

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти (освітній ступінь))

на тему СИСТЕМА УПРАВЛІННЯ ПОТОКАМИ ПОДІЙ В РЕЖИМІ РЕАЛЬНОГО
ЧАСУ ЗА ДОПОМОГОЮ ІНТЕРНЕТУ РЕЧЕЙ

Виконав: студент 2 курсу, групи КНТ-613М
Спеціальності 123 Комп'ютерна інженерія

Освітня програма (спеціалізація)

Спеціалізовані комп'ютерні системи

(код і назва спеціальності)

ШЕВЧЕНКО Д.О.

(прізвище та ініціали)

Керівник ІЛ'ЯШЕНКО М.Б.

(прізвище та ініціали)

Рецензент СТЕПАНЕНКО О.О.

(прізвище та ініціали)

2024 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування вищого навчального закладу)

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти (освітній ступінь) магістерський
Спеціальність 123 Комп'ютерна інженерія
(код і назва)
Освітня програма (спеціалізація) Спеціалізовані комп'ютерні системи
(назва)

ЗАТВЕРДЖУЮ
Зав. кафедри Кудерметов Р.К.

“ _____ ” _____ 2024 року

ЗАВДАННЯ НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

ШЕВЧЕНКО Денис Олександрович

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Система управління потоками подій в режимі реального часу за допомогою Інтернету речей

керівник проекту (роботи) ІЛЛЯШЕНКО Матвій Борисович, к. т. н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “18” жовтня 2024 року № 149

2. Строк подання студентом проекту (роботи) 01 грудня 2024 року

3. Вихідні дані до проекту (роботи) iBeacon, IoT, RFID, Bluetooth Low Energy, WiFi, Complex Event Processing,

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) _____

1) Аналіз використання систем Інтернету речей.

2) Керування подіями у системи інтернету речей.

3) Впровадження технології Ibeason в режимі реального часу у системи інтернету речей.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	ІЛЛЯШЕНКО М.Б., к. т. н., доцент		
Нормоконтроль	ПОЛЬСЬКА О.В., ст. викладач		

7. Дата видачі завдання 01.10.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз технічного завдання	10.10.2024 р.	
2	Огляд проблем безпеки у системі Інтернету речей	15.10.2024 р.	
3	Технології впровадження Інтернету речей	27.10.2024 р.	
4	Технології для управління подіями в реальному часі	05.11.2024 р.	
5	Управління подіями за допомогою технології iBeacon	17.11.2024 р.	
6	Впровадження технології iBeacon	25.11.2024 р.	
7	Оформлення ПЗ	01.12.2024 р.	

Студент Денис ШЕВЧЕНКО
(підпис) (ініціали та прізвище)

Керівник проекту (роботи) Матвій ІЛЛЯШЕНКО
(підпис) (ініціали та прізвище)

РЕФЕРАТ

ПЗ: 72 с., 20 рис., 1 табл., 25 джерел.

BLE, CEP, ESP, iBEACON, IoT, MONITORING, RANGING, RFID, SMART HOUSE, SMART CITY, SMART LIGHT.

Мета - вивчення сучасної концепції розгортання та управління подіями у контексті Інтернету речей, включаючи об'єкти даних, їх управління, ієрархії управління, а також основні технології впровадження Інтернету речей, такі як iBeacon та RFID. Ці технології сприяють збору й відстеженню необхідних даних, зменшують час очікування та скорочують трудові витрати при управлінні подіями.

Завдання - для досягнення поставленої мети необхідно виконати такі завдання:

- дослідити основну концепцію Інтернету речей і її перспективи розгортання у сучасному світі;
- розглянути ключові технології впровадження та управління подіями у контексті Інтернету речей;
- навести приклади практичного використання цих технологій;
- розробити програмний продукт як приклад застосування технологій;
- створити стратегію стартап-проєкту для впровадження описаних технологій як конкурентоспроможного продукту.

Предмет дослідження - технології, які застосовуються для управління подіями в Інтернеті речей.

Наукова новизна. Наукова новизна роботи полягає у дослідженні технологій управління подіями в реальному часі в контексті Інтернету речей. Практична цінність - значущість роботи полягає в аналізі методів і засобів для управління подіями в режимі реального часу за допомогою Інтернету речей.

ABSTRACT

Explanatory note to the master's work: 72 p.; 20 figures; 1 table; 25 sources.

BLE, CEP, ESP, iBEACON, IoT, MONITORING, RANGING, RFID, SMART HOUSE, SMART CITY, SMART LIGHT.

The purpose of this paper is to study the current concept of event deployment and management in the context of the Internet of Things, including data objects, their management, management hierarchies, and the main technologies for implementing the Internet of Things, such as iBeacon and RFID. These technologies facilitate the collection and tracking of relevant data, reduce waiting times and reduce labour costs in event management.

To achieve this goal, you need to complete the following tasks:

- explore the basic concept of the Internet of Things and its prospects for deployment in the modern world;
- to consider the key technologies for implementing and managing events in the context of the Internet of Things;
- to provide examples of practical use of these technologies;
- develop a software product as an example of technology application;
- to create a start-up project strategy for the implementation of the described technologies as a competitive product.

The subject of the study is the technologies used to manage events in the Internet of Things.

The scientific novelty of the work is to study real-time event management technologies in the context of the Internet of Things.

The practical significance of the work lies in the analysis of methods and tools for managing real-time events using the Internet of Things.

ЗМІСТ

Скорочення та умовні позначки.....	8
Вступ	9
1 Аналіз використання систем Інтернету речей	13
1.1 Поняття системи Інтернету речей.....	13
1.2 Історія системи Інтернету речей	14
1.3 Керування за допомогою Інтернету речей	18
1.3.1 Географічне покриття та мобільність	23
1.3.2 Стандартизація iot та бездротове зондування.....	25
1.4 Сучасний стан Інтернету речей.....	28
1.5 Існуючі проблеми безпеки у системі Інтернету речей.....	31
1.6 Висновки до розділу.....	35
2 Керування подіями у системи інтернету речей	36
2.1 Керування даними	36
2.2 Керування учасниками.....	39
2.2.1 Технології для управління подіями RFID	39
2.2.2 Технології для управління подіями iBeacon.....	40
2.3 Розумне освітлення.....	42
2.4 Розумний будинок	46
2.5 Обробка відео у потоковому режимі	49
2.6 Обробка подій	51
2.7 Висновки до розділу.....	55
3 Впровадження технології IBeacon в режимі реального часу у системи інтернету речей	55
3.1 Опис технологій для використання	56
3.1.1 Eddystone (Google).....	58
3.1.2 altbeacon (Radius Networks).....	58
3.1.3 Kontakt.io Beacons.....	59

3.1.4 Estimote Beacons	59
3.1.5 Gimbal Beacons.....	60
3.2 Принцип роботи технології	61
3.3 Висновки до розділу.....	70
Висновки.....	71
Перелік джерел посилання	73

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AI	– Artificial Intelligence (Штучний інтелект)
BLE	– Bluetooth Low Energy (Bluetooth з низьким споживанням енергії)
ESP	– Event Stream Processing (Обробка потоку подій)
IoT	– Internet of Things (Інтернет речей)
IIoT	– Industrial IoT (Промисловий IoT)
LDR	– Light-dependent resistors (Світлозалежні резистори)
ML	– Machine learning (Машинне навчання)
PIR	– Per Infrared sensors (Інфрачервоні датчики)
RFID	– Radio frequency identification technologies (Технології радіочастотної ідентифікації)
PLC	– Power Line Communication (Зв'язок по лінії електропередач)

ВСТУП

Протягом XX століття численні технології кардинально змінили стиль життя: радіозв'язок, телебачення, комп'ютери, мобільні телефони та Інтернет стали невід'ємною частиною сучасності. Значне поширення отримали й технології Інтернету речей, основна ідея яких полягає в можливості підключення різних об'єктів до мережі для обробки даних з навколишнього середовища, обміну цією інформацією та виконання дій на її основі. Інтернет речей вважають новим етапом технічної революції, що трансформує побут, виробництво, мобільні пристрої та індустрію. Основні функції цієї концепції спрямовані на полегшення повсякденного життя, підвищення ефективності й якості роботи, а також економію енергії. Відтак, в Україні також зростає інтерес до технологій Інтернету речей.

Інтернет речей - це мережа, яка об'єднує фізичні об'єкти та пристрої з вбудованими датчиками й програмним забезпеченням, що забезпечує передачу та обмін даними між фізичним світом і комп'ютерними системами через стандартні протоколи зв'язку. Крім датчиків, мережа може включати виконавчі пристрої, інтегровані у фізичні об'єкти та з'єднані через дротові або бездротові мережі [1]. Ці взаємопов'язані об'єкти можуть зчитувати дані, здійснювати певні дії, бути програмованими та ідентифікованими, дозволяючи виключити участь людини завдяки використанню інтелектуальних інтерфейсів.

Основна концепція Інтернету речей полягає у можливості підключення до мережі різних об'єктів, які людина використовує у повсякденному житті, таких як холодильники, кондиціонери, автомобілі, велосипеди і навіть кросівки. Всі ці пристрої оснащені вбудованими датчиками або сенсорами, які здатні обробляти інформацію з навколишнього середовища, обмінюватися даними і виконувати дії на основі отриманої інформації. Наприклад, система «розумний будинок» аналізує параметри навколишнього середовища і автоматично регулює

температуру в приміщенні: взимку - інтенсивність опалення, а влітку - відкриття або закриття вікон для провітрювання, все це без участі людини.

Для зберігання та аналізу даних, що надходять від численних сенсорів, зручно використовувати IoT-платформи, доступні як на комерційній основі, так і безкоштовно, з можливістю розміщення на хмарних платформах або на власних системах користувача.

Сучасний Інтернет речей забезпечує комунікацію між об'єктами, дозволяючи їм самостійно взаємодіяти одне з одним та з навколишнім середовищем. Це дозволяє пристроям автоматично виконувати певні функції, приймати рішення і обмінюватися інформацією без втручання людини, що є важливим як у побуті, так і в автомобільних та інфраструктурних системах.

Фахівці відзначають, що IoT є однією з найперспективніших технологій останніх років, яка вже сьогодні стимулює появу сотень нових продуктів і компаній, що активно конкурують з IT-гігантами. Багато користувачів навіть не помічають, що вже активно користуються такими пристроями. В Україні, наприклад, системи "розумного будинку", що містять десятки сенсорів, стають все більш поширеними. Переваги Інтернету речей, як уже наявні, так і ті, що ще розробляються, краще зрозуміти на прикладах, оскільки ця технологія має багато сфер застосування.

Термін "Інтернет речей" було вперше сформульовано ще у 1999 році, і сьогодні ця сфера є одним із провідних світових трендів. Сучасні технології IoT дозволяють підключати до мережі навіть уже існуючі пристрої, розширюючи їх функціональність, що підкреслює значення Інтернету речей як рушійної сили четвертої індустріальної революції, яка триває в усьому світі [2].

Перехід від "Інтернету людей" до "Інтернету речей" відбувся у 2008–2009 роках, коли кількість підключених до мережі пристроїв вперше перевищила кількість інтернет-користувачів. Цей етап став початком нової ери технологій – Інтернету речей. За прогнозами аналітиків, у найближчі роки відбудеться суттєвий ріст IoT. Так, аналітична компанія Gartner передбачала, що до 2020 року кількість підключених до Інтернету пристроїв досягне 26 мільярдів, а обсяги

ринку обладнання, програмного забезпечення та послуг сягнуть 1,9 трильйонів доларів. Найбільші IT-компанії, зокрема Intel та Google, активно працюють над розвитком IoT. Зокрема, Intel ще у 2014 році створила підрозділ “Internet of Things Solutions Group”, а Google придбала компанію Nest Labs за 3,2 мільярда доларів для впровадження інтелектуальних термостатів на американському ринку. Також у цьому напрямі активно розвиваються виробники побутової техніки.

Яскравим прикладом застосування IoT є система “розумний будинок”, яка може контролювати параметри навколишнього середовища та автоматично регулювати температуру в приміщеннях. У зимовий період система автоматично налаштовує інтенсивність обігріву залежно від зовнішньої температури, сили вітру та часу доби, що сприяє ефективному використанню енергоносіїв. Сьогодні концепція “розумного будинку” асоціюється з IoT і охоплює пристрої, такі як термостати, системи відеоспостереження, холодильники і телевізори. Цей сегмент технологій базується на ситуативних децентралізованих бездротових мережах. У сучасних домівках та офісах часто встановлюють такі системи, що дозволяють, наприклад, віддалено контролювати будинок через смартфон або автоматично керувати кліматичними умовами у приміщеннях. Основні функції цих систем - це забезпечення безпеки та ефективне використання енергоресурсів.

Також великою сферою застосування IoT є автомобільний транспорт, де ця технологія допомагає здійснювати діагностику авто під час експлуатації, попереджати аварійні ситуації, автоматично замовляти запчастини та надавати рекомендації щодо обслуговування автомобіля.

Метою цієї роботи є дослідження сучасних підходів до розгортання та управління подіями у сфері Інтернету речей, зокрема об’єктів даних, способів їх керування, ієрархічної структури управління, а також ключових технологій IoT, таких як iBeacon та RFID. Ці технології сприяють ефективному збору та відстеженню даних, зменшують час очікування і скорочують витрати на управління подіями. У роботі представлено приклади практичного застосування таких технологій [3].

Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати основні концепції Інтернету речей та можливості їх застосування у сучасному світі;
- розглянути ключові технології, що забезпечують впровадження та управління подіями у контексті Інтернету речей;
- надати приклади практичного застосування зазначених технологій;
- розробити програмний продукт, який демонструє можливості використання цих технологій;
- розробити стратегію стартап-проєкту, що дозволить перетворити досліджувану технологію на конкурентоспроможний продукт.

1 АНАЛІЗ ВИКОРИСТАННЯ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Поняття системи Інтернету речей

Інтернет речей є однією з найбільш актуальних концепцій у сучасній футурології, яка вже перестає бути просто теорією і активно втілюється в життя. IoT являє собою комп'ютерну модель, основною ідеєю якої є підключення різноманітних об'єктів до мережі для обробки даних із навколишнього середовища, обміну ними та автоматизованого прийняття рішень з виконанням відповідних дій на основі отриманої інформації (рис. 1.1).

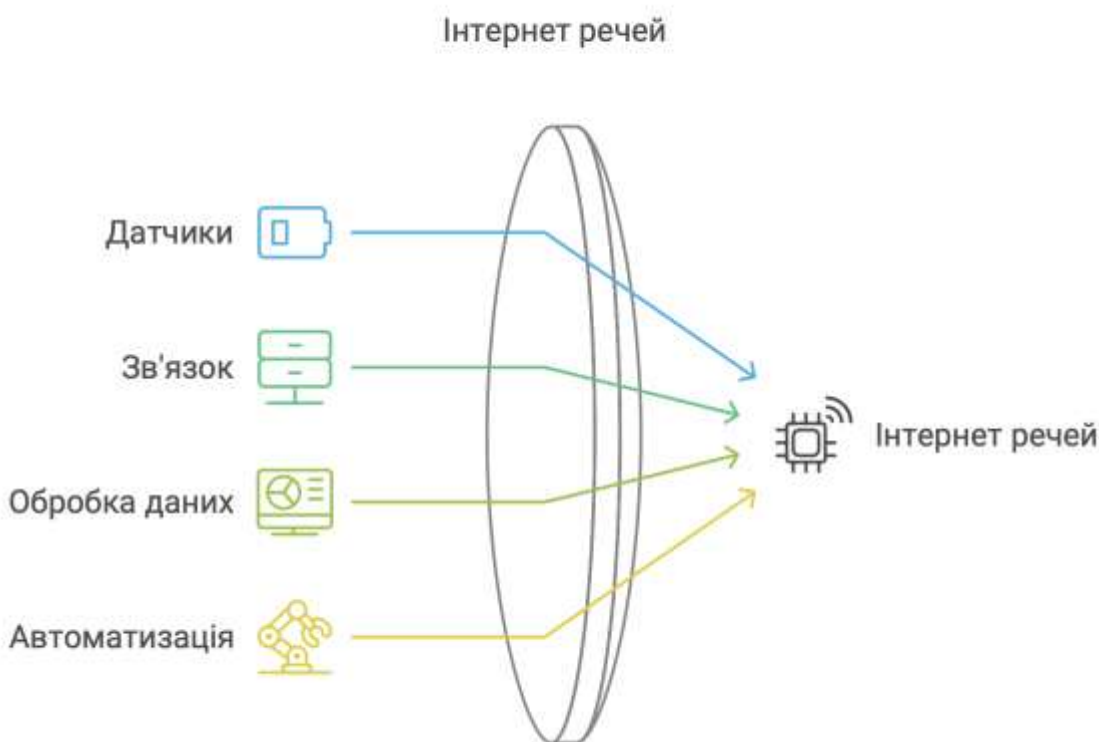


Рисунок 1.1 – Представлення Інтернету речей

Інтернет речей – це мережа фізичних об'єктів, таких як пристрої, транспортні засоби, побутова техніка та інші предмети, обладнані електронікою, програмним забезпеченням, датчиками та виконавчими механізмами, які надають їм можливість підключатися до мережі та обмінюватися даними між собою.

