Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Кібербезпеки*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Аналіз застосування технологій IoT у бездротових інфокомунікаційних системах
(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІ-22-1*
Микола БОБІК
(власне ім'я, прізвище)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)

Тип програми *освітньо-професійна*

Освітня програма
«Інформаційно-мережна інженерія»
(повна назва освітньої програми)

Керівник доцент *Юрій КОЛТУН*
(посада, власне ім'я, прізвище)

Допускається до захисту

В.о. зав. кафедри _____ *Дарія ЧЕБОТАРЬОВА*
(підпис) (власне ім'я, прізвище)

2026 р.

Не містить відомостей заборонених до відкритого публікування.

Здобувач / *Микола БОБІК* /

Керівник / *Юрій КОЛТУН* /

Харківський національний університет радіоелектроніки

Факультет *Кібербезпеки*
Кафедра *Інформаційно-мережної інженерії*
(повна назва)
Рівень вищої освіти *перший (бакалаврський)*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«*02*» *червня* 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Бобіку Миколі Сергійовичу*
(прізвище, ім'я, по батькові)
1. Тема роботи *Аналіз застосування технологій IoT у бездротових інфокомунікаційних системах*
затверджена наказом університету від «*02*» *червня* 2026 р. № 466 *Ст*
2. Термін подання студентом роботи до екзаменаційної комісії *14 липня 2026 р.*
3. Вихідні дані до роботи *Тип телекомунікаційних структур: бездротові інфокомунікаційні системи. Технології IoT, що потрібно проаналізувати:RFID, LoRaWAN та M2M.*
Проаналізувати особливості організації та функціонування концепції IoT, та її архітектурні моделі, а також технологічні принципи організації та архітектурні моделі технологій RFID, LoRaWAN та M2M.

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Загальні технологічні особливості та архітектурні рішення концепції інтернету речей.
2. Технологія радіочастотної ідентифікації (RFID)
3. Технологічні принципи організації широкозонних мереж великого радіуса дії з низьким енергоспоживанням (LoRaWAN).
4. Технологія між машинної взаємодії (M2M).
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) *Слайди у форматі Power Point (назва, мета і актуальність роботи, загальна концепція організації інтернету речей та його робота, базові архітектурні моделі інтернету речей, технології IoT систем, технологія радіочастотної ідентифікації (RFID), широкозонна мережа великого радіуса дії з низьким енергоспоживанням (LoRaWAN), технологія між машинної взаємодії (M2M), порівняння технологій RFID, LoRaWAN та M2M, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	02.06.26	*виконано*
2	*Підбір літератури за темою роботи.*	03.06 – 07.06.26	*виконано*
3	*Виконання розділу 1*	08.06 – 12.06.26	*виконано*
4	*Виконання розділу 2*	13.06 – 19.06.26	*виконано*
5	*Виконання розділу 3*	20.06 – 29.06.26	*виконано*
6	*Виконання розділу 4*	30.06 – 07.07.26	*виконано*
7	*Оформлення пояснювальної записки*	08.07 – 12.07.26	*виконано*
8	*Оформлення презентаційного матеріалу,*		
	підготовка до захисту у ЕК, захист.	13.07 – 18.07.26	*виконано*

Дата видачі завдання *02 червня 2026 р.*

Здобувач _____
(підпис)

Керівник роботи _____ *(доц. Юрій КОЛТУН)*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 73 с., 17 рис., – табл., 23 джерела, 1 додаток.

ІНТЕРНЕТ РЕЧЕЙ, IOT, КОГНІТИВНИЙ IOT, CIOT, АРХІТЕКТУРНА МОДЕЛЬ, РАДІОЧАСТОТНА ІДЕНТИФІКАЦІЯ, RFID, РІДЕР RFID, RFID-МІТКА, LORAWAN, LPWAN, МІЖ МАШИННА ВЗАЄМОДІЯ, M2M

Об'єкти дослідження – система IoT, технології: RFID, LoRaWAN, M2M.

Мета роботи – загальний аналіз застосування технологій IoT у бездротових інфокомунікаційних системах, зокрема тих, що організовані на основі технологій LoRaWAN, RFID та M2M, а також аналіз архітектурних моделей цих технологій.

