забезпечує високу швидкість передачі даних, мінімальні затримки та підтримку великої кількості одночасних підключень. Wi-Fi HaLow, у свою чергу, забезпечує нижче енергоспоживання та більший радіус дії порівняно із традиційним Wi-Fi, що робить його перспективним рішенням для IoT-систем.

У процесі дослідження було встановлено, що однією з головних проблем сучасних IoT-систем є недостатня сумісність обладнання різних виробників. Пристрої можуть використовувати різні стандарти передачі даних, протоколи взаємодії та програмні платформи, що ускладнює інтеграцію обладнання у єдину мережу.

Для вирішення цієї проблеми перспективним напрямом є впровадження універсальних стандартів взаємодії, зокрема Matter та Thread. Використання таких стандартів дозволяє забезпечити стабільну взаємодію IoT-пристроїв різних виробників, спростити процес налаштування обладнання та підвищити масштабованість системи.

Перспективним напрямом розвитку IoT-мереж є також інтеграція технологій штучного інтелекту та машинного навчання. Використання AI-алгоритмів дозволяє системі автоматично аналізувати поведінку користувача, прогнозувати зміни параметрів середовища та оптимізувати роботу IoT-пристроїв. Наприклад, система Smart Home може автоматично регулювати освітлення, температуру та режими роботи обладнання відповідно до звичок мешканців.

У процесі дослідження було встановлено, що використання AI-алгоритмів дозволяє підвищити енергоефективність системи, оптимізувати використання ресурсів та зменшити навантаження на мережу. Крім того, машинне навчання може використовуватися для прогнозування можливих несправностей обладнання та виявлення аномальної мережевої активності.

Для узагальнення результатів аналізу доцільно використати таблицю 3.4.

Таблиця 3.4 – Основні напрями вдосконалення IoT-мереж

Напрямок вдосконалення	Основна проблема	Запропоноване рішення
Кібербезпека	Ризик несанкціонованого доступу	Шифрування, MFA, оновлення firmware
Edge computing	Високі затримки передачі	Локальна обробка даних
Енергоефективність	Високе енергоспоживання	ZigBee, BLE, sleep-mode
Мережева інфраструктура	Перевантаження Wi-Fi	5G, Wi-Fi HaLow
Сумісність обладнання	Різні стандарти виробників	Matter, Thread
AI та автоматизація	Обмежена адаптивність системи	Машинне навчання та AI-аналіз

Практичний аналіз також показав необхідність підвищення надійності IoT-мереж. Навіть короточасне порушення зв'язку може призводити до помилок у роботі систем автоматизації. Тому перспективним напрямом удосконалення є впровадження резервування каналів зв'язку, дублювання gateway та використання механізмів автоматичного відновлення роботи системи у випадку аварійних ситуацій.

Важливим напрямом розвитку є також спрощення процесу використання IoT-систем кінцевими користувачами. Незважаючи на широкі функціональні можливості Smart Home, складність налаштування обладнання та інтеграції різних пристроїв може обмежувати поширення IoT-технологій серед населення. У зв'язку з цим перспективним є розвиток інтуїтивних інтерфейсів, автоматизованого налаштування мережі та систем голосового керування.

Таким чином, проведений аналіз показав, що подальший розвиток IoT-мереж повинен бути спрямований на підвищення рівня кібербезпеки, оптимізацію енергоспоживання, вдосконалення мережевої інфраструктури, забезпечення сумісності обладнання та впровадження інтелектуальних методів аналізу даних. Реалізація запропонованих напрямів вдосконалення дозволить підвищити ефективність функціонування IoT-систем, забезпечити їхню стабільність, масштабованість та безпечне використання у сучасному цифровому середовищі.

3.5 Висновки до розділу 3

У третьому розділі на основі практичного аналізу системи «розумного дому» (Smart Home) досліджено особливості функціонування реальної IoT-мережі, визначено її переваги, недоліки та обґрунтовано напрями подальшого вдосконалення.

1. Розглянуто архітектуру гібридної IoT-системи Smart Home, побудованої з використанням технологій ZigBee (для сенсорних вузлів) та Wi-Fi (для відеоспостереження, хмарного сервісу та мобільних пристроїв). Показано,

що комбінування цих технологій дозволяє досягти балансу між низьким енергоспоживанням (автономна робота ZigBee-сенсорів 1–3 роки) та високою швидкістю передачі даних для мультимедійних застосунків.