Кожен об'єкт має унікальну ідентифікацію завдяки вбудованій обчислювальній системі і може взаємодіяти в рамках наявної інтернет-інфраструктури [4].

З 2016 року кількість підключених пристроїв зросла на 31%, досягнувши 8,4 мільярда у 2017 році. Експерти прогнозують, що до 2020 року кількість IoT-пристроїв сягне 30 мільярдів, а ринкова вартість цього сегмента може досягти 7,1 трильйона доларів.

IoT забезпечує можливість віддаленого моніторингу та керування об'єктами через існуючу мережеву інфраструктуру, сприяючи інтеграції фізичного світу з комп'ютерними системами. Це призводить до підвищення ефективності, точності, економічної вигоди і зниження необхідності у втручанні людини. Коли Інтернет речей доповнюється сенсорами, він стає частиною ширшого класу кібер-фізичних систем, що охоплюють такі технології, як інтелектуальні мережі, віртуальні електростанції, розумні будинки, інтелектуальні транспортні засоби та міста. Ці пристрої збирають корисні дані за допомогою існуючих технологій та автоматично передають їх іншим пристроям.

1.2 Історія системи Інтернету речей

Термін "Інтернет речей" (англ. "Internet of Things") був вперше запропонований Кевіном Ештоном у 1999 році під час його роботи в компанії "Procter & Gamble". Ештон використав цей термін для опису системи, в якій фізичні об'єкти з підключеними датчиками можуть взаємодіяти з мережею Інтернет. Його ідея полягала в тому, що комп'ютери могли б відстежувати об'єкти, обладнані ідентифікаторами, автоматично і без людського втручання. Спочатку для реалізації цієї концепції він передбачав використання технології радіочастотної ідентифікації, яка застосовується у великих компаніях для автоматизованого відстеження товарів [5].

Крім RFID, ідентифікація об'єктів може здійснюватися за допомогою

інших технологій, таких як NFC, штрих-коди, QR-коди та цифрові водяні знаки. Сьогодні термін "Інтернет речей" охоплює широкий спектр сценаріїв, де інтернет-з'єднання та обчислювальні можливості поширюються на різноманітні пристрої та предмети повсякденного вжитку.

Інтернет речей – це концепція, яка об'єднує фізичні об'єкти, обладнані датчиками, мікроконтролерами, програмним забезпеченням та засобами комунікації, у єдину мережу. Ці пристрої можуть обмінюватися даними, автоматизувати процеси та виконувати задачі без втручання людини. Історія розвитку Інтернету речей демонструє, як людство поступово інтегрувало об'єкти навколишнього світу в цифровий простір, створюючи нові можливості для автоматизації, аналізу та управління.

Ідеї, які пізніше сформували концепцію IoT, виникли ще у середині XX століття. У 1960-х роках у Сполучених Штатах почали розробляти мережу ARPANET – прообраз сучасного інтернету. Хоча на той час іще не існувало ідеї Інтернету речей, ARPANET продемонструвала можливість обміну інформацією між віддаленими об'єктами через мережу. У цей період також почали з'являтися технології автоматичної ідентифікації об'єктів, такі як RFID. Перші RFID-системи дозволяли відстежувати місцеперебування об'єктів за допомогою радіосигналів, що стало одним із ключових елементів майбутнього IoT.

У 1980-х роках почали з'являтися персональні комп'ютери, які зробили цифрові технології більш доступними. Паралельно відбувався розвиток комунікаційних мереж. Одним із перших прикладів пристрою, який можна назвати прообразом IoT, був "розумний" кавовий апарат, створений у Кембриджському університеті в 1982 році. Цей пристрій підключали до локальної мережі, і він дозволяв користувачам віддалено перевіряти, чи є кава в машині. Хоча це рішення було дуже простим, воно продемонструвало, що фізичні об'єкти можна інтегрувати в цифрове середовище для зручності користувачів.

Новий етап розвитку Інтернету речей розпочався у 1990-х роках із появою інтернету. У 1991 році Тім Бернерс-Лі представив концепцію World Wide Web, яка дозволила об'єднати величезну кількість користувачів і пристроїв у глобальну

мережу. Сам термін "Інтернет речей" з'явився у 1999 році завдяки Кевіну Ештон, досліднику з Массачусетського технологічного інституту. Ештон працював над проектом автоматизації логістичних процесів у компанії Procter & Gamble і запропонував використовувати RFID-технології для відстеження товарів у режимі реального часу. Він зазначив, що Інтернет речей дозволить інтегрувати фізичний світ у цифровий простір, що відкриє нові можливості для бізнесу.

З початку 2000-х років розвиток IoT почав стрімко прискорюватися. Завдяки поширенню бездротових технологій, таких як Wi-Fi, Bluetooth і мобільний зв'язок третього покоління (3G), стало можливим підключення пристроїв до інтернету без фізичного кабелю. Це сприяло появі перших комерційних IoT-продуктів, зокрема "розумних" холодильників, які могли відстежувати запаси продуктів. У цей період Міжнародний союз електрозв'язку визнав IoT однією з найперспективніших технологій і звернув увагу на необхідність її стандартизації.

Перспективи розвитку IoT були окреслені у 2004 році, коли модель майбутнього середовища для взаємодії фізичних пристроїв передбачила важливі можливості для використання цієї технології в побутових умовах. У журналі Scientific American у 2004 році була опублікована стаття, яка описала концепцію "розумного будинку", де побутові прилади і системи, такі як будильник, кондиціонер, система поливу та охорони, можуть взаємодіяти через комунікаційні мережі та автоматично виконувати процеси на основі даних з датчиків.

У звіті Національної розвідувальної ради США у 2008 році IoT була включена до списку шести потенційно революційних технологій, зазначаючи, що масове підключення повсякденних предметів до Інтернету може вплинути на національну безпеку через можливі загрози для інформаційної безпеки.

Згідно з даними аналітиків компанії Cisco, період з 2008 по 2009 рік став "народженням" Інтернету речей: у цей час кількість пристроїв, підключених до Інтернету, вперше перевищила кількість людей, що використовують мережу, що ознаменувало перехід від "Інтернету людей" до "Інтернету речей".

З 2009 року у Брюсселі за підтримки Єврокомісії щорічно проходить

конференція "Internet of Things", на якій виступають єврокомісари, представники Європарламенту, високопосадовці та керівники провідних компаній, таких як SAP і Telefonica, а також науковці з університетів і дослідницьких лабораторій.

З початку 2010-х років IoT також став основою для розвитку "туманних обчислень" (Fog computing), які поширюють концепцію хмарних обчислень на величезну кількість розподілених пристроїв, що взаємодіють у рамках платформи IoT.

У 2010-х роках IoT став невід'ємною частиною технологічного прогресу. Розвиток мобільного зв'язку четвертого покоління (4G) та хмарних обчислень дозволив масштабувати IoT-рішення. З'явилися популярні платформи, такі як Google Cloud IoT, Amazon Web Services IoT та Microsoft Azure IoT, які надали бізнесам інструменти для створення та управління IoT-мережами. На ринок почали виходити численні споживчі пристрої, такі як розумні термостати, освітлення, охоронні системи та носяться гаджети. Водночас IoT почав впроваджуватися у промисловість, енергетику, медицину та сільське господарство.

З 2011 року компанія Gartner включає IoT у цикл розвитку нових технологій на стадії "технологічного тригера" і прогнозує досягнення зрілості в наступні десять років. У 2012 році Gartner публікує спеціальний цикл для технологій Інтернету речей, підкреслюючи значення цієї галузі [6].

Сьогодні Інтернет речей переживає фазу глобального поширення. За даними аналітичних компаній, кількість IoT-пристроїв у світі перевищила 30 мільярдів, і цей показник продовжує зростати. Технології п'ятого покоління (5G) значно покращили швидкість передачі даних та знизили затримку, що особливо важливо для критичних IoT-застосувань, таких як автоматизовані транспортні системи. Водночас інтеграція IoT із блокчейн-технологіями забезпечила вищий рівень безпеки даних, а використання штучного інтелекту дало змогу автоматизувати аналіз та управління системами.

Інтернет речей відіграє ключову роль у трансформації сучасного суспільства. У медицині IoT дозволяє створювати системи моніторингу стану

здоров'я пацієнтів у реальному часі. У транспорті – це основа для розвитку автономних автомобілів та інтелектуального управління дорожнім рухом. У сільському господарстві IoT-датчики використовуються для моніторингу умов вирощування культур, а в енергетиці – для підвищення ефективності використання ресурсів.

Однак із розвитком IoT виникають нові виклики. Питання кібербезпеки стає надзвичайно важливим, оскільки кожен підключений пристрій є потенційною точкою вразливості. Також проблемою залишається відсутність єдиних стандартів у галузі IoT, що ускладнює інтеграцію пристроїв від різних виробників. Окрім того, швидке зростання кількості пристроїв вимагає ефективних рішень для їх масштабованості та управління.

Таким чином, історія Інтернету речей демонструє, як технологічний прогрес поступово змінює спосіб взаємодії людей із навколишнім середовищем. IoT став важливою частиною цифрової епохи, яка продовжує формувати майбутнє суспільства, економіки та техніки.

1.3 Керування за допомогою Інтернету речей

Інтернет речей має великий потенціал для моніторингу та контролю міських і сільських інфраструктурних об'єктів, таких як мости, залізничні колії, транспортні мережі та енергетичні установки. Ця технологія забезпечує можливість спостерігати за структурними змінами, які можуть спричинити небезпеку, та дозволяє завчасно виявляти ризики й запобігати аваріям [7].

IoT значно сприяє розвитку будівельної галузі, зокрема через економію ресурсів, скорочення часу на виконання завдань і впровадження безпаперових процесів, що підвищує продуктивність. Завдяки збору та обробці даних у реальному часі, фахівці можуть приймати оперативні рішення, які дозволяють заощаджувати кошти та оптимізувати робочі процеси. Крім того, IoT сприяє

ефективному плануванню ремонтних і технічних робіт, полегшуючи координацію завдань між постачальниками послуг та користувачами цих інфраструктурних об'єктів.

Завдяки IoT-пристроям, моніторинг та управління критично важливою інфраструктурою стають більш ефективними. Такі пристрої можуть допомогти у покращенні координації під час надзвичайних ситуацій, а також забезпечують якісніше обслуговування об'єктів інфраструктури. Загалом, використання IoT в управлінні інфраструктурою сприяє подовженню строку служби об'єктів, зниженню витрат на експлуатацію та покращенню якості обслуговування у всіх галузях, що пов'язані з інфраструктурою (рис. 1.2).

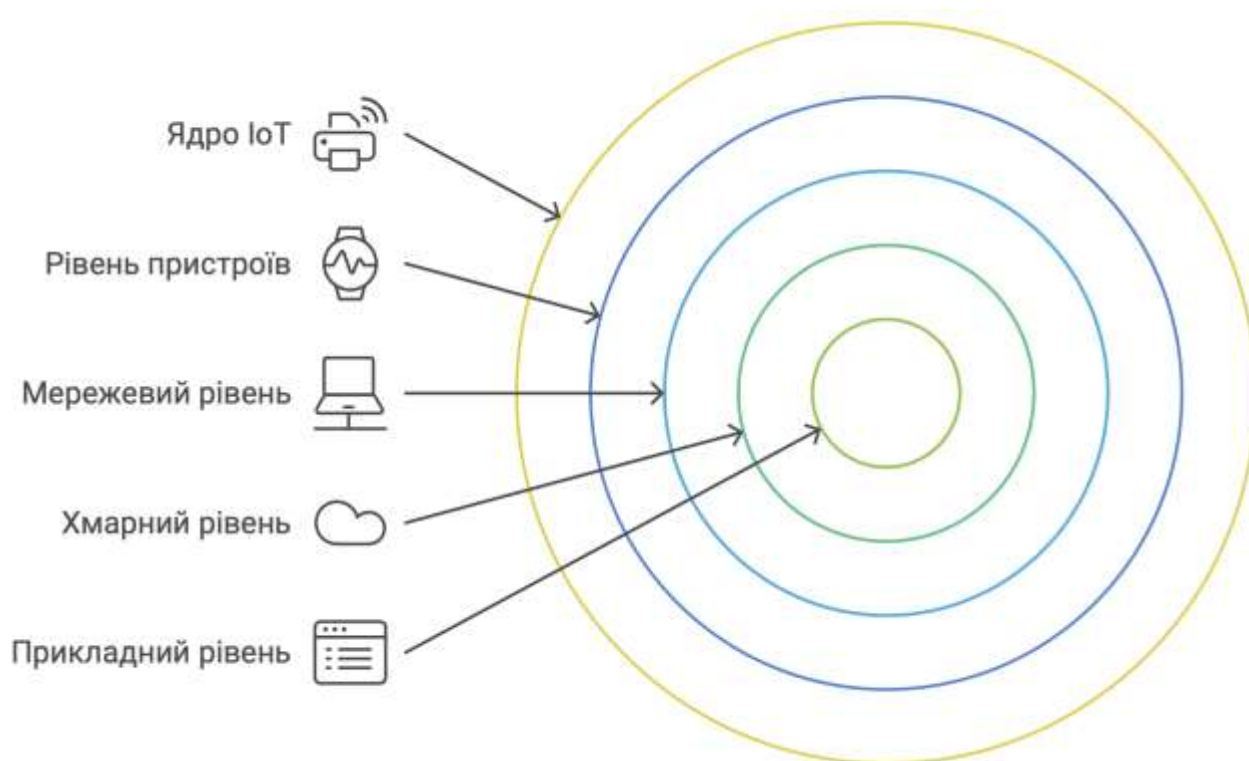


Рисунок 1.2 – Дизайн архітектури Інтернету речей

Інтернет речей знаходить широке застосування у промисловості, де він забезпечує мережеве управління, управління виробничим обладнанням, управління активами та виробничими процесами. IoT-технології, інтегруючи машини, датчики та системи контролю, сприяють швидкому виготовленню нових продуктів, дозволяють оперативно реагувати на зміни у попиті та оптимізувати

виробничі процеси та постачання в реальному часі. Такі інтелектуальні IoT-системи, впроваджені у виробництві, відкривають нові можливості для підвищення ефективності підприємств.

Цифрові системи управління, що автоматизують контрольні процеси, підвищують безпеку установок і сприяють оптимізації виробничих процесів. IoT також охоплює управління активами через моніторинг стану обладнання, статистичний аналіз і вимірювання для максимальної надійності роботи систем. Виробничі IoT-системи можуть бути інтегровані у Smart Grid, що дозволяє оптимізувати споживання енергії та керувати нею в реальному часі. Функції вимірювання, автоматизованого управління, оптимізації об'єктів та забезпечення охорони праці здійснюються за допомогою численних мережевих датчиків, що працюють на платформі IoT.

Промисловий Інтернет речей - це особливий напрямок IoT, що стосується промислових додатків та широко використовується в концепції Індустрії 4.0, яка передбачає четверту промислову революцію. ПоТ допомагає компаніям розвивати нові бізнес-моделі, підвищувати продуктивність, використовувати аналітику для інновацій та трансформувати робочу силу. За прогнозами, впровадження ПоТ здатне збільшити світовий ВВП на 12 трлн доларів до 2030 року, що робить його потужним драйвером економічного розвитку [8].

Ключовою метою інтелектуальних систем технічного обслуговування є зменшення непередбачуваних простоїв, що сприяє підвищенню продуктивності праці та скороченню витрат на технічне обслуговування на 30%. У цьому контексті кібер-фізичні системи виступають інтерфейсом між фізичним і цифровим світом та є основою для обробки промислових даних. Архітектура 5C (connection, conversion, cyber, cognition, configuration) дозволяє перетворювати зібрані дані на дії, оптимізуючи використання фізичних ресурсів і забезпечуючи більш раціональне управління виробничими процесами.

Інтеграція сенсорних та керованих систем, підключених до Інтернету речей, відкриває нові можливості для оптимізації споживання енергії, що є особливо актуальним у контексті зростаючого попиту на енергозберігаючі

технології. IoT пристрої можуть бути вбудовані в усі форми енергозберігаючих пристроїв - перемикачі, розетки, лампочки, телевізори та інші побутові прилади. Вони здатні взаємодіяти з комунальними системами, такими як енергетичні мережі, для оптимального балансу між виробництвом та використанням електроенергії.