Зроблено загальний аналіз концепції інтернету речей, а також технологічних особливостей організації і функціонування найбільш поширених технологій, що підтримуються цією концепцією, зокрема RFID, LoRaWAN та M2M, які визначають способи організації взаємодії в IoT між пристроями, датчиками, інформаційними сервісами, тощо. Розглянуто архітектурні моделі, як безпосередньо концепції IoT, так і зазначених технологій, проаналізовані принципи організації взаємодії між пристроями, датчиками, мережевою інфраструктурою та прикладними сервісами.

THE ABSTRACT

Explanatory note 73 pages, 17 fig., – tab., 23 sources, 1 app.

INTERNET OF THINGS, IoT, COGNITIVE IoT, CIoT, ARCHITECTURAL MODEL, RADIO FREQUENCY IDENTIFICATION, RFID, RFID READER, RFID TAG, LoRaWAN, LPWAN, MACHINE-TO-MACHINE COMMUNICATION, M2M

Objects of research – IoT system, technologies: RFID, LoRaWAN, M2M.

The purpose of work – a general analysis of the application of IoT technologies in wireless information and communication systems, particularly those based on LoRaWAN, RFID, and M2M technologies, as well as an analysis of the architectural models of these technologies.

A general analysis of the Internet of Things concept has been conducted, along with an examination of the technological characteristics of the organization and operation of the most widely used technologies supported by this concept – in particular, RFID, LoRaWAN, and M2M, –which define the ways in which interactions within the IoT are organized among devices, sensors, information services, and so on. Architectural models of both the IoT concept itself and the aforementioned technologies are examined, and the principles governing interactions between devices, sensors, network infrastructure, and application services are analyzed.

ЗМІСТ

С.

Перелік скорочень 8

Вступ 9

1 Загальні технологічні особливості та архітектурні рішення концепції інтернету речей 12

1.1 Основні поняття, особливості побудови та функціонування IoT 12

1.2 Базові архітектурні моделі інтернету речей 17

1.2.1 Базова трирівнева архітектурна модель IoT-системи 18

1.2.2 Базова чотирирівнева архітектурна модель IoT-системи 19

1.2.3 Базова п’ятирівнева архітектурна модель IoT-системи 22

1.3 Технологічні особливості і архітектурна модель когнітивного IoT 24

1.4 Технології що застосовуються у разі організації IoT-систем 29

2 Технологія радіочастотної ідентифікації (RFID) 32

2.1 Загальні особливості технології RFID 32

2.2 Компоненти і принцип дії системи RFID 33

2.3 Технологія RFID ближньої зони 36

2.4 Технологія RFID дальньої зони 38

3 Технологічні принципи організації широкозонних мереж великого радіуса дії з низьким енергоспоживанням (LoRaWAN) 42

3.1 Загальні особливості технології LoRaWAN та принципи її функціонування 42

3.2 Архітектура системи IoT із застосуванням технології LoRaWAN 43

3.3 Переваги і недоліки технології LoRaWAN та її практичне застосування 47

4 Технологія між машинної взаємодії (M2M) 50

4.1 Загальні особливості технології M2M, її взаємозв’язок з IoT та принцип роботи 50

4.2 Архітектура M2M 53

Висновки 59

Перелік джерел посилання 63

Додаток А Слайди презентації 66

ПЕРЕЛІК СКОРОЧЕНЬ

CIoT (Cognitive Internet of Things) – когнітивний інтернет речей;

CR (Cognitive Radio) – когнітивне радіо;

CRN (Cognitive Radio Network) – когнітивна радіомережа;

GSM (Global System for Mobile Communications) – глобальна система мобільного зв'язку;

HTTP (Hyper Text Transfer Protocol) – протокол передачі гіпертексту;

IoT (Internet of Things) – Інтернет речей;

LoRaWAN (Long Range Wide Area Network) – широкозонна мережа великого радіуса дії;

LPWAN (Low Power Wide Area Network) – мережа з низьким енергоспоживанням;

LTE (Long Term Evolution) – технології довготривалого розвитку;

M2M (Machine-to-Machine) – між машинна взаємодія;

QoS (Quality of Service) – якість обслуговування;

RFID (Radio Frequency Identification) – радіочастотна ідентифікація;

SDR (Software-Defined Radio) – програмно-конфігуроване радіо;

SF (Spreading Factor) – коефіцієнт розширення спектра.