2. Детально проаналізовано принцип роботи системи: від збору даних сенсорами температури, вологості, руху, диму тощо через ZigBee-мережу з mesh-топологією до центрального шлюзу, подальшої обробки на gateway та передачі на хмарну платформу через Wi-Fi. Встановлено, що використання mesh-топології ZigBee підвищує стабільність і надійність мережі, а хмарний сервіс забезпечує дистанційний моніторинг та управління в реальному часі.

3. Визначено основні переваги (автоматизація, енергоефективність, віддалений доступ) та недоліки (залежність від інтернет-з'єднання, ризики кібербезпеки, проблеми сумісності обладнання різних виробників, високе навантаження на Wi-Fi-мережу) впровадження IoT-систем у житловому секторі.

4. Обґрунтовано перспективні напрями вдосконалення IoT-мереж: підвищення кібербезпеки (шифрування, багатофакторна автентифікація, регулярне оновлення firmware), впровадження edge computing для зменшення затримок і залежності від хмари, використання енергоефективних технологій (5G, Wi-Fi HaLow, Thread, Matter), а також інтеграція методів штучного інтелекту та машинного навчання для адаптивної автоматизації та прогнозової аналітики.

ВИСНОВКИ

У результаті виконання дипломної роботи було проведено комплексний аналіз принципів побудови мереж Інтернету речей, досліджено особливості архітектури IoT-систем, технології передачі даних та практичні аспекти функціонування IoT-мереж на прикладі системи Smart Home. У ході дослідження основну увагу було зосереджено саме на аналізі побудови IoT-мереж, принципах взаємодії їхніх складових, структурі мережевої архітектури, особливостях використання різних технологій передачі даних та оцінці їхньої ефективності у реальних умовах експлуатації.

У процесі дослідження було встановлено, що мережі Інтернету речей мають багаторівневу архітектуру, яка включає сенсорний рівень, мережеву інфраструктуру, рівень обробки даних та прикладний рівень управління. Проведений аналіз показав, що ефективність функціонування IoT-систем значною мірою залежить від правильного вибору технологій передачі даних, організації мережевої взаємодії та способу інтеграції пристроїв у єдину інформаційну систему.

У роботі було проаналізовано основні технології передачі даних, які використовуються у сучасних IoT-мережах, зокрема Wi-Fi, Bluetooth Low Energy, ZigBee, LoRaWAN, NB-IoT, LTE-M та 5G IoT. Для кожної технології було розглянуто структуру побудови мережі, тип топології, швидкість передачі даних, радіус дії, енергоспоживання, принцип взаємодії пристроїв та сфери практичного застосування.

Проведений аналіз показав, що технологія Wi-Fi є ефективним рішенням для IoT-систем, які потребують високої швидкості передачі даних та підтримки мультимедійних сервісів. Водночас її використання супроводжується високим енергоспоживанням та підвищеним навантаженням на мережу при великій кількості підключених пристроїв.

У результаті дослідження було встановлено, що Bluetooth Low Energy є доцільним рішенням для персональних IoT-пристроїв та сенсорних систем із

низьким енергоспоживанням. Аналіз показав, що основними перевагами BLE є енергоефективність та простота інтеграції, тоді як недоліками залишаються невеликий радіус дії та обмежена пропускна здатність.

Особливу увагу у роботі було приділено аналізу ZigBee-мереж. Дослідження показало, що використання mesh-топології забезпечує високу стабільність функціонування мережі та можливість підтримки великої кількості сенсорних вузлів при низькому енергоспоживанні. Встановлено, що ZigBee є одним із найбільш ефективних рішень для систем автоматизації будівель та Smart Home.

У процесі аналізу LoRaWAN було визначено, що дана технологія є ефективною для побудови IoT-мереж великого радіуса дії. Основними перевагами LoRaWAN є низьке енергоспоживання та можливість передачі даних на відстань до декількох кілометрів. Водночас низька швидкість передачі даних обмежує використання технології у системах, які потребують передачі великих обсягів інформації у режимі реального часу.

Під час дослідження NB-IoT та LTE-M було встановлено, що використання стільникових технологій забезпечує широке покриття мережі та стабільний зв'язок для віддалених IoT-пристроїв. Водночас використання таких технологій супроводжується залежністю від інфраструктури мобільних операторів та підвищеними енергетичними витратами.