Ці пристрої дозволяють користувачам ефективно управляти споживанням енергії, зокрема через віддалене керування. Завдяки інтеграції з хмарними інтерфейсами, користувачі можуть контролювати роботу своїх пристроїв дистанційно або централізовано. Крім того, функції планування дозволяють автоматизувати процеси, наприклад, включення та вимикання систем опалення, зміни умов освітлення тощо. Це дозволяє досягти значної економії енергії та зменшення витрат, що важливо як для домогосподарств, так і для комерційних об'єктів.

Особливо важливим є застосування IoT в Smart Grid (розумних енергетичних мережах). Вони забезпечують автоматичне збирання та обробку інформації про споживання енергії, що дозволяє покращити ефективність, надійність, економічність та стійкість процесів виробництва та розподілу електроенергії. Використовуючи Advanced Metering Infrastructure, що підключена до Інтернету, енергетичні компанії можуть не тільки збирати дані від кінцевих споживачів, а й автоматично управляти пристроями, що входять в систему автоматизації розподілу енергії [9].

Таким чином, IoT стає важливим інструментом для створення більш стійких, ефективних та економічних енергетичних систем, що мають можливість адаптуватися до змінюваних умов і забезпечувати оптимальне використання ресурсів.

Застосування IoT для природоохоронного моніторингу набуває все більшого значення, оскільки такі технології здатні забезпечити ефективний та постійний контроль за станом навколишнього середовища. Завдяки використанню спеціалізованих датчиків, IoT дозволяє здійснювати моніторинг різних аспектів навколишнього середовища, таких як:

- якість повітря - датчики можуть вимірювати концентрацію шкідливих газів, таких як вуглекислий газ (CO_2), діоксид азоту (NO_2), сірчаний ангідрид (SO_2) та інші забруднювачі, що дає змогу оперативно реагувати на зміни в екологічному стані;

- якість води - IoT-системи можуть контролювати показники води, такі як температура, рівень кисню, pH, забруднення та наявність шкідливих бактерій, що важливо для забезпечення здоров'я водних екосистем та безпеки водопостачання;

- ґрунт - за допомогою датчиків можна вимірювати рівень вологоти, кислотність, температуру та інші характеристики ґрунту, що є важливим для сільського господарства та природоохоронних організацій, які піклуються про стан природних ресурсів;

- спостереження за дикою природою - IoT дозволяє встановлювати датчики для відстеження руху тварин, моніторингу їх здоров'я та середовища існування, що має важливе значення для охорони біорізноманіття та боротьби зі змінами клімату.

Крім того, IoT може бути використаний для розробки систем раннього попередження про природні катастрофи, такі як землетруси або цунамі, що дозволяє терміново інформувати про небезпеку та координацію дій рятувальних служб. Такі системи вимагають інтеграції різних типів датчиків для відстеження сейсмічної активності та рівня води в океанах, що може дозволити швидше реагувати на загрози.

1.3.1 Географічне покриття та мобільність

IoT-пристрої можуть охоплювати велику географічну область, що робить їх ідеальними для моніторингу навколишнього середовища на територіях, де немає доступу до стаціонарних станцій або коли потрібне широке охоплення (наприклад, у віддалених районах, лісах або на морі). Такі пристрої можуть бути мобільними, що дозволяє розміщувати їх у важкодоступних місцях або переміщувати по мірі необхідності для отримання даних з різних регіонів [10].

Географічне покриття та мобільність є фундаментальними аспектами Інтернету речей, які визначають можливості інтеграції пристроїв у різноманітних

середовищах та забезпечення їх ефективної роботи. Ці аспекти стають особливо важливими в умовах швидкого розвитку технологій зв'язку, підвищення мобільності користувачів і розширення сфер застосування IoT.

Географічне покриття у контексті IoT стосується можливості підключення пристроїв до мережі у різних локаціях. На глобальному рівні це забезпечується завдяки розвитку телекомунікаційних технологій, таких як Wi-Fi, мобільний зв'язок (3G, 4G, 5G) та супутникові мережі. Кожна з цих технологій має свої переваги і недоліки. Наприклад, Wi-Fi підходить для локальних середовищ із високою щільністю пристроїв, таких як «розумні будинки» чи офіси, але має обмежене покриття. Мобільні мережі, навпаки, забезпечують значно ширше географічне охоплення, однак вимагають підтримки відповідних стандартів зв'язку, таких як LTE-M або NB-IoT. Супутниковий зв'язок використовується у віддалених місцевостях, де немає можливості розгорнути наземну інфраструктуру, наприклад, у морських транспортних системах чи для моніторингу природних ресурсів.

Для IoT, яке працює у глобальному масштабі, географічне покриття визначає, наскільки ефективно пристрої можуть взаємодіяти між собою та з центральними системами управління. Наприклад, у сфері логістики, де IoT використовується для відстеження вантажів у реальному часі, покриття має критичне значення. Завдяки глобальним технологіям зв'язку компанії можуть моніторити стан товарів на кожному етапі транспортування, незалежно від місця їх перебування.

Мобільність, у свою чергу, є ключовим фактором для забезпечення роботи IoT у динамічних середовищах. Вона стосується здатності пристроїв підтримувати безперервне підключення до мережі під час їх переміщення. Прикладом може бути використання IoT у транспортних засобах, де датчики постійно передають інформацію про місцезнаходження, стан автомобіля та навколишні умови. Мобільність IoT забезпечується завдяки інтелектуальному управлінню передачею даних між різними базовими станціями або точками доступу.

З розвитком технологій 5G мобільність у IoT досягла нового рівня. Ця технологія не лише забезпечує високу швидкість передачі даних, але й дозволяє мінімізувати затримки у передачі сигналу, що є критично важливим для таких додатків, як автономний транспорт чи розумні міста. Наприклад, у системах розумного управління дорожнім рухом датчики та камери в реальному часі збирають інформацію про потоки транспорту, яку аналізують і використовують для оптимізації роботи світлофорів чи створення маршрутів для автомобілів. Для цього необхідна як висока мобільність пристроїв, так і стійке географічне покриття.

Інший приклад мобільності в IoT – це пристрої для охорони здоров'я. Носимі гаджети, такі як фітнес-браслети або монітори серцевого ритму, дозволяють користувачам залишатися мобільними, водночас передаючи дані в режимі реального часу до медичних центрів. Це дає змогу лікарям оперативно реагувати на можливі ризики для здоров'я пацієнта, навіть якщо він перебуває далеко від лікарні.

Разом із перевагами географічного покриття та мобільності існують певні виклики. Одним із них є питання енергоефективності. Мобільні IoT-пристрої часто працюють від акумуляторів, тому тривале підключення до мережі може швидко виснажувати енергоресурси.

Для розв'язання цієї проблеми використовуються енергоефективні протоколи, такі як Bluetooth Low Energy або LoRaWAN, а також технології Harvesting Energy, які дозволяють пристроям генерувати енергію з навколишнього середовища.

Іншою проблемою є забезпечення безперебійного підключення пристроїв у динамічних середовищах. Для цього IoT-системи використовують механізми "перемикання" між точками доступу, щоб мінімізувати втрату сигналу під час руху. Наприклад, у транспортних системах це може включати передачу даних між базовими станціями мобільного зв'язку, коли транспортний засіб рухається між зонами покриття.

1.3.2 Стандартизація IoT та бездротове зондування

Завдяки стандартизації технологій IoT, що дозволяє підключати різні пристрої до єдиної мережі, і розвитку бездротових технологій зондування, можна ефективно зібрати дані з великих територій без потреби в громіздких і дорогих інфраструктурах. Це знижує витрати на встановлення моніторингових систем і дозволяє швидше отримувати точні дані в реальному часі. В результаті ці технології можуть стати революційними для екологічного моніторингу, оскільки вони надають нові можливості для швидкого збору та обробки інформації [11].

Загалом, впровадження IoT в природоохоронний моніторинг може істотно поліпшити контроль за станом навколишнього середовища, зробити моніторинг більш доступним і точним, а також забезпечити швидке реагування на екологічні загрози.

Інтеграція фізичних об'єктів у мережу Інтернету речей, які не обов'язково оснащені засобами підключення до мереж, вимагає використання технологій для їх ідентифікації. Хоча основою концепції IoT стала технологія RFID, для ідентифікації можуть застосовуватися й інші методи автоматичної ідентифікації, зокрема штрих-коди, QR-коди та технології визначення місцезнаходження в реальному часі, як-от GPS, що широко використовуються в сучасних смартфонах і навігаторах. В умовах розвитку Інтернету речей необхідно забезпечити унікальність ідентифікаторів пристроїв, що потребує стандартизації.

Для пристроїв, які безпосередньо підключаються до Інтернету, традиційним ідентифікатором є MAC-адреса мережевого адаптера, що дозволяє визначати пристрій на каналному рівні. При цьому кількість доступних адрес у системі MAC-48 практично безмежна, однак для додатків це може бути незручним рішенням. Значно більші можливості ідентифікації забезпечує протокол IPv6, який надає унікальні мережеві адреси, що дозволяє підключати понад 300 мільйонів пристроїв на кожного жителя планети.

Важливу роль в Інтернеті речей відіграють засоби вимірювання, які перетворюють інформацію про зовнішнє середовище на дані, що заповнюють обчислювальну систему необхідною інформацією. Для цього використовується

широкий спектр вимірювальних пристроїв - від простих датчиків (наприклад, температури, тиску, освітленості), приладів для обліку споживання (такі як інтелектуальні лічильники) до складних інтегрованих систем вимірювання. Одним із ключових викликів є забезпечення максимальної автономності таких пристроїв, зокрема, вирішення проблеми енергопостачання датчиків. Розробка ефективних рішень для автономного живлення сенсорів - таких як використання фотоелементів, перетворення енергії вібрацій, вітру чи бездротової передачі енергії - дозволяє масштабувати сенсорні мережі без збільшення витрат на їх обслуговування, таких як зміна батарейок або підзарядка акумуляторів.

Інтеграція з Інтернетом передбачає використання IP-адреси як унікального ідентифікатора для пристроїв. Однак через обмежені адресні простори в IPv4 (які дозволяють використовувати лише 4,3 мільярда унікальних адрес), об'єктам IoT необхідно буде застосовувати IPv6. Цей протокол забезпечує унікальні адреси мережевого рівня для не менше ніж 300 мільйонів пристроїв на кожного жителя Землі. У рамках Інтернету речей об'єктами будуть не лише пристрої з сенсорними можливостями, але й пристрої, що виконують певні функції (наприклад, лампочки або замки, керовані через Інтернет). Отже, успішний розвиток IoT у майбутньому значною мірою залежить від широкого впровадження IPv6, яке є необхідним для забезпечення масштабованості та стабільності інфраструктури.

Для бездротової передачі даних у контексті IoT важливу роль відіграють характеристики, такі як ефективність, відмовостійкість, адаптивність і здатність до самоорганізації мережі. Одним із стандартів, який визначає доступ до таких бездротових мереж, є IEEE 802.15.4. Цей стандарт є основою для протоколів, таких як ZigBee, WiFi, Bluetooth, 6LoWPAN, що дозволяє створювати енергоефективні персональні мережі [13].

ZigBee - це комунікаційна технологія, заснована на протоколі IEEE 802.15.4, і використовується для побудови низькошвидкісних бездротових приватних мереж. ZigBee має такі переваги, як низьке енергоспоживання, мала швидкість передачі даних, низька вартість і висока пропускна здатність [14]. Ця технологія особливо застосовується для передачі даних між пристроями, що

знаходяться на невеликій відстані один від одного, таких як периферійні пристрої (миші, клавіатури) та побутова електроніка (телевізори, DVD-плеєри), а також пристрої промислового управління (датчики, монітори, автоматизація).

WiFi - це локальна бездротова технологія, що працює на частотах 2,4 ГГц і 5 ГГц, і дуже добре підходить для передачі великих обсягів даних між пристроями. Однак вона потребує значних енергетичних витрат і має обмежену пропускну здатність, що робить її менш ефективною для довготривалого використання без регулярної заміни батарей у пристроях.

Однією з провідних технологій для розгортання Інтернету речей є PLC - технологія передачі даних по лініях електропередач. Вона відіграє важливу роль, оскільки багато IoT-додатків мають доступ до електричних мереж (наприклад, торгові автомати, банкомати, інтелектуальні лічильники та контролери освітлення, які вже підключені до мережі електропостачання). Крім того, протокол 6LoWPAN, який реалізує IPv6 поверх IEEE 802.15.4 або PLC, є відкритим стандартом, стандартизованим IETF, і є особливо важливим для розвитку Інтернету речей завдяки своїй універсальності та здатності забезпечити ефективну передачу даних у різних типах мереж.

1.4 Сучасний стан Інтернету речей

Інтернету речей приділяється значна увага на міжнародному рівні, зокрема з 2009 року у Брюселі, за підтримки Єврокомісії, регулярно проводяться конференції Annual Internet of Things, на яких виступають єврокомісари, науковці та лідери провідних IT-компаній. Прогнози аналітиків вказують на значне зростання популярності IoT у найближчі роки. Згідно з прогнозами Gartner, до 2020 року кількість пристроїв, підключених до Інтернету, досягне 26 мільярдів, а дохід від продажу обладнання, програмного забезпечення та послуг перевищить \$1,9 трлн. Деякі інші аналітичні агентства прогнозують ще більш

оптимістичні показники.

Великі світові ІТ-компанії вже активно змагаються за лідерство на ринку Інтернету речей. Так, корпорація Intel у 2014 році, після випуску свого чіпа «SoC Edison», оголосила конкурс Make it Wearable з призовим фондом \$1,3 млн на найкраще застосування технології IoT, а також створила підрозділ «Internet of Things Solutions Group» для розвитку цього напрямку. Компанія Google, на початку 2014 року, придбала за \$3,2 млрд фірму Nest Labs, яка розробляє інтелектуальні термостати, сприяючи впровадженню IoT технологій на американському ринку. Виробники побутової техніки також активно працюють у цьому напрямку. Наприклад, на виставці CES 2014 у Лас-Вегасі було представлено багато побутових пристроїв (холодильники, телевізори, пральні машини), здатних підключатися до Інтернету, і передбачається, що ринок таких технологій досягне обсягу \$80 мільярдів.

Лідерами у розробці та впровадженні Інтернету речей є країни з розвинутою індустрією мікропроцесорів та вбудованих комп'ютерів, зокрема США, Китай і Південна Корея. Водночас значний прогрес у цій галузі демонструють також європейські країни та Японія.

Станом на сьогодні IoT є одним із найдинамічніших напрямів розвитку сучасних технологій, який стрімко трансформує промисловість, бізнес та повсякденне життя. Завдяки інтеграції фізичних пристроїв з цифровими технологіями IoT створює глобальну мережу взаємопов'язаних пристроїв, що здатні збирати, аналізувати та обмінюватися даними в режимі реального часу. Це сприяє не лише підвищенню ефективності систем, але й створенню нових можливостей для розвитку різних галузей економіки.

Однією з головних характеристик сучасного стану IoT є його стрімке зростання. За оцінками аналітиків, кількість підключених пристроїв IoT у світі вже перевищила 15 мільярдів і, за прогнозами, зросте до 25-30 мільярдів до 2030 року. Найбільший внесок у це зростання роблять пристрої, що використовуються у промисловості (Industrial IoT), розумних будинках, транспорті, охороні здоров'я, сільському господарстві та розумних містах.

У сучасних IoT-системах активно використовуються різноманітні технології передачі даних, такі як Wi-Fi, Bluetooth, ZigBee, LoRaWAN, 4G/5G та супутниковий зв'язок. Кожна з цих технологій знаходить своє місце у різних сценаріях використання. Наприклад, LoRaWAN використовується для пристроїв з низьким енергоспоживанням і великим радіусом дії, тоді як 5G забезпечує надвисоку швидкість передачі даних і мінімальні затримки, що є критично важливим для автономного транспорту чи промислової автоматизації.

Однією з ключових тенденцій IoT є зростання значення штучного інтелекту та машинного навчання у аналізі великих обсягів даних, які генерують IoT-пристрої. Завдяки цим технологіям пристрої можуть не лише збирати інформацію, але й аналізувати її, прогнозувати майбутні події та приймати автономні рішення. Наприклад, у сфері охорони здоров'я це дозволяє відстежувати стан пацієнта в реальному часі та попереджати про можливі загрози для здоров'я.

Ще однією важливою рисою сучасного IoT є зростання уваги до кібербезпеки. Зі збільшенням кількості підключених пристроїв зростає ризик кібератак, які можуть порушувати роботу критично важливих систем. Тому розробники IoT-рішень активно впроваджують засоби захисту, такі як шифрування даних, багатофакторна автентифікація та блокчейн для забезпечення цілісності даних і довіри між пристроями.