БД – база даних;

БС – базова станція;

ДА – домен автономності;

ІКТ – інформаційно-комунікаційна технологія;

КА – когнітивний агент;

КВ – когнітивний вузол;

КЕ – когнітивний елемент;

ПВ – простий вузол;

ПД – передача даних;

ПЗ – програмне забезпечення;

РЕЗ – радіоелектронні засоби;

СУ – система управління;

ЦОД – центр обробки даних.

ВСТУП

Стрімке поширення концепції Інтернету речей (Internet of Things, IoT) у сучасному інформаційному суспільстві супроводжується постійним зростанням кількості підключених пристроїв, підвищенням обсягів даних, що передаються та розвитком інтелектуальних систем, які взаємодіють між собою через інфокомунікаційні мережі завдяки процесам інтеграції і конвергенції їх технологій, послуг і апаратно-програмного забезпечення [1]. Ці процеси характеризується активним впровадженням автоматизованих засобів контролю, збору даних, обробки та передачі інформації, – що у підсумку забезпечують підвищення ефективності функціонування і взаємодії людей у різних сферах його діяльності. У зв’язку з цим концепція організації IoT набула значного практичного-соціального значення, як одна з ключових складових розвитку цифрової економіки та телекомунікаційних систем будь якої держави [2].

Технологічна ідея створення концепції IoT полягає в об’єднанні мережного обладнання, датчиків, контролерів та інших пристроїв у єдину мережну інфраструктуру з можливістю автоматичного обміну даними без безпосередньої участі людини [3]. Такі пристрої здатні збирати інформацію про параметри навколишнього середовища, виконувати її аналіз та передавати результати до центрів обробки даних (ЦОД) або інших вузлів мережі. Базовою фізичною і технологічною основою функціонування платформи IoT є використання сучасних інфокомунікаційних технологій, бездротових мереж, хмарних платформ та засобів машинної взаємодії.

На сьогодні технології IoT активно впроваджуються у різних сферах життєдіяльності суспільства. Значного поширення вони набули у системах «розумного дому», «розумного міста», промисловій автоматизації, транспортній інфраструктурі, енергетиці, медицині, логістиці, сільському господарстві, системах моніторингу навколишнього середовища та побутових інформаційних сервісах [4]. Застосування технологій IoT дозволяє забезпечити дистанційний контроль технічних процесів, оптимізувати використання ресурсів, підвищувати рівень безпеки, оперативно приймати рішення на основі актуальних даних, тощо.

Особливого значення набуває використання IoT в інфокомунікаційних системах і мережах, оскільки саме ця інфраструктура застосовується для передачі даних (ПД) між великою кількістю вузлів, пристроїв та сервісів. Тут

впровадження платформ IoT безпосередньо пов’язане із підвищенням ефективності використання пропускної здатності мереж, підвищенням енергоефективності, надійності зв’язку, масштабованості та якості обслуговування (Quality of Service, QoS). На практиці для застосування платформ IoT в інфокомунікаційних системах використовуються різноманітні технології, серед яких найбільш цікавими з точки зору теми моєї кваліфікаційної роботи є LoRaWAN, RFID та технології між машинної взаємодії (Machine-to-Machine, M2M).

Зокрема технологія LoRaWAN є одним із перспективних рішень для побудови мереж великого радіусу дії з низьким енергоспоживанням [5]. Її використання забезпечує передачу невеликих обсягів даних на значні відстані, що є важливим для систем моніторингу та неперервного контролю спеціалізованих мереж, екологічних параметрів та інфраструктурних об’єктів. Технологія RFID застосовується для автоматичної ідентифікації об’єктів у різних за своїм призначенням системах: від логістичних або складських до виробничих, шляхом радіочастотної взаємодії між RFID-мітками та зчитувачами, що дозволяє здійснювати безконтактний обмін даними та оперативний контроль об'єктів у реальному часі [6]. Бездротові сенсорні мережі використовуються для організації розподілених систем збору даних, що дозволяє здійснювати контроль параметрів середовища у режимі реального часу. Технології M2M забезпечують автоматизовану взаємодію між технічними пристроями без участі людини, що є важливою складовою сучасних автоматизованих систем управління (СУ).