Практична частина роботи була присвячена аналізу IoT-системи Smart Home, побудованої із використанням Wi-Fi та ZigBee. У межах дослідження було проаналізовано структуру мережі, принципи передачі даних між сенсорами, gateway, cloud-сервісом та виконавчими пристроями. Проведений аналіз підтвердив ефективність комбінованого використання Wi-Fi та ZigBee у межах єдиної IoT-мережі.

У процесі практичного дослідження було встановлено, що використання ZigBee для сенсорних пристроїв дозволяє забезпечити мінімальне енергоспоживання та підтримку великої кількості вузлів у мережі. Одночасно

використання Wi-Fi забезпечує високу швидкість передачі даних для IP-камер, cloud-сервісів та мобільного доступу до системи.

Проведений аналіз показав, що використання комбінованої IoT-архітектури дозволяє забезпечити баланс між швидкістю передачі інформації, стабільністю роботи мережі, масштабованістю та енергоефективністю системи. Водночас у процесі дослідження було виявлено низку проблем, пов'язаних із практичним впровадженням IoT-мереж.

Основними недоліками сучасних IoT-систем визначено залежність від стабільності інтернет-з'єднання, ризики кібербезпеки, проблеми сумісності обладнання різних виробників та високе навантаження на Wi-Fi-мережу при великій кількості підключених пристроїв. Також встановлено, що значна кількість IoT-пристроїв створює додаткові ризики несанкціонованого доступу до мережі та потребує впровадження сучасних механізмів захисту інформації.

На основі проведеного дослідження було визначено перспективні напрями вдосконалення IoT-мереж. До основних напрямів розвитку віднесено підвищення рівня кібербезпеки, використання edge computing, впровадження технологій 5G та Wi-Fi HaLow, розвиток енергоефективних протоколів передачі даних, інтеграцію штучного інтелекту та стандартизацію взаємодії пристроїв через технології Matter та Thread.

У результаті дослідження встановлено, що подальший розвиток IoT-мереж повинен бути спрямований на підвищення надійності мережевої взаємодії, оптимізацію енергоспоживання, забезпечення масштабованості систем та вдосконалення механізмів інформаційної безпеки. Реалізація зазначених напрямів дозволить підвищити ефективність функціонування IoT-систем та забезпечити їх широке впровадження у різних сферах життєдіяльності суспільства.

Таким чином, результати виконаної роботи підтвердили, що Інтернет речей є перспективним напрямом розвитку сучасних інформаційно-комунікаційних технологій, а правильна побудова IoT-мереж та обґрунтований

вибір технологій передачі даних є ключовими факторами ефективного функціонування сучасних IoT-систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л., Гнатюк С. О. Інтернет речей: сучасний стан та перспективи розвитку. Інформаційні технології і засоби навчання. 2019. Т. 70, № 2. С. 1–15.
2. Гнатюк С. О. Основи кібербезпеки. Київ: КПІ ім. Ігоря Сікорського, 2020. 300 с.
3. Конахович Г. Ф., Пузиренко О. Ю. Комп'ютерні мережі. Київ: Каравела, 2018. 408 с.
4. Конахович Г. Ф. Телекомунікаційні системи та мережі. Київ: Каравела, 2017. 512 с.
5. Соловйов В. М. Комп'ютерні мережі та телекомунікації. Київ: Ліра-К, 2019. 456 с.
6. ДСТУ ISO/IEC 30141:2020. Інформаційні технології. Інтернет речей. Еталонна архітектура. Київ: ДП «УкрНДНЦ», 2020.
7. Кравченко О. В. Бездротові технології передачі даних. Харків: ХНУРЕ, 2018. 320 с.
8. Романюк В. А. Технології бездротового зв'язку: Wi-Fi, Bluetooth, ZigBee. Київ: Політехніка, 2019. 280 с.
9. Жуков І. А., Зінченко О. В. Інтернет речей: теоретичні аспекти та практичне застосування. Вісник НТУУ «КПІ». Серія: Інформатика. 2020. № 2. С. 45–52.
10. Гуменюк І. В. Архітектура Інтернету речей. Наукові записки. Серія: Комп'ютерні науки. 2021. № 1. С. 23–30.
11. Литвиненко О. С. Захист інформації в мережах Інтернет речей. Сучасні інформаційні технології. 2020. № 3. С. 89–95.
12. Ткаченко В. П. Проблеми безпеки Інтернету речей. Кібербезпека: освіта, наука, техніка. 2021. № 3.
13. Дяченко П. А. Основи побудови мереж Інтернету речей. Телекомунікаційні науки. 2022. № 2. С. 56–63.