У промисловому секторі IoT активно використовується для моніторингу та управління виробничими процесами, що дозволяє підвищувати ефективність виробництва, зменшувати витрати та мінімізувати простой обладнання. Наприклад, за допомогою сенсорів IoT компанії можуть прогнозувати поломки машин і проводити їхнє технічне обслуговування до того, як станеться аварія.

У сільському господарстві IoT сприяє розвитку концепції "розумного фермерства". Сучасні системи використовують сенсори для вимірювання вологості ґрунту, температури, рівня освітлення та інших параметрів. Завдяки цьому фермери можуть оптимізувати процеси зрошення, внесення добрив і збирання врожаю, підвищуючи продуктивність і зменшуючи негативний вплив

на навколишнє середовище.

У сфері розумних міст IoT дозволяє створювати інтегровані системи управління транспортом, освітленням, енергетикою та комунальними послугами. Наприклад, розумні світлофори можуть регулювати трафік на основі реального завантаження доріг, зменшуючи затори та викиди CO₂.

Окремо слід відзначити розвиток IoT у сфері охорони здоров'я. Носимі пристрої, такі як фітнес-браслети або медичні монітори, дозволяють користувачам постійно стежити за своїм станом здоров'я. Крім того, лікарі можуть дистанційно спостерігати за пацієнтами, що є особливо актуальним у віддалених регіонах.

Сучасний стан IoT характеризується також стрімким зростанням економічної значущості. Аналітики прогнозують, що ринок IoT до 2030 року досягне обсягу понад 1 трильйон доларів США. Це свідчить про те, що технологія стає ключовим рушієм інновацій і трансформацій у різних галузях.

Водночас існують певні виклики, які потребують вирішення. Одним із головних є стандартизація IoT. Сьогодні різні виробники використовують власні протоколи та технології, що ускладнює інтеграцію пристроїв між собою. Крім того, залишається актуальним питання енергоефективності IoT-пристроїв, особливо тих, які працюють у віддалених районах і не мають доступу до постійного джерела живлення.

Отже, сучасний стан Інтернету речей демонструє не лише його стрімкий розвиток, але й широкі перспективи для майбутнього. Завдяки інтеграції передових технологій IoT перетворюється на фундаментальний інструмент для вирішення глобальних проблем і підвищення якості життя. Водночас подальше вдосконалення технології вимагає зусиль щодо підвищення безпеки, енергоефективності та стандартизації, що стане ключовим фактором її сталого розвитку.

1.5 Існуючі проблеми безпеки у системі Інтернету речей

Інтернет речей здатний значно змінити повсякденне життя, надаючи користувачам новий рівень зручності та комфорту. Однак якщо елементи цієї системи не будуть належним чином захищені від несанкціонованого доступу, використання надійних криптографічних алгоритмів, це може призвести не до користі, а до шкоди, відкриваючи кіберзлочинцям можливість зламати інформаційну безпеку. Оскільки пристрої з вбудованими комп'ютерами зберігають значну кількість персональної інформації про власника, зокрема можуть визначати його точне місцезнаходження, доступ до таких даних може бути використаний зловмисниками для здійснення злочинів. Відсутність єдиних стандартів для захисту таких автономних мереж досі уповільнює впровадження IoT у повсякденне життя [15].

У 2013 році були оприлюднені результати дослідження, яке виявило загальний стан безпеки в Інтернеті. У 2012 році вчений перевіряв відкриті порти на всіх доступних IP-адресах. Для того, щоб впоратися з обсягом роботи, дослідник створив комп'ютерного хробака, який шукав пристрої з недостатнім захистом: ті, що не мали паролів або використовували дуже прості паролі (наприклад, «root» або «admin»). Створений ним ботнет, що отримав назву «Carna», зібрав понад 9 ТБ даних, виконав 52 мільйони запитів ICMP ping, 180 мільярдів службових записів і 2,8 мільярда запитів TCP SYN на 660 мільйонів IP-адрес. Загалом було опитано 71 мільярд портів, і хробак зміг поширитися на понад 400 тисяч пристроїв.

У 2013 році були оприлюднені вихідні коди хробака Aidra (також відомого як LightAidra). Цей хробак став одним із прикладів використання інтернету речей для здійснення кібератак.

У вересні 2016 року після публікації статті про угруповання, які продають послуги ботнетів для проведення DDoS-атак, вебсайт журналіста Брайана Кребса (Brian Krebs) став жертвою однієї з таких атак. Пік трафіку під час атаки досягав

665 Гб/с, що робить її однією з найбільших і найпотужніших відомих DDoS-атак. Оскільки хостинг-провайдер відмовився безкоштовно надавати свої послуги, сайт довелося тимчасово закрити до моменту знаходження нового хостера. Атака була здійснена за допомогою ботнета, що складався з інфікованих "розумних" відеокамер, що є частиною Інтернету речей. У жовтні того ж року зловмисники опублікували вихідний код шкідливого програмного забезпечення, відомого як Mirai, що створило ризик неконтрольованого поширення атак іншими злочинцями.

Ботнет Mirai став можливим через вразливість, яка полягала у використанні однакового, незмінного пароля, встановленого виробником, для доступу до облікових записів адміністраторів на "розумних" пристроях. Загалом було відомо про 61 різну комбінацію логін-пароль, що дозволяли отримати доступ до таких облікових записів за допомогою методу перебирання. Дослідження показали, що багато з вразливих пристроїв було виготовлено за допомогою компонентів китайських компаній XiongMai Technologies та Dahua. Станом на 23 вересня, коли атака досягла піку, в Інтернеті було знайдено понад 560 000 пристроїв, які були вразливими до такого типу атак.

Інтернет речей є одним із найшвидше зростаючих сегментів сучасних технологій, але поряд із його поширенням виникають серйозні виклики в галузі кібербезпеки. Оскільки IoT-системи складаються з мільярдів пристроїв, підключених до глобальної мережі, забезпечення їхньої безпеки стає критично важливим завданням. Особливості архітектури, масштабів та функціональності IoT створюють унікальні загрози, які значно відрізняються від тих, що характерні для традиційних комп'ютерних систем.

Одна з головних проблем безпеки IoT пов'язана з недостатньою захищеністю пристроїв. Більшість IoT-пристроїв є малопотужними, з обмеженими обчислювальними ресурсами, що ускладнює впровадження складних алгоритмів шифрування чи захисту даних. Це робить їх вразливими до атак, таких як перехоплення даних або маніпуляція командами. Крім того, багато пристроїв працюють на застарілому або уразливому програмному забезпеченні, яке часто не

оновлюється своєчасно через відсутність механізмів автоматичного оновлення.

Другою проблемою є відсутність єдиних стандартів у сфері безпеки IoT. На ринку присутня велика кількість виробників IoT-пристроїв, які використовують різні протоколи зв'язку, архітектури та методи автентифікації. Через це виникають складнощі в забезпеченні сумісності між пристроями, а також уніфікованого підходу до їх захисту. Відсутність стандартів призводить до нерівномірного рівня безпеки серед пристроїв, що підвищує ризик атак на менш захищені елементи системи.

Ще однією серйозною проблемою є недостатня увага до безпеки під час розробки IoT-пристроїв. У прагненні мінімізувати вартість і час на розробку, виробники часто нехтують необхідністю інтеграції базових механізмів захисту. Наприклад, використання стандартних паролів за замовчуванням, відсутність шифрування переданих даних або слабка автентифікація відкривають широкі можливості для злоумисників.

Масштабність IoT також створює ризики для конфіденційності даних. IoT-пристрої постійно збирають і обробляють величезні обсяги чутливої інформації, включаючи дані про місцезнаходження, стан здоров'я, споживання енергії тощо. У разі компрометації пристрою ці дані можуть стати доступними для неавторизованих осіб, що створює загрозу для приватності користувачів.

Загрозу також становлять атаки типу "злом ланцюга поставок" (supply chain attacks), коли злоумисники впроваджують уразливості ще на етапі виробництва IoT-пристроїв. Такі атаки важко виявити, і вони можуть масово впливати на величезну кількість користувачів.

Крім того, IoT-системи стають об'єктами атак типу DDoS (розподілені атаки відмови в обслуговуванні). Великі мережі незахищених пристроїв можуть бути використані для створення ботнетів, які виконують масштабні атаки на сервіси чи інфраструктури. Яскравим прикладом є ботнет Mirai, який у 2016 році використовував тисячі скомпрометованих IoT-пристроїв для атаки на провайдерів інтернет-послуг.

Вразливість до фізичних атак також є однією з проблем безпеки IoT.

Пристрої, які працюють у відкритих чи важкодоступних місцях, можуть бути піддані фізичному втручанню. Зловмисники можуть модифікувати пристрій, перехоплювати дані або навіть замінювати його фальшивим.

Не менш важливою є проблема безпечного управління автентифікацією та доступом до IoT-пристроїв. Часто автентифікація обмежується слабкими паролями, а відсутність багатфакторного підтвердження доступу дозволяє зловмисникам отримувати контроль над пристроями без значних зусиль.

У промислових IoT-системах додаткові загрози виникають через інтеграцію з критично важливими системами, такими як енергетика, транспорт або виробництво. Атаки на ці системи можуть мати катастрофічні наслідки, включаючи простої виробництва, порушення енергопостачання чи транспортного руху.

Отже, сучасний стан безпеки в IoT демонструє наявність значних викликів, які потребують невідкладного вирішення. Необхідні спільні зусилля розробників, виробників і регуляторів для створення стандартів безпеки, впровадження надійних механізмів автентифікації, регулярного оновлення програмного забезпечення та підвищення обізнаності користувачів про безпечне використання IoT-пристроїв. Лише комплексний підхід до безпеки дозволить мінімізувати ризики і забезпечити надійне функціонування IoT у сучасному світі.

1.6 Висновки до розділу

У цьому розділі була розглянута основна концепція Інтернету речей, його історія, ключові поняття, характеристики, технології, проблеми та сучасний стан.

Основна ідея Інтернету речей полягає в можливості підключення різноманітних об'єктів до мережі, обробки інформації, отриманої з навколишнього середовища, обміну цією інформацією та, залежно від результатів, прийняття рішень і виконання певних дій.

Також увага була зосереджена на дослідженні розгортання Інтернету речей у контексті розвитку розумних міст, що базується на порівняльному аналізі таких міст у різних країнах. Метод аналізу полягав у вивченні розгортання Інтернету речей як частини державних політик чи програм, що дозволяє застосовувати класичні інструменти оцінки. Цей підхід дозволив дослідити впровадження Інтернету речей не лише через технологічні характеристики, а й з урахуванням всіх інших важливих параметрів.

Було виявлено, що Інтернет речей і розумні міста ще далеко від досягнення своїх амбітних цілей, зокрема у задоволенні потреб і очікувань кінцевих користувачів. У рамках цього аналізу була запропонована модель вартості даних Інтернету речей, що організована в процесі створення та обробки даних. Модель передбачає наявність брокера даних, який структурує, координує та управляє потоком даних між постачальниками (на рівні інфраструктури) та кінцевими користувачами (на рівні послуг), забезпечуючи зв'язок між вихідними та інтелектуальними даними.

Впровадження більшої прозорості та створення спільного бачення ланцюга вартості та екосистеми є ключовим кроком для забезпечення сталого і економічно обґрунтованого розгортання Інтернету речей та розумних міст у майбутньому.

2 КЕРУВАННЯ ПОДІЯМИ У СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Керування даними

Застосунки Інтернету речей потребують гнучкого та масштабованого управління даними для пристроїв і подій. Щоб забезпечити надійну основу для цих застосунків, платформа Інтернету речей має відповідати цим ключовим вимогам. З точки зору управління даними, пристрої та події є окремими поняттями, що дозволяє виділити два основних об'єкти даних [16]:

- пристрої;

- події.

Пристрої: більшість IoT-додатків базуються на певних фізичних пристроях.

Типи пристроїв можуть значно варіюватися: від ручних електроінструментів до великих вантажівок.

Події: обробка подій, що генеруються пристроями, є критично важливою для більшості застосунків Інтернету речей. Ці події можуть включати технічні інциденти, наприклад, збій обладнання, або події, що відображають поведінку користувачів, наприклад, зацікавленість покупця у певному товарі чи магазині.

Ефективне управління пристроями та подіями в IoT-системах базується на створенні незалежних ієрархічних структур:

- малі автономні апаратні елементи - це можуть бути датчики, контролери та інші невеликі апаратні компоненти, які функціонують самостійно;

- пристрої - можуть підключатися до кількох апаратних елементів через локальні мережі, використовуючи спеціалізовані драйвери для різного обладнання. Такі пристрої зазвичай мають доступ до IoT-платформи через мережі мобільного зв'язку (GSM, EDGE) або через пряме підключення до Інтернету;

- системи систем - це група пристроїв, які об'єднуються в єдину систему, наприклад, електромережу, що складається з кількох електростанцій.

Перевага використання чітко структурованих ієрархій пристроїв в IoT-додатках полягає в тому, що основна платформа додатків (іноді звана програмним забезпеченням) може надавати широкий спектр функцій незалежно від типу пристрою. Ці функції включають:

- зв'язок між пристроями - забезпечує ефективний обмін інформацією між різними рівнями ієрархії, включаючи передачу подій від віддалених пристроїв до сервера, а також виконання операцій, ініційованих сервером, які надсилаються до пристроїв для виконання;

- базове управління - охоплює централізоване управління базою даних пристроїв, аналіз даних, безпечне опрацювання подій, виконання бізнес-правил і процесів, а також надання консолі керування для адміністраторів технічних

систем.

В IoT-додатках виділяють такі типи даних:

- елементи пристроїв - кожен пристрій заноситься до бази даних як окремий елемент, включаючи інформацію про його місцезнаходження, а також додаткові атрибути та характеристики;

- події, пов'язані з пристроями - кожен пристрій має повний запис усіх подій, пов'язаних із ним, включаючи технічні події, наприклад сповіщення про відмову.

Керування даними пристроїв та подій створює значні виклики для стратегій управління даними в IoT-додатках. Основними викликами є:

- обсяги даних - можуть швидко зростати в залежності від частоти збору інформації та кількості пристроїв. Наприклад, десять мільйонів смарт-лічильників, які зчитують дані кожні 15 хвилин протягом 20 років, генерують величезну кількість інформації;

- схеми даних - окрім структурованих даних (наприклад, показників лічильників), IoT-додатки працюють із напівструктурованими та неструктурованими даними. Наприклад, подія може включати додаткові дані, такі як цифрове зображення для документування події, або неструктурований запис у специфічному технічному форматі, що генерується спеціалізованим датчиком;

- еволюція схем даних - у великих IoT-системах неможливо забезпечити однакові конфігурації або версії апаратного та програмного забезпечення для всіх пристроїв у полі. Тому рішення для управління даними повинно підтримувати одночасну роботу з різними версіями пристроїв та подій. Крім того, часто виникає необхідність інтегрувати дані пристроїв і подій із серверними системами для аналітики та автоматизації процесів. Оскільки такі системи часто змінюються, важливо забезпечити можливість безперервного оновлення та адаптації схеми даних.

2.2 Керування учасниками

У сучасному світі смартфони оснащені технологіями, такими як NFC, GPS, Wi-Fi та BLE, які відкривають широкі можливості для автоматизації процесів. Зокрема, ці функції можуть значно полегшити реєстрацію учасників на заходах. Наприклад, за допомогою BLE смартфони відвідувачів можуть автоматично взаємодіяти з програмним забезпеченням заходу, реєструючи їх під час наближення до місця проведення. Після цього на мобільний пристрій учасника надсилається відповідне сповіщення. Такий підхід не лише економить час, а й дозволяє замінити ручний процес реєстрації автоматизованою системою, що зменшує потребу в залученні додаткового персоналу [17].

Існують різні технології, які використовуються для збору та обробки даних у різних сферах. Серед них найпоширенішими є RFID та iBeacon.

2.2.1 Технології для управління подіями RFID

RFID широко використовується в таких сферах, як логістика, бібліотеки, системи автоматичних платежів та парки розваг. Технологія працює за допомогою міток, закріплених на об'єктах, які містять інформацію про них. Вона дозволяє здійснювати автоматичну реєстрацію користувачів і взаємодію між системами.

Переваги RFID:

- не потребує фізичного контакту чи прямої видимості;
- забезпечує швидке та точне зчитування, близьке до 100% ідентифікації;
- працює навіть у складних умовах (бруд, фарба, вода, пластик тощо);
- пасивні мітки мають майже необмежений термін експлуатації;
- мітки здатні зберігати великий обсяг інформації та підтримують функції запису.

Недоліки RFID:

- у деяких випадках мітки можуть не деактивуватися повністю, що призводить до повторного спрацьовування.