Також треба зауважити, що важливим напрямом розвитку концепції IoT є інтеграція її технологій із мережами мобільного зв’язку на основі технологій довготривалого розвитку (Long Term Evolution, LTE). Використання мереж LTE для IoT забезпечує можливість побудови масштабованих мереж із широкою зоною покриття, підтримкою мобільності та достатнім рівнем надійності передачі даних. Разом із тим застосування мереж LTE для розширення і ефективного функціонування концепції IoT у потребує аналізу та оцінки параметрів базової мережі, зокрема бюджету втрат сигналу, зон покриття бездротових мереж, параметрів висхідної та низхідної лінії зв’язку. Дослідження зазначених характеристик дозволяє визначити можливості мережі щодо підтримки великої кількості IoT-пристроїв та забезпечення необхідної якості передачі інформації [7].

Таким чином можна бачити, що зростання кількості IoT-пристроїв, розширення сфер їх використання та підвищення вимог до сучасної

телекомунікаційної інфраструктури потребують аналізу ефективних технологічних і архітектурних рішень для організації бездротового зв’язку та визначення особливостей і підходів практичного впровадження IoT у сучасних інфокомунікаційних системах. Звідси метою цієї кваліфікаційної роботи є загальний аналіз застосування технологій IoT у бездротових інфокомунікаційних системах, зокрема тих, що організовані на основі технологій LoRaWAN, RFID та M2M, а також аналіз архітектурних моделей цих технологій. Це дозволяє визначити особливості їх побудови, принципи функціонування, механізми взаємодії основних компонентів та оцінити можливості їх практичного застосування під час створення сучасних бездротових інфокомунікаційних систем IoT. Актуальність проведення такого аналізу обумовлена необхідністю дослідження сучасних технологій Інтернету речей та особливостей їх застосування у бездротових інфокомунікаційних системах.

1 ЗАГАЛЬНІ ТЕХНОЛОГІЧНІ ОСОБЛИВОСТІ ТА АРХІТЕКТУРНІ РІШЕННЯ КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Основні поняття, особливості побудови та функціонування IoT

Як у вступі вже було зазначено, «Інтернет речей» (IoT) – це концепція організації мережної системи, яка об’єднує безліч фізичних об’єктів (так званих «речей») із вбудованими датчиками, ПЗ і модулями зв’язку. Ці об’єкти можуть здійснювати збір даних, обмінюватися ними між собою та взаємодіяти через Інтернет без участі людини. По суті концепція IoT перетворює ці об’єкти із звичайних пристроїв на інтелектуальні, використовуючи для цього технології, що в них закладені, такі як повсюдні та широко розповсюджені обчислення, вбудовані пристрої, комунікаційні технології, сенсорні мережі, інтернет-протоколи та додатки. Зокрема «розумні» об’єкти разом із їх можливими задачами являють собою додатки, що є специфічними для певної предметної області або сфери діяльності (вертикальні ринки (Vertical Market)), тоді як повсюдні обчислювальні та аналітичні послуги утворюють сервіси, що будуть незалежними від конкретної сфери діяльності (горизонтальні ринки (Horizontal Markets)) [3, 8]. На рисунку 1.1 показано загальну концепцію IoT, у якій прикладні додатки різних предметних областей або сфер діяльності взаємодіють із сервісами загального призначення, що є незалежними від конкретної сфери застосування. У той же час в межах кожної предметної області або сфери датчики та виконавчі пристрої здійснюють безпосередню взаємодію та обмін даними між собою [3].

На цей час використання IoT постійно зростає і отримує широке застосування як дома, так і в бізнесі, що у свою чергу сприяє підвищенню якості життя людей у всьому світі, а також розвитку світової економіки. Зокрема, в якості прикладів щодо Інтернету речей можна вказати, як на невеличкі розумні годинники, що контролюють, наприклад, фізичні характеристики здоров’я користувача чи/або його комунікації з іншими людьми, так і великі системи типу розумних будинків, у яких, зокрема, можна здійснювати контроль та автоматичне регулювання рівня освітлення, опалення чи вологості або здійснювати управління системами клімат-контролю, телевізорами та іншою домашньою технікою. Також наочним прикладом є так звана система реалізації розумного підприємства (Smart Factory), у якій здійснюється контроль промислового обладнання та реалізуються механізми виявлення проблемних місць з подальшим переналаштуванням роботи [8].