- 14.Мельник О. О. Інтернет речей у концепції «розумного міста». Економіка та держава. 2021. № 5. С. 112–117.
- 15.Міністерство цифрової трансформації України. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки. Київ, 2020.
- 16.Державна служба спеціального зв'язку та захисту інформації України. Рекомендації щодо кіберзахисту пристроїв Інтернету речей. Київ, 2022.
- 17.Atzori L., Iera A., Morabito G. The Internet of Things: A survey. Computer Networks. 2010. Vol. 54, No. 15. P. 2787–2805.
- 18.Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013. Vol. 29, No. 7. P. 1645–1660.
- 19.Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials. 2015. Vol. 17, No. 4. P. 2347–2376.
- 20.ITU-T Y.2060. Overview of the Internet of Things. Geneva: ITU, 2012.
- 21.ISO/IEC 30141:2018. Internet of Things (IoT) Reference Architecture. Geneva: ISO, 2018.
- 22.Rose K., Eldridge S., Chapin L. The Internet of Things: An Overview. Internet Society, 2015.
- 23.NIST. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. Gaithersburg, 2020.
- 24.Bahga A., Madiseti V. Internet of Things: A Hands-On Approach. Indianapolis: Universities Press, 2014.
- 25.Kranz M. Building the Internet of Things. Indianapolis: Wiley, 2016.
- 26.Vermesan O., Friess P. Internet of Things: Converging Technologies for Smart Environments. Aalborg: River Publishers, 2013.

27. Whitmore A., Agarwal A., Da Xu L. The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*. 2015. Vol. 17, No. 2. P. 261–274.
28. Da Xu L., He W., Li S. Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*. 2014. Vol. 10, No. 4. P. 2233–2243.
29. Borgia E. The Internet of Things vision: Key features, applications and open issues. *Computer Communications*. 2014. Vol. 54. P. 1–31.
30. Cisco Systems. Internet of Things (IoT) Overview. URL: <https://www.cisco.com>

ДОДАТКИ

Додаток А

Структура IoT-системи «розумного дому» відповідно до її архітектури



Додаток Б

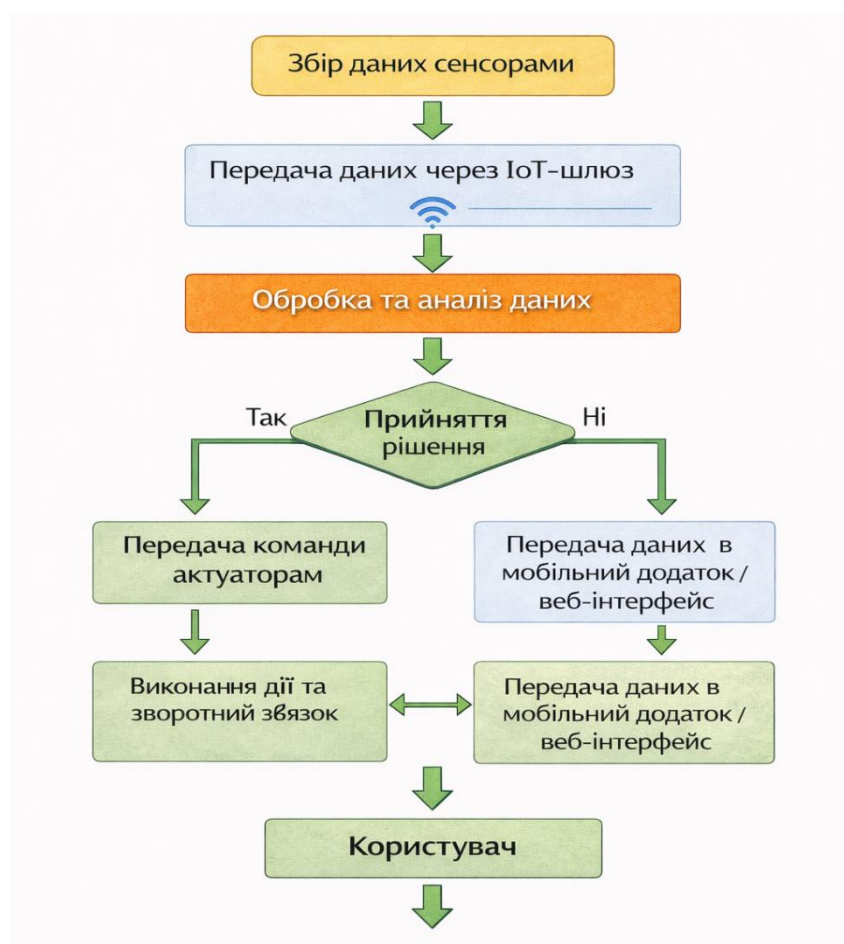
Таблиця Б.1 – Порівняльна характеристика технологій передачі даних у IoT-мережах