- мітки можуть бути легко пошкоджені чи видалені з об'єкта;
- існує ризик використання міток для шпигунства без згоди власника;
- можливе несанкціоноване збирання персональних даних, наприклад, інформації з паспортів чи купленої літератури;
- мітки можна обманути за допомогою спеціальних пристроїв, які зчитують дані на відстані. такий пристрій дозволяє перехоплювати інформацію та повторно передавати її до системи.

Отже, використання RFID і iBeacon може значно спростити та автоматизувати процеси управління подіями, скоротити час очікування та підвищити ефективність. Однак ці технології також мають свої ризики, зокрема у сфері конфіденційності даних, що вимагає особливої уваги до питань безпеки.

2.2.2 Технології для управління подіями iBeacon

Зазвичай iBeacon застосовується в місцях із великою кількістю людей, таких як торговельні центри, вокзали чи аеропорти, для передачі корисної інформації у відповідний момент часу.

iBeacon - це технологія, яка використовує можливості смартфонів, зокрема BLE, NFC та GPS, для визначення місця розташування, надсилання сповіщень та інших взаємодій. Особливістю технології є те, що замість традиційного використання географічних координат (довготи і широти), iBeacon визначає відстань до пристрою на основі сигналу BLE, який випромінює фізичний пристрій, наприклад смартфон чи "розумний годинник" (рис. 2.1).

Технологія iBeacon, призначена для роботи в приміщеннях, доповнює традиційні сервіси позиціонування, такі як GPS чи сигнали мобільних операторів. Її можна використовувати в різних сценаріях.

Наприклад, з дозволу користувача (наданого шляхом встановлення спеціального додатка) iBeacon відкриває нові можливості для мобільного маркетингу в роздрібній торгівлі, надає додаткову інформацію відвідувачам музеїв чи виставок, а також дозволяє отримувати актуальні дані, незалежно від точного розташування користувача [17].



Рисунок 2.1 - Взаємодія смартфону з датчиком iBeacon

Використовуючи датчики BLE і WiFi, можна створювати карти тепла та руху, які відображають, наприклад, кількість відвідувачів торговельного центру відповідно до їхнього місцезнаходження. Ці дані дозволяють менеджерам подій оптимізувати організацію заходів і просторове планування місць проведення.

Крім того, такі карти дають змогу аналізувати найбільш популярні зони ("гарячі зони"), у яких відвідувачі проявляли найбільший інтерес. На основі цієї інформації можна розробляти нові стратегії для підвищення ефективності продажів продуктів. Таким чином, ці технології відкривають нові можливості для розвитку маркетингу (рис. 2.2).

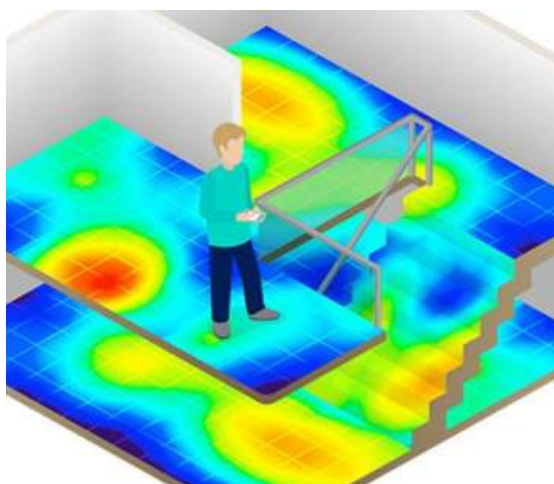


Рисунок 2.2 - "Гарячі зони" приміщення

Інтернет речей - це мережа повсякденних об'єктів, включаючи навіть пристрої, що використовуються для приготування їжі. IoT відстежує всі події, пов'язані з використанням харчових продуктів, і генерує кількісні дані про них. Автоматизовані системи обліку, які використовують технологію RFID, зберігають інформацію про придбані продукти. На основі цих даних система може прогнозувати, які продукти потрібно буде купити в майбутньому. Це сприяє оптимізації витрат і зменшенню фінансових витрат.

2.3 Розумне освітлення

Система освітлення, яка враховує погодні умови, може автоматично визначати час увімкнення ввечері або за наявності туману. Проєкт "розумного освітлення" передбачає обладнання ламп датчиками руху, які реагують на присутність людей та автомобілів. Також система може забезпечувати управління всіма освітлювальними пристроями "розумного будинку" через мобільний телефон за допомогою бездротового зв'язку.

Сучасне освітлювальне обладнання стало рушієм нової технологічної революції. Як важлива частина міської інфраструктури, вуличне освітлення є лідером у цифровій трансформації. Основною метою таких ініціатив є енергоефективність і стійкість. Застарілі вуличні освітлювальні системи можуть задовольняти базові потреби в освітленні для забезпечення безпеки дорожнього руху, однак їх енергоспоживання та витрати на обслуговування є надмірними через використання застарілих джерел світла. Це стимулює розробку нових технологій освітлення, які забезпечують значну економію енергії, підвищують надійність і продуктивність.

Впровадження світлодіодних технологій (твердотільного освітлення) стало значним кроком у поступовому заміщенні неефективних систем і прискорило перехід до "розумного освітлення". Це, своєю чергою, сприяє розвитку

інфраструктури для "розумного міста".

Комбінація мережевої комунікації, інтелектуального моніторингу та аналітичних можливостей дає змогу муніципалітетам динамічно керувати системами вуличного освітлення. Технології IoT дозволяють масштабувати системи управління великими мережами вуличного освітлення, обробляти та аналізувати великі обсяги даних, що генеруються світильниками, з метою підвищення ефективності освітлення, максимізації енергоощадності та зниження витрат на обслуговування.

Таким чином, технології IoT інтегрують світлодіодне вуличне освітлення з комп'ютерними системами, що дозволяє покращити функціональність міської інфраструктури.

Інтернет речей виходить за межі простої взаємодії між пристроями (M2M) у сфері управління освітленням [18]. Рішення на базі IoT можна впроваджувати у ширшому контексті розвитку "розумних міст" у всьому світі. Інтелектуальні системи вуличного освітлення можуть стати ключовими компонентами міської інфраструктури, забезпечуючи додаткові функції, такі як:

- моніторинг громадської безпеки;
- управління дорожнім рухом;
- метеорологічний моніторинг;
- екологічний контроль;
- інтелектуальна парковка;
- доступ до Wi-Fi;
- корисні вимірювання;
- голосові оповіщення тощо (рис. 2.3).

Вуличне освітлення на основі IoT являє собою цифрові системи освітлення, інтегровані в мережу Інтернет, де кожен ліхтар виконує функцію мережевого вузла для збору, передачі та прийому даних. Архітектура IoT базується на трирівневій ієрархічній моделі. На нижньому рівні знаходяться кінцеві вузли, встановлені на ліхтарях, які здійснюють зондування та вимірювання.



Рисунок 2.3 - “Розумне освітлення міста”

Другий рівень забезпечує комунікацію як із віддаленими серверами систем управління, так і з кінцевими вузлами. Найвищий рівень представлений прикладним шаром, до якого входить система дистанційного керування або сервер, що відповідає за оптимізацію керування, підвищення ефективності освітлювальних систем і виконання встановлених стратегій.

Система освітлення може включати різноманітні вузли, які спрощують моніторинг і контроль роботи ліхтарів та інших IoT-функцій. До таких вузлів належать світлозалежні резистори, пасивні інфрачервоні датчики, датчики струму та реле. LDR, або фоторезистори, слугують перетворювачами, які змінюють свій опір залежно від яскравості світла. Вони працюють за принципом фотопровідності, регулюючи яскравість ліхтарів відповідно до погодних умов. PIR-датчики виявляють потік чи щільність руху, визначаючи довжину хвиль інфрачервоного випромінювання, що проходить через їхню передню панель. Крім цього, система може включати годинник, який надає інформацію про час, датчики температури для визначення місцевих кліматичних умов, а також датчики струму, які перетворюють електричний струм (змінний чи постійний) на вимірювану напругу. Реле виконують функцію дистанційного вмикання або вимикання

ліхтарів.

Зібрані аналогові дані перетворюються на цифрові, а їх обробка здійснюється на другому рівні архітектури IoT за допомогою мікроконтролера, оснащеного вбудованим процесором, спеціалізованими інтегральними схемами або іншими компонентами. Для виконання завдань, таких як адаптивне керування яскравістю, LED-драйвери взаємодіють із мікроконтролерами. Останні також підключені до модулів зв'язку, які функціонують як шлюзи для передачі інформації між системами дистанційного керування, модулями зв'язку та ліхтарями.

Системи освітлення на базі IoT використовують комбінацію різних технологій зв'язку, що охоплюють довгий, середній та малий діапазони. Існує три основні типи зв'язку, які застосовуються для мережевих підключень у розумних системах вуличного освітлення:

- зв'язок через силові лінії (plc);
- широкосмугові лінії електропередач (bpl);
- бездротовий зв'язок, який реалізується за допомогою радіочастотних модулів.

Бездротова технологія є ключовим елементом для впровадження мережевих інтелектуальних систем вуличного освітлення, оскільки кабельні мережі можуть бути складними та дорогими в розгортанні, особливо в великих чи важкодоступних районах. У концепції IoT найкращими для взаємодії між численними розумними пристроями є низькоенергетичні стандарти комунікації. Бездротові мережі стають все популярнішими для інфраструктури IoT, забезпечуючи з'єднання пристроїв між собою та з хмарними сервісами. Одним із таких стандартів є ZigBee, який побудований на основі IEEE 802.15.4 для бездротових локальних мереж. ZigBee визначає протоколи високого рівня для зв'язку, що забезпечує надійність і великий радіус дії мереж.

Для реалізації ZigBee необхідне додаткове обладнання, таке як координатор, маршрутизатор і кінцеві пристрої ZigBee.

Серед інших технологій, які використовуються в IoT, є Wi-Fi, 6LoWPAN

(стандарт для адаптації зв'язку IPv6), Z-Wave, Bluetooth Low Energy, бездротові сенсорні мережі, Dash7 (протокол WSN, що працює на частоті 433 МГц і забезпечує кращу проникність через стіни порівняно з 2,4 ГГц), радіочастотна ідентифікація та зв'язок ближнього радіусу.

2.4 Розумний будинок

Розумний будинок (smart home) - це будівля або комерційне приміщення (наприклад, butik, офіс чи інша установа), яке оснащено високоякісними системами, що забезпечують ефективну роботу різних функцій через централізоване управління. Однією з ключових можливостей є інтеграція всіх електроприладів будівлі в єдину мережу, що дозволяє керувати ними з єдиного пульта або дисплея. Основна ідея полягає в тому, щоб управляти системами будинку бездротовим способом, забезпечуючи зручний доступ до всіх підключених пристроїв [19].

Однією з функцій розумного будинку є моніторинг та регулювання параметрів навколишнього середовища, таких як температура, вологість, освітлення тощо. Це дозволяє ефективно керувати споживанням енергоресурсів. Всі прилади можуть бути підключені до комп'ютерної мережі, що дає можливість керувати ними через ПК або віддалено через Інтернет. Завдяки інтеграції інформаційних технологій в житлове середовище, системи і пристрої в будинку узгоджують свої дії, порівнюючи задані програми з реальними зовнішніми умовами, наприклад, змінами температури чи освітленості (рис. 2.4).

Для визначення високотехнологічних характеристик приміщення часто використовують терміни: intelligent building, smart-home, digital home. Розумний будинок створюється за допомогою професійного проектування та програмування компаніями, які спеціалізуються на розробці проектів smart-home.



Рисунок 2.4 - Мультимедійний дисплей для керування розумним будинком

Програми, що інтегруються в алгоритми multi-room розумного дому, розробляються з урахуванням потреб мешканців та можливих ситуацій, які виникають через зміни в навколишньому середовищі або з питань безпеки. Особливістю smart-home є можливість керування з одного пульта, на якому можна натискати одну кнопку для створення бажаної атмосфери. Система multi-room аналізує навколишнє середовище та параметри приміщення, на основі чого приймає рішення і виконує команди користувача з відповідними налаштуваннями. Крім того, побутові електронні прилади в розумному будинку можуть бути об'єднані в домашню мережу Universal Plug'n'Play з виходом в інтернет.

Основні функції розумного дому:

- надійна та проста у використанні система охорони та відео-нагляду;
- автоматична корекція освітлення, залежно від часу доби та руху людей по приміщенню (це особливо важливо для сімей з дітьми або людьми похилого віку);

- автоматизація побутових турбот - у розумному будинку всі системи взаємодіють для виконання побутових завдань, що значно полегшує життя. це можуть бути такі функції, як полив саду чи його захист від сонця чи грози за допомогою погодних датчиків, відкриття дверей для вигулу домашніх тварин без участі господарів, і т.д.;

- контроль за витоками води чи газу;

- енергозбереження - інтелектуальний будинок є енергоефективною системою, де автоматика на 500 м² споживає лише близько 60 w;

- покращення умов для людей з обмеженими можливостями або літніх осіб завдяки автоматизації побутових завдань;

- можливість керувати будинком через інтерфейс, використовуючи телефонну лінію, мобільний зв'язок або інтернет - це дозволяє контролювати побутові прилади через смартфон або веб-браузер ще до приходу додому;

- централізоване управління всіма функціями з одного пульта-дисплея;

- інтерактивні плакати - це пристрої, що використовують технологію pfc для надсилання сповіщень користувачам, які знаходяться поруч. відвідувачі можуть взаємодіяти з плакатами або продуктами, що їх цікавлять, за допомогою своїх мобільних пристроїв, щоб отримати додаткову інформацію.

Одним із завдань IoT є збір даних з кожного пристрою. Організатори подій можуть об'єднувати всі зібрані дані учасників для створення списку потенційних клієнтів, які зацікавлені в пропонованих продуктах [20].

Це дає організаторам можливість:

- надавати цільові рекомендації учасникам;

- отримувати список потенційних відвідувачів, зацікавлених в їх пропозиціях;

- привертати увагу відвідувачів до певних об'єктів, які знаходяться поруч;

- оптимально розподіляти відвідувачів по виставковому майданчику, зменшуючи переповненість в окремих зонах.

2.5 Обробка відео у потоковому режимі

Потокова обробка - це технологія, яка дає змогу додаткам здійснювати обробку поточних даних у режимі реального часу, включаючи їх збір, інтеграцію, візуалізацію та аналіз. Вона дозволяє швидко обробляти великі обсяги даних, що надходять з різних джерел, у реальному часі (рис. 2.5).

Потокова обробка та потокова аналітика дозволяють ефективно обробляти великі обсяги даних Інтернету речей, не порушуючи працездатності існуючих джерел даних, систем зберігання та корпоративних інфраструктур. Однією з основних переваг потокової обробки є можливість працювати з даними як з безперервним потоком, що рухається від минулого до майбутнього, а не як зі статичними таблицями. Це дозволяє швидше адаптуватися до змін у бізнес-аналітиці та потребах компаній. Результати аналізу створюються як безперервні операції.