Рисунок 1.1 – Загальна концепція організації Інтернету речей

Для того, щоб підтримувати таке постійне розширення впровадження Інтернету речей у всі сфери життя і діяльності світового суспільства, потрібно щоб нові технології, інновації, додатки та послуги також розвивалися пропорційно до вимог ринку та потреб користувачів. Крім того, необхідно постійно розроблювати нові пристрої та удосконалювати існуючі, щоб вони відповідали вимогам користувачів не тільки за своїм функціоналом, алей й щодо їх доступності в будь-якому місці та в будь-який час. Також потрібні нові протоколи для забезпечення сумісності між різними пристроями, що працюють з різними «речами» [3].

Історія розвитку концепції IoT пов’язана з еволюцією комп’ютерних мереж, засобів автоматичної ідентифікації об’єктів та бездротових технологій передачі даних. Ідея створення середовища, у якому фізичні об’єкти можуть автоматично

обмінюватися інформацією через мережу, формувалася поступово протягом останніх трьох десятиліть і сьогодні є одним із ключових напрямів розвитку цифрових технологій та інфокомунікаційних систем.

Однією з перших, але на той час неформальних подій у подальшому становленні IoT, вважається 1982 рік, коли в університеті Карнеги-Меллон (Carnegie Mellon University) в Пітсбурзі (США) групою аспірантів факультету комп'ютерних наук було встановлено on-line контроль за автоматом Coca-Cola через університетський комп'ютер PDP-10. В автоматі були розташовані датчики, які дозволяли дистанційно отримувати інформацію про наявність в ньому напоїв та їх температуру, що оптимізувало час у випадку потреби йти за банкою Coca-Cola. Хоча на той час термін «Інтернет речей» ще не існував, але саме цей проєкт продемонстрував можливість взаємодії фізичних об'єктів із комп'ютерними мережами [8, 9].

Безпосередньо термін «Інтернет речей» був запропонований у 1999 році Кевіном Ештоном (Kevin Ashton) виконавчим директором центру Auto-ID Labs (незалежна мережа лабораторій та дослідницька група у сфері мережної радіочастотної ідентифікації та нових сенсорних технологій) при Массачусетському технологічному інституті. Працюючи над проєктами із застосуванням технологій радіочастотної ідентифікації (Radio Frequency Identification, RFID), він та його колеги запропонували систему, у якій фізичні об'єкти можуть автоматично ідентифікуватися та обмінюватися інформацією без участі людини. Зокрема Ештон запропонував використовувати RFID-мітки замість штрих-кодів для відстеженн я товарів у ланцюгу поставок, що згодом і призвело до створення стандарту RFID. RFID-мітка – це ідентифікаційна мітка, яка дозволяє ідентифікувати об'єкти за допомогою радіосигналів. На неї можна нанести певну інформацію, яку згодом можна зчитати за допомогою пристрою. Саме з цього моменту концепція IoT почала формуватися як окремий науково-технічний напрям [4, 8, 9].

Вже у 2005 році під егідою Міжнародної організації по стандартизації ITU (International Telecommunication Union) було опубліковано доповідь «ITU Internet Reports 2005: The Internet of Things», в якій було сформульовано бачення глобальної мережі взаємопов'язаних пристроїв, що здатні збирати, передавати та обробляти дані. У доповіді описувалися такі фундаментальні елементи IoT, як RFID, сенсорні мережі, нанотехнології та мініатюризація пристроїв. Зверталася увага на нові можливості для розвитку бізнесу, «розумних міст», медицини та

цифровізації суспільства, що особливо стало актуальним для країн, які розвиваються [10]. Ця публікація стала поштовхом до активізації наукових досліджень і стандартизації технологій IoT на міжнародному рівні.

Подальший розвиток концепції IoT пов’язаний із 2011 - 2012 роками, коли кількість підключених до мережі пристроїв вперше перевищила чисельність населення Землі. У цей період відбулося стрімке поширення хмарних обчислень, мобільного Інтернету, бездротових сенсорних мереж та технологій міжмашинної взаємодії M2M. Це створило технічні передумови для масового впровадження рішень IoT у промисловості, транспорті, енергетиці та побутовій сфері.