Технологія	Дальність передачі	Швидкість	Енергоспоживання	Топологія	Сфера застосування
Wi-Fi	до 100 м	100–600 Mbps	високе	зірка	розумний дім, відеоспостереження
Bluetooth Low Energy (BLE)	до 10–50 м	до 2 Mbps	дуже низьке	точка-точка	носимі пристрої, медицина

ZigBee	до 100 м	до 250 kbps	низьке	mesh	автоматизація будівель
LoRaWAN	до 10–15 км	0,3–50 kbps	мінімальне	зірка	smart city, агросфера

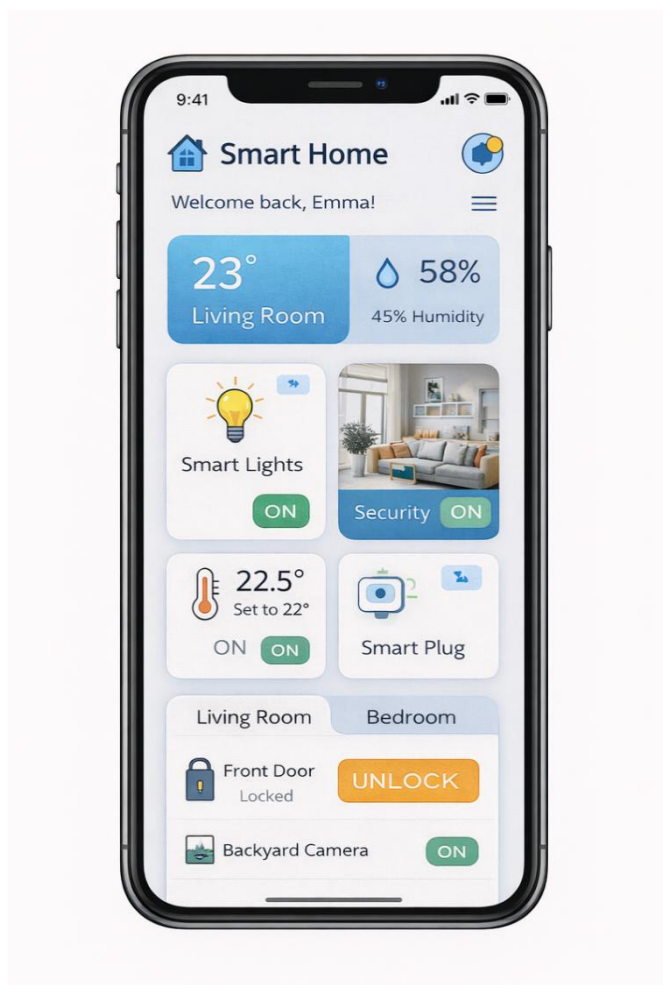
Додаток В

Рисунок В.1 – Блок-схема функціонування IoT-системи «розумного дому»



Додаток Г

Рисунок Г.1 – Інтерфейс користувача IoT-системи «розумного дому»



На ілюстрації можна побачити зразок користувацького вигляду IoT-системи «розумного дому» втіленого через мобільну програму. Цей інтерфейс дає змогу віддалено керувати ключовими можливостями системи, як-от освітлення, клімат-контроль, охоронні системи та інші під'єднані гаджети.

Сам інтерфейс складається з панелі управління, де прописуються теперішні показники оточення, а також містить засоби для коригування системних параметрів. Людина, що користується, може бачити інформацію про роботу пристроїв у мить їхньої зміни та швидко відгукуватися на будь-які відхилення.

Використання такого вигляду сприяє простоті експлуатації IoT-рішення, нарощує ступінь нагляду за житловим простором та допомагає цільовому розпорядженню ресурсами.