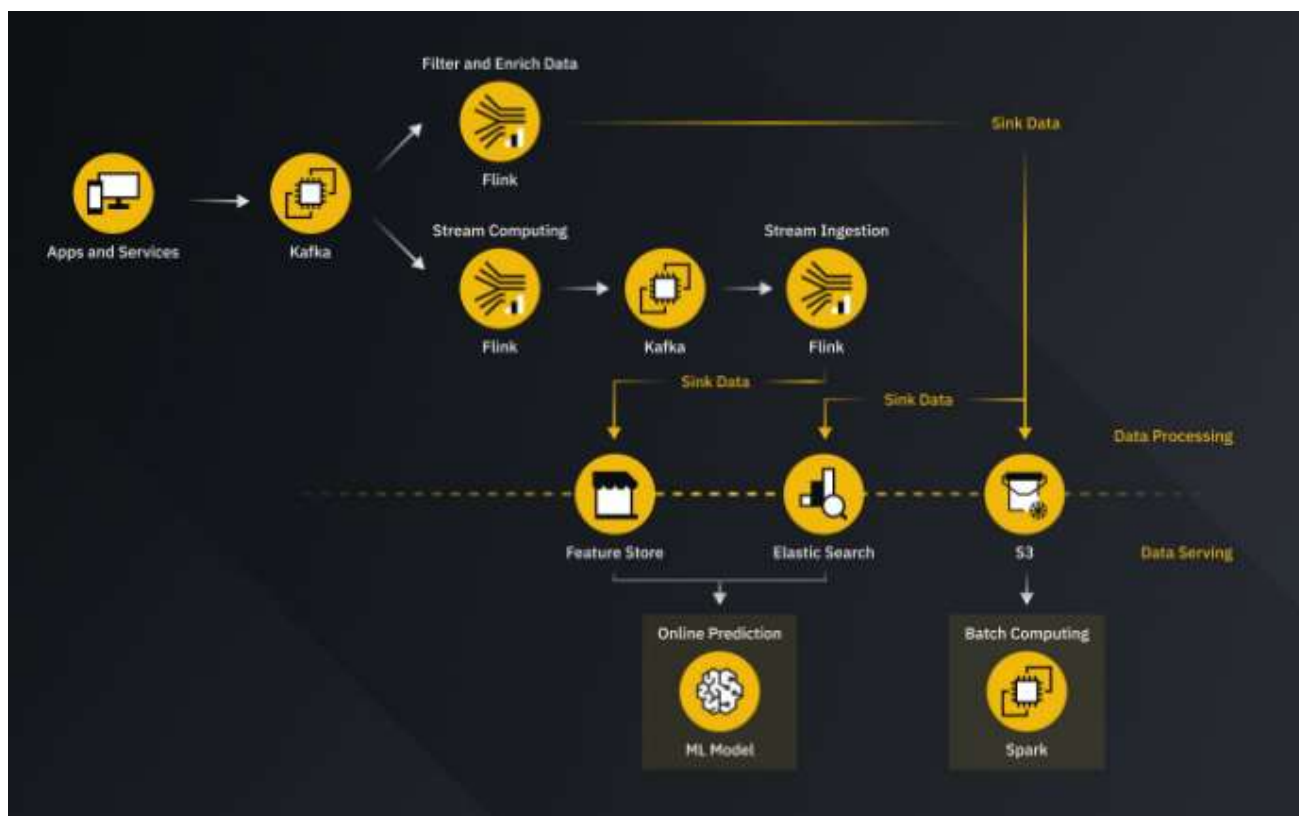


Рисунок 2.5 - Потокова обробка даних в реальному часі

Наприклад, компанії можуть аналізувати продажі в реальному часі, автоматично повторно замовляючи продукцію або коригуючи ціни залежно від поточних продажів по регіонах

Потокова обробка в режимі реального часу вирішує низку завдань у рамках розгортання Інтернету речей, зокрема:

- обробка великої кількості поточних подій (збирання, регулювання, фільтрація, автоматизація, прогнозування, моніторинг, попередження);
- швидка інтеграція з інфраструктурою та джерелами даних;
- виявлення аномалій;
- реабілітація та адаптація до змінних ринкових умов у реальному часі;
- продуктивність і масштабованість при зростанні обсягів та складності даних;
- аналітика в масштабах іот - пошук та перегляд даних у реальному часі, постійна обробка запитів;
- автоматизовані сповіщення;
- захист даних через сповіщення в реальному часі;
- миттєва реакція на запити споживачів.

Сьогодні технологія потокової обробки широко застосовується в різних галузях та урядових органах, де потоки даних генеруються через IoT. Одним із ключових аспектів є безпека даних, оскільки сучасні системи оповіщення потребують аналізу шаблонів даних у реальному часі. Лише потокова обробка дозволяє фільтрувати, агрегувати та аналізувати дані за мілісекунди. У рамках IoT потокова обробка використовується для моніторингу мережі, виявлення шахрайства, управління розумними замовленнями, ціноутворенням, керування ринковими даними та багатьма іншими завданнями.

Потокова обробка дозволяє швидко вирішувати проблеми, що виникають із даними в реальному часі, покращуючи задоволеність клієнтів та ефективність роботи організацій і урядів.

2.6 Обробка подій

Комплексна обробка подій (Complex Event Processing) - це новітня мережна технологія, що активно застосовується в Інтернеті речей. Вона використовує розподілені на основі повідомлень системи, бази даних та програми для обробки даних у реальному часі. CEP перетворює вхідні дані про події на більш складні та корисні дані, що допомагає краще розуміти події, які відбуваються [19]. Основною ідеєю є використання даних про події для прийняття рішень і покращення ситуаційної обізнаності у реальному часі. Вона поєднує інформацію з кількох джерел для виявлення подій або шаблонів, що дозволяє отримати більш комплексні рішення, які допомагають в управлінні подіями, прогнозуванні ситуацій, оцінці загроз і можливостей.

CEP заснована на кількох основних технологіях:

- виявлення патернів подій;
- абстракція подій;
- моделювання ієрархії подій;
- визначення співвідношень між подіями (наприклад, тимчасові залежності);
- абстракції процесів, керованих подіями.

Ця технологія має величезне значення для швидкої реакції на важливі події та зміни в режимі реального часу. Зі зростанням кількості датчиків та інтелектуальних пристроїв, що збирають дані, здатність швидко реагувати на події стає критично важливою для бізнесу та інших організацій. Тому CEP швидко стає важливим рішенням для розгортання IoT-систем, особливо коли йдеться про ситуації, де невчасна реакція може призвести до великих втрат.

Обробка потоків подій (Event Stream Processing) - це набір технологій, які використовуються для побудови інформаційних систем, що обробляють потоки подій. Основним завданням ESP є виявлення значущих шаблонів у потоках подій (даних), а також здійснення пошуку взаємозв'язків між подіями, кореляцію, аналіз

ієрархії подій та інших аспектів, таких як аналіз часових рядів і складових подій.

ESP включає в себе технології для візуалізації подій, їх зберігання, програмне забезпечення та мови програмування для обробки подій. Ця технологія активно використовується для:

- виявлення шахрайства в фінансових установах;
- оперативного аналізу активностей на фондових ринках;
- оцінки продуктивності обладнання в різних галузях, наприклад, у нафтовій та газовій промисловості;
- аналізу відтоку клієнтів і проведення маркетингових кампаній в телекомунікаціях.

ESP дозволяє швидко аналізувати величезні обсяги подій, що надходять з різних пристроїв. Події зберігаються в пам'яті, що дає змогу проводити більш складні маніпуляції з ними в реальному часі. Це допомагає оперативно виявляти патерни, фільтрувати та нормалізувати дані, а також забезпечувати ефективне реагування на зміни у зовнішньому середовищі (рис. 2.6).

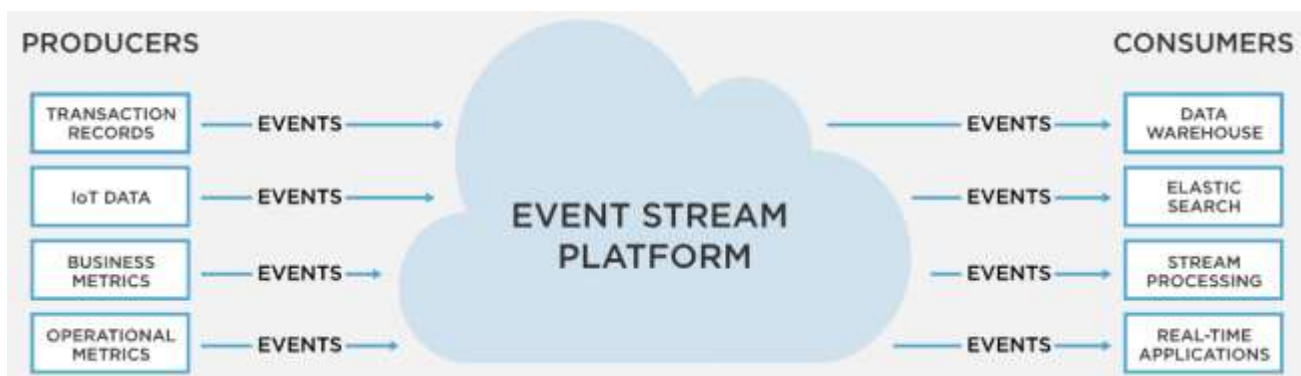


Рисунок 2.6 - Обробка потоків подій

Обробка потоків подій використовує кілька методів для керування потоками даних, що є важливими для ефективної роботи Інтернету речей. Ось основні методи, які застосовуються в ESP для обробки даних.

Методи керування потоками даних в ESP [20]:

- оцінка (data evaluation) - ESP стандартизує дані, коли вони надходять. це включає прості перетворення та застосування правил для нормалізації або

підготовки даних до подальшої обробки. завдяки цьому система може отримати чітке уявлення про потік даних і забезпечити його узгодженість;

- агрегація даних дозволяє об'єднувати потоки даних з різних джерел для подальшого аналізу. це важливо для виявлення патернів або тенденцій на основі сукупної інформації, що надходить з пристроїв IoT;

- кореляція ESP дозволяє підключатися до кількох потоків даних та виявляти взаємозв'язки між ними. наприклад, система може виявити серію подій, таких як зміни стану пристроїв: коли стан а був застосований на b, а потім на c. цей метод дозволяє відслідковувати розвиток подій і вчасно реагувати на них;

- тимчасовий аналіз (temporal analysis) дає змогу оцінювати, як події розвиваються з часом. це включає в себе відстеження подій на основі часу або виявлення певних шаблонів, таких як перевищення порогових значень для системи, що може вказувати на проблеми або потребу у втручанні.

Роль обробки потоків подій в IoT [21]:

- виявлення цікавих подій та запуск відповідних дій ESP дозволяє визначати складні схеми в режимі реального часу на конкретних пристроях IoT. Наприклад, система може виявити несправності у роботі обладнання або очікувані події обслуговування. Крім того, вона може виявляти потенційне шахрайство або ініціювати маркетингові пропозиції в реальному часі;

- сукупна інформація для моніторингу ESP активно використовується для постійного моніторингу даних від датчиків та пристроїв. Це дозволяє системам виявляти тенденції, корелювати певні порогові значення (наприклад, коли температура або вологість перевищує задані межі), що сигналізує про потенційні проблеми. Це допомагає вчасно попередити про можливі ризики;

- очищення та перевірка даних датчиків є одним з викликів для IoT є "брудні" дані, тобто дані, які можуть бути неповними, некоректними або містити різноманітні формати і час передачі. ESP включає методи очищення та перевірки якості даних, що дозволяє фільтрувати, нормалізувати та перевіряти достовірність даних перед їх подальшим використанням;

- прогнозовані та оптимізовані операції в режимі реального часу дозволяє

не лише реагувати на події, а й прогнозувати можливі ситуації в реальному часі. Завдяки розширеним аналітичним алгоритмам, які використовують історичні дані, ESP дозволяє системам передбачати, як події, що відбуваються, можуть вплинути на майбутні процеси. Наприклад, в транспорті можна прогнозувати, як прибуття поїзда або автобуса вплине на рух інших транспортних засобів.

Переваги використання ESP:

- швидка реакція на події та зміни в реальному часі;
- покращення обізнаності про стан пристроїв та ситуацію загалом;
- оптимізація операцій та прийняття рішень на основі поточних даних;
- підвищення ефективності управління ризиками та моніторингу.

Таким чином, технологія обробки потоків подій (ESP) є потужним інструментом для аналізу даних з пристроїв IoT у реальному часі, що дозволяє не тільки оперативно реагувати на події, але й передбачати їх та оптимізувати операції для досягнення кращих результатів.

2.7 Висновки до розділу

У цьому розділі було розглянуто основні об'єкти даних, способи їх управління, ієрархічні структури керування, а також ключові технології впровадження Інтернету речей, такі як iBeacon та RFID, які сприяють відстеженню та збору необхідних даних, зменшують час очікування та трудові витрати на управління подіями. Було наведено приклади їх використання.

Головною метою концепції Інтернету речей є автоматизація процесів і подій, які можуть відбуватися без участі людини, на основі аналізу взаємодії "розумних пристроїв". Це охоплює зміни в побуті, виробництві, мобільних пристроях та індустріальних секторах. Основні функції цієї концепції включають полегшення повсякденного життя (наприклад, через "розумні будинки" і "розумне харчування"), підвищення ефективності роботи (інтерактивні плакати, карти

тепла і рухів), зниження фінансових і матеріальних витрат (автоматизоване управління учасниками), а також енергоефективність ("інтелектуальне освітлення").

Також було розглянуто основні технології для управління подіями в реальному часі, такі як потокова обробка подій, комплексна обробка подій і обробка потоків подій. Приведено приклади їх застосування, основні функції, завдання та сфери використання. Ці технології дають змогу аналізувати, збирати та обробляти потоки даних і подій у реальному часі, приймати оперативні рішення та знижувати ризики виникнення проблем.

З ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ iBEACON В РЕЖИМІ РЕАЛЬНОГО ЧАСУ У СИСТЕМІ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Опис технологій для використання

iBeacon - це технологія, створена компанією Apple та презентована на конференції WWDC у 2013 році. Відтоді різні виробники розробили сумісні з iBeacon апаратні передавачі, які зазвичай називають маяками (рис. 3.1). Це малопотужні пристрої Bluetooth, що можуть інформувати найближчі пристрої на базі iOS про свою присутність. Завдяки цій технології смартфони та інші пристрої здатні виконувати певні дії, якщо вони перебувають у безпосередній близькості до iBeacon [22].

iBeacon використовує BLE для передачі унікального ідентифікатора, який розпізнається через додаток або операційну систему. Цей ідентифікатор разом із кількома додатковими байтами даних дозволяє визначати фізичне місцезнаходження пристрою, відстежувати користувачів або виконувати дії на основі їхнього розташування. Технологія iBeacon також може використовуватися як система внутрішнього позиціонування, що допомагає смартфонам визначати своє приблизне розташування.



Рисунок 3.1 - Датчики iBeacon

Наприклад, у магазині програмне забезпечення смартфона здатне визначити його відносну близькість до iBeacon. Це дозволяє роздрібним магазинам пропонувати клієнтам спеціальні акції через мобільний маркетинг, здійснювати мобільні платежі та навіть надсилати персоналізовані повідомлення в конкретній зоні магазину, на зупинці чи в кімнаті. Такий підхід подібний до раніше використовуваних georush-технологій на основі GPS, але має менший вплив на витрати заряду акумулятора та забезпечує більшу точність.

Головною відмінністю iBeacon від інших технологій на основі місцезнаходження є те, що передавальний пристрій (маяк) працює лише як односторонній передавач, а прийом сигналу здійснюється смартфоном або іншим пристроєм. Для роботи обов'язковою умовою є встановлення на пристрій

спеціального додатка, який взаємодіє з маяками. Це забезпечує контроль за відстеженням користувачів: лише додаток може збирати дані, а не сам iBeacon.

iBeacon — це технологія, розроблена компанією Apple для визначення місцезнаходження та передачі інформації між пристроями через Bluetooth Low Energy.

Однак існує низка аналогів iBeacon, які пропонують схожі можливості та використовуються для різних завдань. Розглянемо деякі з них.

3.1.1 Eddystone (Google)

Eddystone - це відкритий протокол маячків (beacons), розроблений компанією Google. Він є основним конкурентом iBeacon і підтримує різні типи даних, які можуть транслюватися маячками.

Особливості:

а) підтримує декілька форматів передачі даних:

1) Eddystone-UID — ідентифікатор маячка;

2) Eddystone-URL — трансляція URL-адрес для інтеграції з фізичним вебom;

3) Eddystone-TLM — дані телеметрії (температура, батарея тощо);

б) працює на платформах iOS, Android та інших пристроях із підтримкою BLE;

в) має відкритий вихідний код.

Сфери застосування:

- промоакції в магазинах;

- навігація в приміщеннях;

- моніторинг фізичного стану пристроїв.

3.1.2 AltBeacon (Radius Networks)

AltBeacon — це відкритий стандарт маячків, створений компанією Radius Networks. Він був розроблений як універсальна альтернатива iBeacon із можливістю кращої сумісності.

Особливості:

- відкритий протокол, який можна кастомізувати;

- підтримує android і ios;
- менш обмежений ліцензійними умовами, ніж iBeacon або Eddystone.

Сфери застосування:

- логістика та відстеження;
- автоматизація "розумних будинків";
- рекламні кампанії.

3.1.3 Kontakt.io Beacons

Kontakt.io - один із провідних виробників BLE-маячків, які підтримують одночасно iBeacon, Eddystone та інші стандарти.

Особливості:

- гнучкість у налаштуваннях і підтримка мультиформатності;
- маячки з додатковими датчиками (температури, вологості, руху);
- хмарна платформа для управління маячками та даними.

Сфери застосування:

- навігація в торговельних центрах та аеропортах;
- медичні заклади;
- розумні офіси.

3.1.4 Estimote Beacons

Estimote — це платформа маячків, яка використовує BLE для роботи з iBeacon, Eddystone та власними стандартами.

Особливості:

- маячки оснащені датчиками руху, температури та світла;
- висока якість матеріалів і довгий час роботи батареї;
- інтеграція з власною платформою для управління маячками.

Сфери застосування:

- навігація в музеях і торговельних центрах.
- інтерактивний маркетинг.
- "розумні простори".

3.1.5 Gimbal Beacons

Gimbal — це BLE-маячки, які, окрім функцій iBeacon, надають можливості глибокої персоналізації та збору даних.

Особливості:

- підтримка iBeacon і Eddystone;
- інтеграція з платформою аналітики gimbal для створення персоналізованих пропозицій;
- підтримка геозонування (geofencing).