Сучасний етап розвитку IoT розпочався приблизно з 2015 року і триває донині. Він характеризується впровадженням спеціалізованих технологій зв’язку для Інтернету речей, зокрема LoRaWAN, NB-IoT, LTE-M та мереж п’ятого покоління 5G. У цей період IoT став невід’ємною складовою концепцій «розумного міста», цифрового виробництва, Індустрії 4.0 та інтелектуальних транспортних систем. Сьогодні розвиток IoT спрямований на підвищення масштабованості мереж, енергоефективності пристроїв, рівня інформаційної безпеки та інтеграції з технологіями штучного інтелекту.

Таким чином, можна бачити, що концепція Інтернету речей передбачає, що мережі можуть бути підключені мільйони різних пристроїв. Але треба зауважити, що ці пристрої повинні вміти максимально правильно взаємодіяти один з одним. Крім того, необхідно гарантувати їх чітку взаємодію в мережі, тобто гетерогенні пристрої та протоколи, що орієнтовані на різні мережні стандарти і технології, мають працювати разом, конфіденційно і з визначеним рівнем безпеки. Зокрема протоколи маршрутизації мають забезпечувати безперервний обмін даними навіть у випадках зміни мережних параметрів або переміщення пристроїв (наприклад, зміна адресації чи пропускної здатності каналу зв’язку). Також процеси збору, передачі та обробки інформації мають виконуватися з мінімальними затримками, що дозволяє системі оперативно реагувати на зміни стану об’єктів і приймати відповідні рішення в режимі реального часу. Тобто для IoT важливим є вирішення задач щодо забезпечення оптимального адміністрування та технічного супроводу, зокрема у здійсненні моніторингу стану пристроїв, виявленні та усунення помилок, налаштуванні параметрів функціонування, а також контролю за продуктивністю мережі, у тому числі за допомогою спеціалізованих протоколів і засобів управління.

Узагальнено робота мережі IoT складається з декількох етапів (рис.1.2).

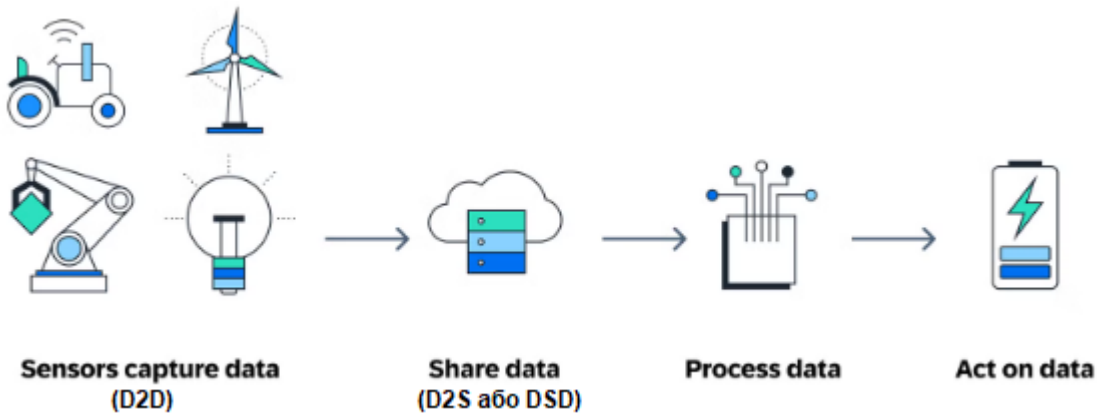


Рисунок 1.2 – Основні етапи в роботі IoT

На першому етапі термінальні пристрої, датчики та сенсори з'єднуються між собою по принципу D2D (Device-to-Device) та збирають дані зі своїх середовищ. На другому етапі, використовуючи доступні мережні з'єднання, пристрої IoT, надсилають ці дані на сервер для подальшого аналізу та обробки, реалізуючи взаємодію D2S (Device-to Server) або до загальнодоступної або приватної хмарної системи за принципом DSD (Device-System-Device) чи зберігають дані локально у відповідності із принципом обробки на периферії. Треба зазначити, що сервер може мати розподілену структуру, тобто мати кілька комп'ютерів або об'єктів, як взаємодіють один з одним за принципом S2S (Server-to-Server). Далі, на третьому етапі, ці дані оброблюються. На цьому етапі ПЗ налаштовується на виконання певних дій на основі цих даних, наприклад, увімкнення вентилятора або надсилання попередження, тощо. На останньому етапі, здійснюється аналіз накопичених даних від всіх пристроїв у мережі IoT та приймаються рішення для ухвалення тих або інших дій чи алгоритмів роботи [11, 12].