Сфери застосування:

- торгові майданчики;
- організація подій;
- реклама в режимі реального часу.

Ці аналоги надають розширені функції та можливості, які можна адаптувати до різних потреб і середовищ. Вибір між ними залежить від конкретних вимог проекту. Порівняння iBeacon та аналогів надано у таблиці 3.1.

Таблиця 3.1 - Порівняння iBeacon та аналогів

Технологія	Підтримка форматів	Особливості	Сфери застосування
iBeacon	iBeacon	Простота використання, інтеграція з iOS	Маркетинг, інтерактивні рішення
Eddystone	UID, URL, TLM	Відкритий код, мультиплатформність	Навігація, промоакції
AltBeacon	AltBeacon	Відкрита архітектура, гнучкість	Логістика, 'розумні будинки'
Kontakt.io	iBeacon, Eddystone	Датчики, хмарне управління	Торгові центри, медицина
Estimote	iBeacon, Eddystone, власний	Багато датчиків, довговічність	Музеї, розумні простори
Gimbal	iBeacon, Eddystone	Персоналізація, аналітика	Події, геозонування

3.2 Принцип роботи технології

Маяк (передавач) періодично (з інтервалом від однієї до кількох секунд) передає рекламні пакети (advertising packets) за стандартом BLE без встановлення з'єднання. Ці пакети містять заголовок і наступне корисне навантаження [23]:

- UUID - 128-бітний унікальний ідентифікатор, який визначає групу маяків, їх тип або приналежність до однієї організації;
- Major - 16-бітне беззнакове значення, що дозволяє групувати маяки з однаковим UUID;
- Minor - 16-бітне беззнакове значення для додаткового групування маяків із однаковим UUID та Major;
- Measured Power - рівень сигналу на відстані 1 м від передавача. Це 8-бітне значення у dBm, яке використовується для оцінки близькості (proximity) маяка до приймача (мобільного пристрою).

Для визначення відстані до маяка (ranging) використовується реальне значення рівня сигналу у dBm, яке порівнюється із "Measured Power". Чим далі приймач від маяка, тим більша різниця між цими значеннями.

У разі використання кількох маяків, окрім визначення відстані до кожного, можна обчислити місце розташування приймача. Для цього застосовують методи:

- трилатерація - обчислення позиції за відстанями до кількох маяків;
- відбитки (Fingerprinting) - попередній запис векторів значень RSSI для набору точок у приміщенні. Під час навігації виміряні дані порівнюються з цими «відбитками», і обирається найбільш відповідна точка.

Після визначення місця розташування мобільний додаток може виконати певні дії, наприклад, показати відповідну інформацію.

Однак рівень сигналу залежить від відстані лише за умови, що радіосигнал поширюється безперешкодно. У реальних умовах приміщень на RSSI впливають такі фактори, як багатопроменеве поширення (multipath propagation), що може викликати як зниження, так і завищення рівня сигналу. Для покращення точності

застосовуються алгоритми згладжування.

Протокол iBeacon запровадив концепцію маякового регіону. Важливо зазначити, що додатки, які працюють із маяками, можуть визначати як окремі маяки, так і їхні групи.

На відміну від звичайного розуміння регіонів, які часто базуються на географічних координатах (наприклад, даних GPS, широті або довготі), *регіон iBeacon* визначається трьома основними характеристиками, спільними з маяками: UUID, Major і Minor.

При моніторингу регіонів визначення здійснюється на основі загальних тегів, що об'єднують кілька маяків, або за допомогою конкретних ідентифікаторів маяка. У цьому контексті фізичне уявлення регіону є діапазоном усіх маяків, що належать до цього регіону.

Моніторинг регіону забезпечує можливість додатку визначати момент, коли пристрій потрапляє в діапазон маяків або виходить з нього (рис. 3.2). Для реалізації цієї функціональності застосовується мова програмування Swift і середовище розробки Xcode.

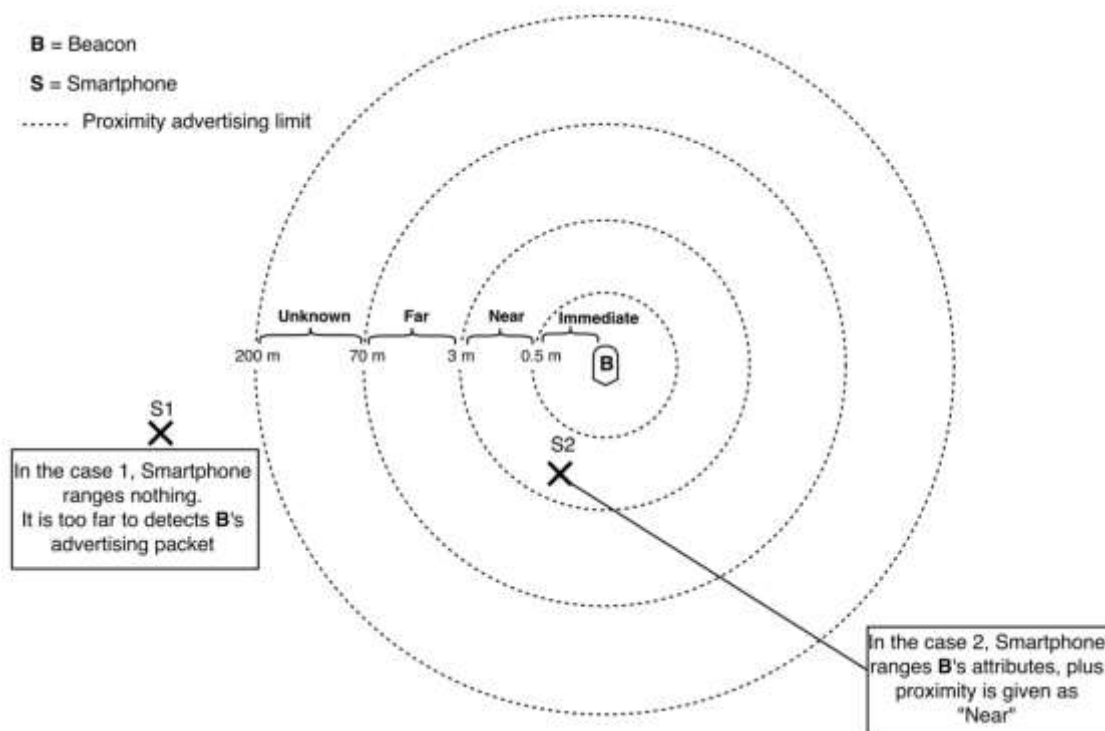


Рисунок 3.2 - Моніторинг регіону

На початковому етапі потрібно внести зміни в налаштування проєкту: активувати використання BLE та GPS у фоновому режимі (рис. 3.3, 3.4). Це дозволить додатку працювати з iBeacon навіть за відсутності взаємодії користувача з пристроєм.



Рисунок 3.3 - Налаштування BLE



Рисунок 3.4 - Налаштування дозволів на використання BLE і GPS

Загальна архітектура роботи системи представлена на рисунку 3.5.

Наступним кроком у реалізації моніторингу регіонів є створення екземпляра класу CLLocationManager, який відповідає за управління геолокацією та взаємодію з маяками [24]. У цьому екземплярі налаштовуються делегати для

обробки подій, зокрема `didEnterRegion` і `didExitRegion`.

Метод `didEnterRegion` викликається, коли пристрій входить у визначений діапазон маяків.

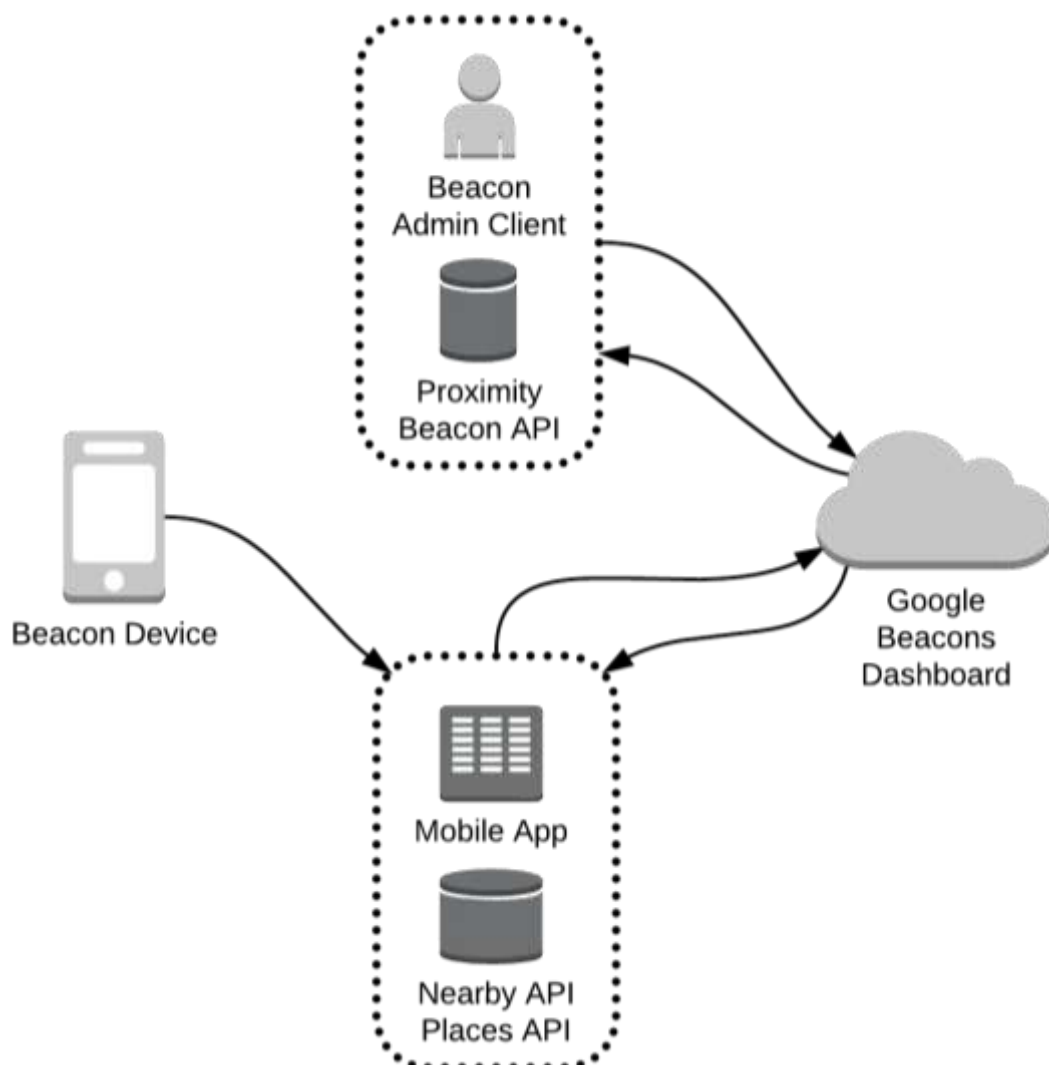


Рисунок 3.5 – Архітектура роботи системи

Метод `didExitRegion` активується, коли пристрій виходить за межі цього діапазону.

Варто зазначити, що події виходу з регіону можуть бути відкладені на приблизно 30 секунд після фактичного виходу користувача. Однак події входу, як правило, фіксуються практично миттєво, з мінімальною затримкою. Це забезпечує точну та оперативну реакцію додатку на зміну положення пристрою відносно маяків (рис.3.6).

```

Let monitoringManager = CLLocationManager(),
Let uuid = UUID(uuidString: "85a99e33-bbbe-4763-a66b-
4d3a3edec09b")!
Let major = CLBeaconMajorValue(12)
Let minor = CLBeaconMinorValue(1)
Let region = CLBeaconRegion(proximityUUID: uuid, major: major,
minor: minor, identifier: "iBeacon")
monitoringManager.startMonitoring(for: region)

```

Рисунок 3.6 - Події входу із мінімальною затримкою

Після завершення налаштування моніторингу регіонів необхідно реалізувати виклики двох методів делегування: `didEnterRegion` і `didExitRegion`. Ці методи дозволяють реагувати на події входу або виходу з регіону, визначеного маяками.

Метод `didEnterRegion` викликається, коли пристрій входить у визначений регіон маяків (рис. 3.7). У ньому можна виконувати певні дії, наприклад:

- відправляти сповіщення користувачу;
- відображати релевантну інформацію;
- запускати необхідні функції програми.

Метод `didExitRegion` викликається, коли пристрій залишає межі регіону (рис.3.8). Він дозволяє виконати дії, пов'язані з виходом з діапазону маяка:

- відправляти повідомлення;
- завершувати певні функції або записувати дії.

Основні моменти методів:

- у налаштуваннях програми необхідно дозволити відправлення сповіщень та використання геолокації у фоновому режимі;
- обидва методи дають можливість динамічно реагувати на зміну положення пристрою відносно регіону маяків;
- реалізація залежить від конкретних вимог програми, але найчастіше вона включає відправку сповіщень, запуск функцій або відображення додаткової інформації.

```
func locationManager(_ manager: CLLocationManager, didEnterRegion region: CLRegion) {
    print("DID ENTER REGION")
}
```

Рисунок 3.7 – Метод делегування didEnterRegion

```
func locationManager(_ manager: CLLocationManager, didExitRegion region: CLRegion) {
    print("DID EXIT REGION")
}
```

Рисунок 3.8- Метод делегування didExitRegion

Після виявлення регіону, де працюють датчики, мобільний пристрій отримує сповіщення про те, що користувач увійшов у зону дії цих датчиків. Зміст цього сповіщення (контент) зазвичай налаштовується на сервері. Для демонстрації був використаний приклад з CMS Leantegra.(рис3.9).

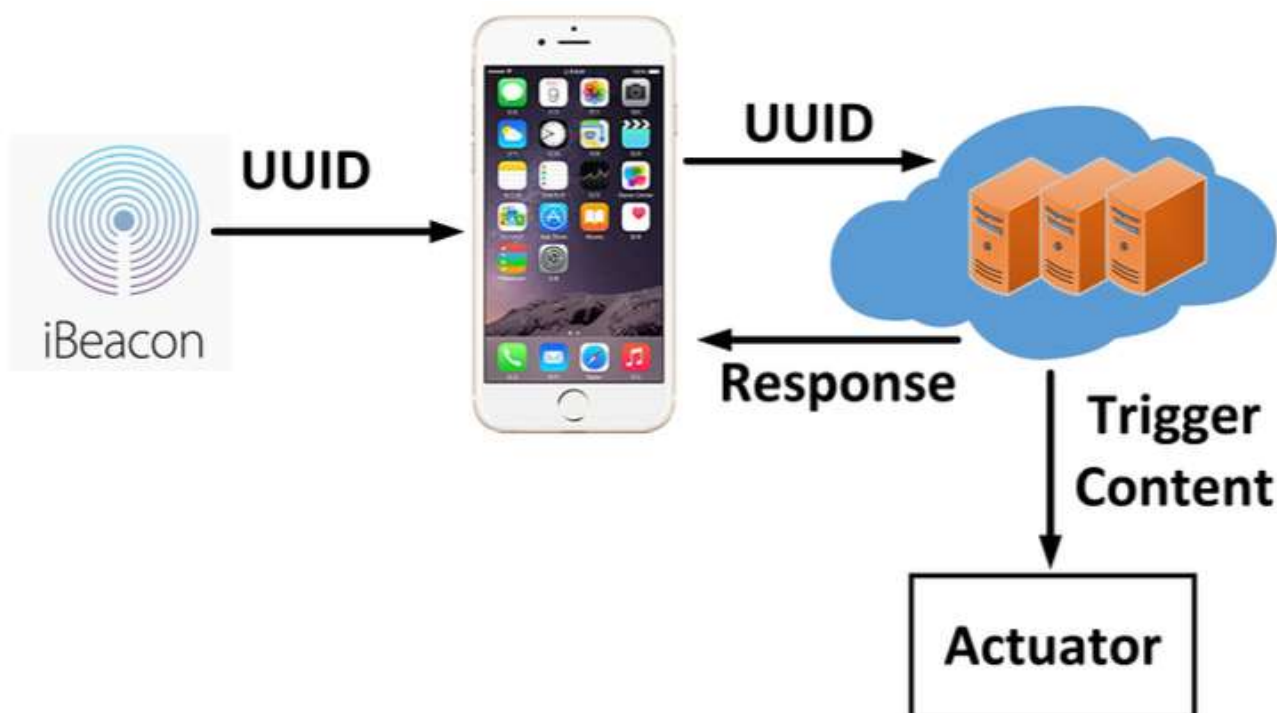


Рисунок 3.9 - Сповіщення на мобільному додатку

Після натискання на сповіщення відкривається інформація про подію, яка може включати текст, зображення, відео та інші матеріали (рис.3.10).