Треба зазначити, що на кожному із зазначених етапів можуть використовуватися різні протоколи та різні технології для зв’язку між вузлами мережі, а також різні мережні архітектури та різні технології для збору необроблених даних. А безпосередньо структура мережі IoT часто визначається проблемою зручності використання. Зокрема структури за топологічним типом «зірка» та деревоподібні структури можуть бути одно- або багаторівневими.

На цей час мережі IoT зазвичай будуються з використанням дротових або бездротових технологій зв’язку. Технології бездротового зв’язку включають технології, що використовуються операторами для стільникових мереж, або бездротових локальних мереж чи сенсорних мереж. Функціональні можливості,

які найчастіше реалізуються в сучасних мережах IoT, називаються комунікаціями M2M. Основна відмінність IoT від інших мереж полягає в тому, що люди не є безпосередніми користувачами мережі. Пристрої (об'єкти), підключені до IoT, не визначаються безпосередньо поведінкою людини, як це відбувається, наприклад, у традиційних мережах зв'язку, де управління терміналом здійснюється безпосередньо користувачем.

Таким чином, можна бачити, що функціонування Інтернету речей ґрунтується на кількох основних принципах. Першим із них є наявність розвиненої комунікаційної інфраструктури, яка забезпечує підключення пристроїв до мережі та їх взаємодію між собою незалежно від місця розташування. Другим принципом є унікальна ідентифікація кожного об’єкта, що дозволяє однозначно розпізнавати пристрої в мережі та здійснювати їх облік і контроль. Третім принципом є можливість обміну даними через мережу зв’язку або Інтернет, завдяки чому об’єкти можуть передавати інформацію, отримувати команди, взаємодіяти з іншими пристроями та брати участь в автоматизованих процесах обробки даних і прийняття рішень. Дотримання цих принципів дозволяє підтримувати стабільну та надійну роботу масштабних IoT-систем в умовах постійного зростання їх складності [3, 8, 9, 12].

1.2 Базові архітектурні моделі інтернету речей

Для Інтернету речей розроблено чимало базових архітектурних моделей із різним ступенем деталізації, які визначають структуру взаємодії різних інформаційно-комунікаційних технологій (ІКТ), засобів зв’язку та програмно-апаратних компонентів, що спільно забезпечують функціонування платформи IoT, а також пропонують рекомендації щодо проведення проектування, розгортання та забезпечення управління IoT-рішеннями. Іншими словами ці моделі у тому чи іншому поданні відображають принципи організації процесів збору, передачі, обробки та використання даних, що надходять від програмних модулів чи компонентів та підключених пристроїв і датчиків [13].

1.2.1 Базова трирівнева архітектурна модель IoT-системи

У 2005 році ITU-T запропонував 3-ьох рівневу базову архітектурну модель, згідно з якою Інтернет речей має забезпечувати взаємодію з реальними фізичними пристроями та об’єктами як на основі збору даних про їх стан, так і шляхом інтелектуальної обробки отриманої інформації (рис 1.3). У цій моделі пристрої та об’єкти взаємодіють між собою в межах певного сервісу або функціонального призначення [14].