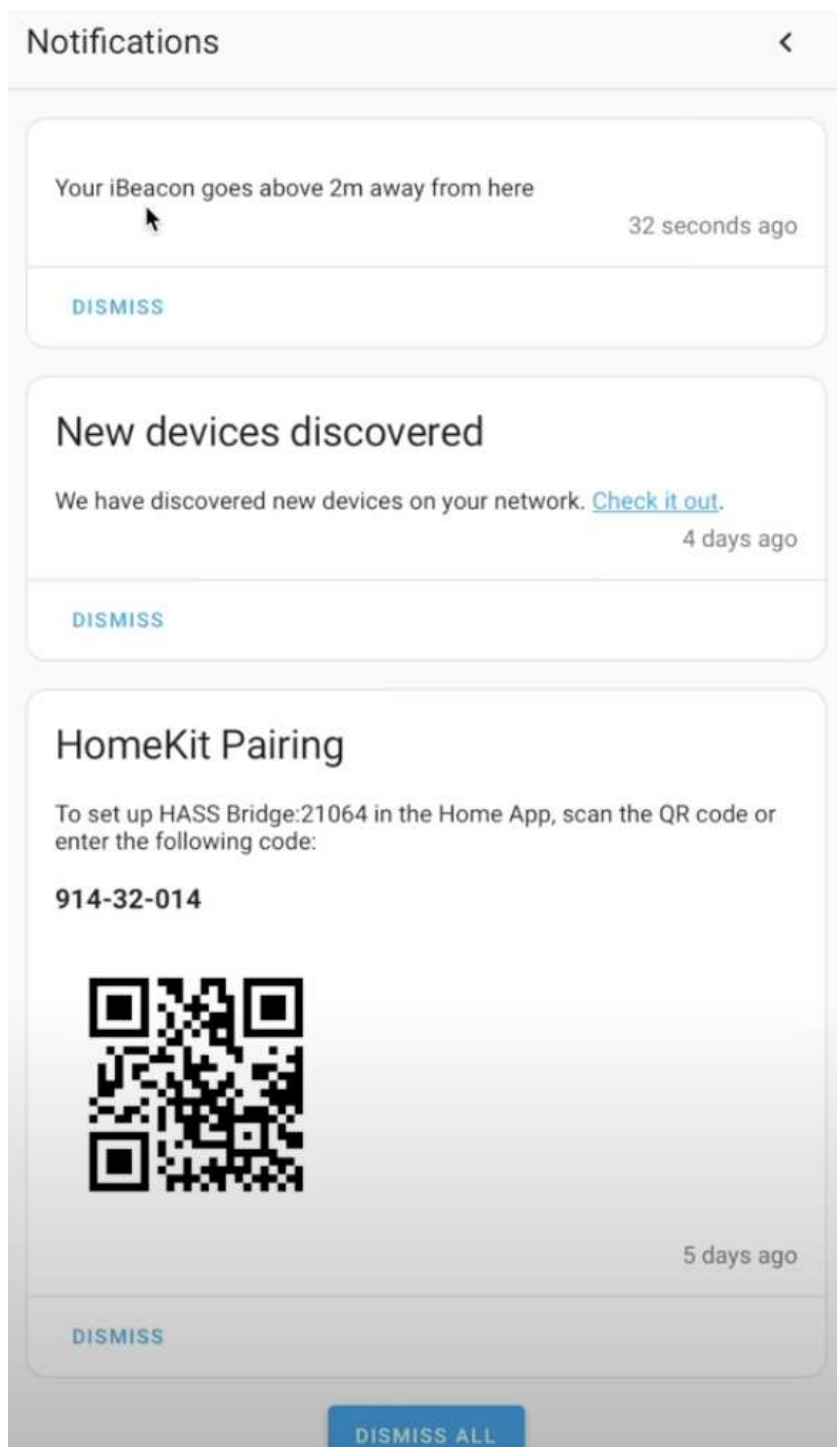


Рисунок 3.10 - Інформація про подію

Коли моніторинг регіону дає змогу виявити рух у межах діапазону маяків, визначення відстані (ranging) стає більш інформативним (рис. 3.11).

Це дозволяє отримати список маяків, що знаходяться в межах досяжності, разом з їхньою приблизною близькістю (proximity) до кожного з них (для цього викликається метод делегата `didRangeBeacons`) (рис. 3.12).

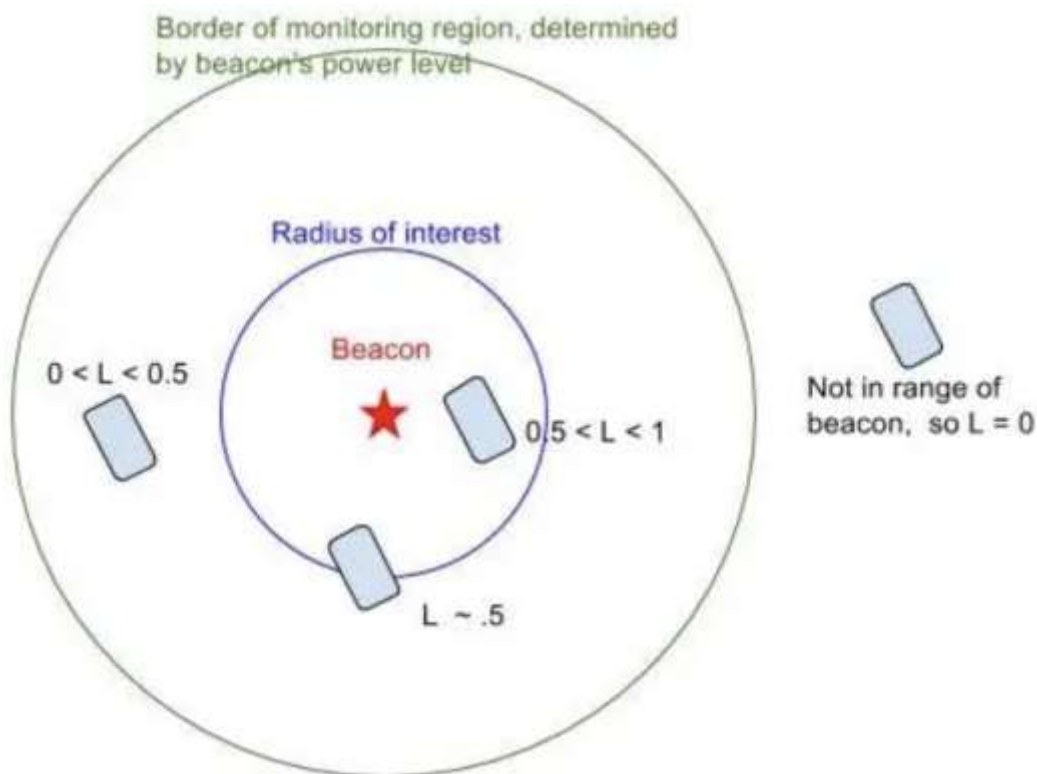


Рисунок 3.11 - Визначення відстані

```
func locationManager(_ manager: CLLocationManager, didRangeBeacons
beacons: [CLBeacon],
inRegion region: CLBeaconRegion) {
    beacons.forEach { (beacon) in
        switch beacon.proximity {
        case .unknown:
            print("Unknown")
        case .far:
            print("Far")
        case .near:
            print("Near")
        case .immediate:
            print("Immediate")
        }
    }
}
```

Рисунок 3.12 - Рух у межах діапазону маяків

Цей метод виконується кожну секунду в режимі реального часу, поки мобільний додаток знаходиться в пам'яті операційної системи [25].

Кожен об'єкт CLBeacon містить таку інформацію про розташування маяка:

- близькість (CLProximity) - визначає, наскільки близько знаходиться маяк;
- точність (CLLocationAccuracy) - вимірює відстань до маяка в метрах;
- RSSI (Int) - реєструє рівень сигналу маяка, виміряний у децибелах.

3.3 Висновки до розділу

У цьому розділі було розглянуто можливість управління подіями в контексті Інтернету речей за допомогою технології iBeacon. Окремо були описані основні інструменти для впровадження ключових функцій цієї технології, таких як моніторинг регіону та визначення відстані, на мобільних пристроях під управлінням операційної системи iOS.

Датчики iBeacon можуть бути використані в різних сферах, зокрема в маркетингу (наприклад, для надсилання сповіщень про знижки в конкретному відділі), на початкових етапах безготівкових платежів, а також на масових заходах, таких як спортивні та культурні події. Крім того, ця технологія може бути корисною для людей з порушеннями зору, оскільки вона дозволяє орієнтуватися в просторі та надає детальну інформацію про навколишнє середовище.

ВИСНОВКИ

У даній роботі було розглянуто основні концепції Інтернету речей, його історію, ключові поняття, характеристики, технології, проблеми та сучасний стан. Основна ідея Інтернету речей полягає у можливості підключення різноманітних об'єктів до мережі, обробки інформації, що надходить від навколишнього середовища, обміну даними та прийняття рішень і виконання дій на основі цієї інформації.

Особлива увага була приділена дослідженню розгортання Інтернету речей в контексті розумних міст, зокрема на основі порівняльного аналізу розумних міст по всьому світу. Для цього використовувався метод оцінки, в якому Інтернет речей розглядався як частина державної політики та програм, що дозволяє застосовувати традиційні інструменти оцінки. Цей підхід дав змогу оцінити розгортання Інтернету речей за всіма параметрами, а не лише за їхніми технологічними характеристиками.

Виявлено, що Інтернет речей і концепція розумних міст ще далекі від досягнення своїх обіцяних цілей, зокрема щодо задоволення потреб кінцевих користувачів. З цією метою була запропонована модель вартості даних Інтернету речей, яка орієнтується на брокера даних, що координує потік інформації між виробниками та користувачами. Запровадження більшої прозорості у цей процес дозволить забезпечити сталий та економічно обґрунтований розвиток Інтернету речей та розумних міст.

Також були розглянуті основні об'єкти даних, методи їх управління, ієрархії управління, а також ключові технології впровадження Інтернету речей, такі як iBeacon та RFID, які сприяють відстеженню та збору даних, зменшенню часу очікування та витрат на управління подіями. Наведено приклади їхнього використання.

Основною метою концепції Інтернету речей є впровадження процесів і подій, які можуть відбуватися без участі людини завдяки аналізу взаємодії

"розумних пристроїв". Це охоплює зміни в побуті, виробництві, мобільних пристроях та індустріальних галузях. Важливими аспектами цієї концепції є полегшення повсякденного життя (наприклад, через "розумні будинки" та "розумне харчування"), підвищення якості та ефективності роботи (інтерактивні плакати, карти тепла і руху), зниження витрат (автоматизоване управління учасниками), енергоефективність ("інтелектуальне освітлення") тощо.

Також було розглянуто основні технології для управління подіями в режимі реального часу, такі як потокова обробка подій, комплексна обробка подій та обробка потоків подій. Ці технології дозволяють аналізувати, збирати та обробляти потоки подій і даних у реальному часі, знижувати ризики виникнення проблемних ситуацій та приймати обґрунтовані рішення.

Зокрема, була розглянута можливість управління подіями в контексті Інтернету речей за допомогою технології iBeacon, а також основні інструменти для впровадження ключових можливостей цієї технології (моніторинг регіонів та визначення відстані) на мобільних пристроях під управлінням операційної системи iOS. Датчики iBeacon можуть використовуватись для маркетингових цілей (наприклад, надсилання сповіщень про знижки), на етапі безготівкових платежів або на масових заходах. Крім того, вони можуть бути корисними для людей з порушеннями зору, оскільки надають детальну інформацію про навколишнє середовище.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Tripathy B., Anuradha J. Internet of Things (IoT): TeChnologies, AppliCations, Challenges and Solutions. Florida - CRC Press, 2017 - 334 p.
2. Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 1. Fundamentals and Technologies /V. S. Kharchenko (ed.) - Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019 - 605p.
3. Data Science for Internet of Things and Internet of Everything: Practicum /Skarga-Bandurova I.S. and Gorbenko A.V. (Eds.) – Ministry of Education and Science of Ukraine, Volodymyr Dahl East Ukrainian National University, National Aerospace University “Kharkiv Aviation Institute”, Ternopil National Economic University, 2019 – 169 p.
4. Технології Інтернет речей : навч. посібник підготовлено для студентів вищих навчальних закладів [Електронний ресурс] / Сторчак К.П. [та ін.]. – Київ: ДУТ, 2021. – 68 с. – Режим доступу: https://duikt.edu.ua/uploads/l_2147_60168233.pdf.
5. RFID-МОДУЛЬ RC522: Повний посібник з опису, підключення та перших кроків у розробці. [Електронний ресурс]. – Режим доступу: <https://idcard.com.ua/ua/blog/rfid-modul-rc522-polnoe-rukovodstvo-po-opisaniyu-podklyucheniyu-i-pervym-shagam-v-razrabotke/?srsltid=afmbooqpelpzo69irwigav2cyfhdvhgsjvgbmts9h4zvcjm9yzqwza4c> (дата звернення 13.09.2024).
6. Rebecca Lee Hammons, Ronald J. Kovac. Fundamentals of Internet of Things for Non-Engineers. Taylor & Francis, 2019.- 430p.
7. Internet of Things for Industry and Human Application. Volume 3. Assessment and Implementation /V.S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 918 p.
8. Концепція «Індустрія 4.0»: проблеми впровадження і окремі правові аспекти її реалізації в Україні монографія /Є. М. Білоусов, І. В. Борисов та ін.; за ред. С.В. Глібка. Харків:, 2021. - 200 с.

9. Карталатов, К., & Чижевський, В. Розподілена генерація та SMART GRID. [Електронний ресурс]. – Режим доступу: <https://doi.org/10.36074/2663-4139.16.08> (дата звернення 10.10.2024).

10. Smart-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України : аналітична доповідь [Електронний ресурс] / Центр Разумкова. – Київ: Заповіт, 2021. – 400 с. – Режим доступу: <https://razumkov.org.ua/uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf>.

11. Internet of Things for Industry and Human Application. Fundamentals of Internet of Things /V.S. Kharchenko (ed.). – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 95 p

12. Огляд сучасних бездротових технологій передачі даних для «Internet of things» та аналіз проблем їх безпеки в контексті використання у системі «Розумний будинок» //Г.О. Щербаненко, О.В. Чебанюк. Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут, 2021 - с. 181-184.

13. Cheruvu S., Kumar A., Smith N., Wheeler D.M. Connectivity Technologies for IoT. In: Demystifying Internet of Things Security, 2020 - p.347–411.

14. ZigBee® Network Protocols and Applications. Taylor & Francis, 2019 - 378 p.

15. Internet of Things for Industry and Human Application. Volume 2. Modelling and Development /V.S. Kharchenko (ed.) - Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. - 547p.

16. Ranger S. What is the IoT? Everything you need to know about the Internet of Things right now [Електронний ресурс]. – Режим доступу : <https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/> (дата звернення 28.10.2024).

17. Xhafa L. Modeling and Processing for Next-Generation Big-Data Technologies / L.Xhafa, L. Barolli, A. Barolli, P. Papajorgji. – Springer, 2016. – 473–497 pp.

18. Steffen Schenkluhn. Device and event management as foundation of IoT

applications [Электронный ресурс] – Режим доступа: <https://blog.bosch-si.com/internetofthings/device-and-event-management-as-foundation-of-iot-applications/> (дата звернения 11.11.2024).

19. Integrating the IoT with Event Management [Электронный ресурс]. – Режим доступа: <https://www.gevme.com/blog/integrating-the-iot-with-event-management/> (дата звернения 23.11.2024).

20. Radio-frequency identification [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Radio-frequency_identification (дата звернения 29.10.2024).

21. iBeacon [Электронный ресурс]. – Режим доступа: <https://en.wikipedia.org/wiki/IBeacon> (дата звернения 23.11.2024).

22. Real Time IoT Analytics & Event Management [Электронный ресурс]. – Режим доступа: <http://www.plasmacomp.com/solutions/iot-m2m/realtime-analytics-event-manageme nt.aspx> (дата звернения 29.10.2024).

23. Event management for simultaneous actions in the Internet of Things [Электронный ресурс]. – Режим доступа: <https://ieeexplore.ieee.org/abstract/document/7845480/> (дата звернения 31.09.2024).

24. Real-Time Stream Processing for Internet of Things [Электронный ресурс]. – Режим доступа: <https://www.digitaldoughnut.com/articles/2017/april/real-time-stream-processing-for-internet-of-things> (дата звернения 19.11.2024).

25. Complex event processing for the Internet of Things and its applications [Электронный ресурс]. – Режим доступа: <https://ieeexplore.ieee.org/abstract/document/6899470/> (дата звернения 23.11.2024).