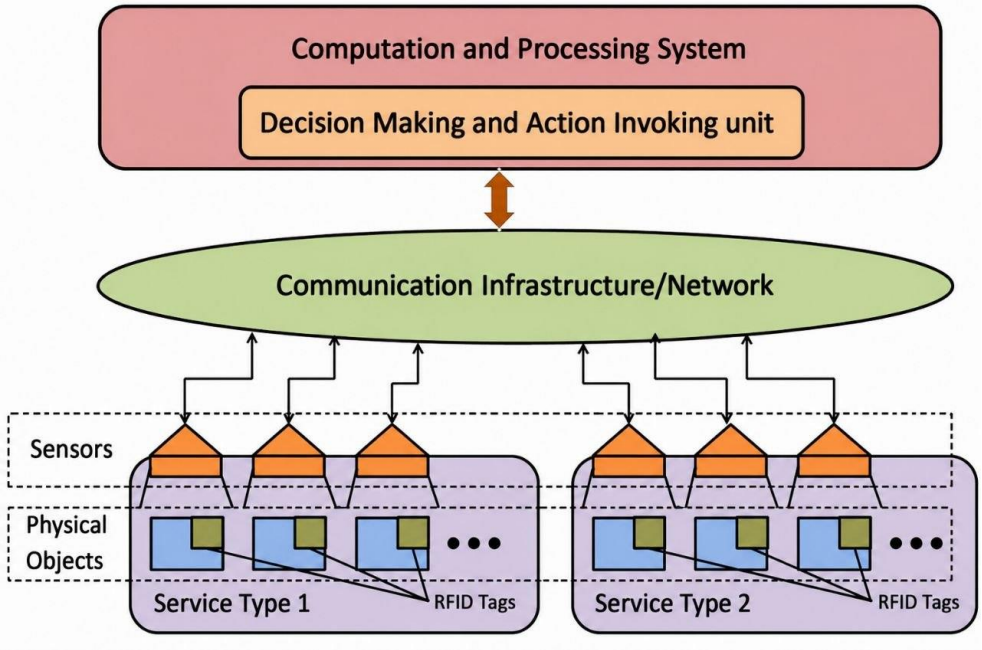


Рисунок 1.3 – Базова трирівнева архітектурна модель IoT-системи

Розглянемо особливості наведеної моделі.

1) Рівень фізичних об’єктів і датчиків (Physical Objects and Sensors Layer). Тут містяться фізичні об’єкти, датчики, RFID-мітки та інші пристрої збору інформації. Виявлення об’єктів, їх ідентифікація та передача інформації, що стосується конкретних об’єктів. Ця інформація складається з даних, що отримуються за допомогою датчиків, про температуру, орієнтацію, рух, вібрацію, швидкість, вологість, хімічний склад повітря, тощо, – залежно від типу тих або інших датчиків. На рис 1.3 показано, що в системі можуть одночасно функціонувати різні типи інтелектуальних сервісів (Service Type 1, Service Type 2), кожен з яких обслуговує певну групу об’єктів. Для надання цих інтелектуальних сервісів (smart services) можна застосовувати комбінацію різних датчиків [14].

Фізичні об’єкти і датчики можуть бути оснащеними RFID-мітками або іншими електронними ідентифікаторами, які можуть зчитуватися інтелектуальними пристроями, наприклад смартфонами або вбудованими RFID-зчитувачами. Кожний об’єкт має унікальний ідентифікатор, а інформація про нього зберігається в RFID-мітці [14].

Далі зібрана інформація передається до мережної інфраструктури для подальшої обробки.

2) Рівень комунікаційної або мережної інфраструктури (Communication Infrastructure/Network Layer) забезпечує надійну передачу даних між фізичними об’єктами та системою обробки інформації. Для фізичної реалізації цього рівня можуть застосовуватися різні технології зв’язку, зокрема Ethernet, Wi-Fi, Bluetooth, ZigBee, LoRaWAN, NB-IoT, LTE, 5G та інші. На цьому рівні можуть також реалізовуватися механізми забезпечення інформаційної безпеки, забезпечення контролю QoS та управління мережними ресурсами [14].

3) На верхньому рівні обробки інформації та прийняття рішень (Computation and Processing System Layer), до складу якого входить модуль прийняття рішень та формування керуючих впливів (Decision Making and Action Invoking Unit), здійснюється накопичення, зберігання, аналіз та інтелектуальна обробка даних, отриманих від пристроїв IoT. Обробка може виконуватися на локальних серверах, в корпоративних ЦОД або в ЦОД хмарних середовищ. На основі результатів аналізу система автоматично формує відповідні команди управління або рекомендації. Наприклад, у разі перевищення допустимого значення температури система може автоматично активувати систему охолодження, надіслати повідомлення оператору або змінити режим роботи обладнання. Тобто система підтримує механізм зворотного зв’язку для інформування оператора про свій поточний стан та результати дій, що виконуються [14].

1.2.2 Базова чотирирівнева архітектурна модель IoT-системи

З розвитком підходів та принципів IoT-систем у 2012 році було розроблено рекомендацію ITU-T Y.2060. У ній описано чотирирівневу архітектурну модель, яка забезпечує структурований підхід до використання об’єктів та реалізації взаємодій у системі Інтернету речей. Вона містить наступні рівні: пристроїв, мережний, підтримки сервісів і додатків, а також прикладний. Крім того, на всіх рівнях підтримуються функції управління та інформаційної безпеки (рис. 1.4) [13].

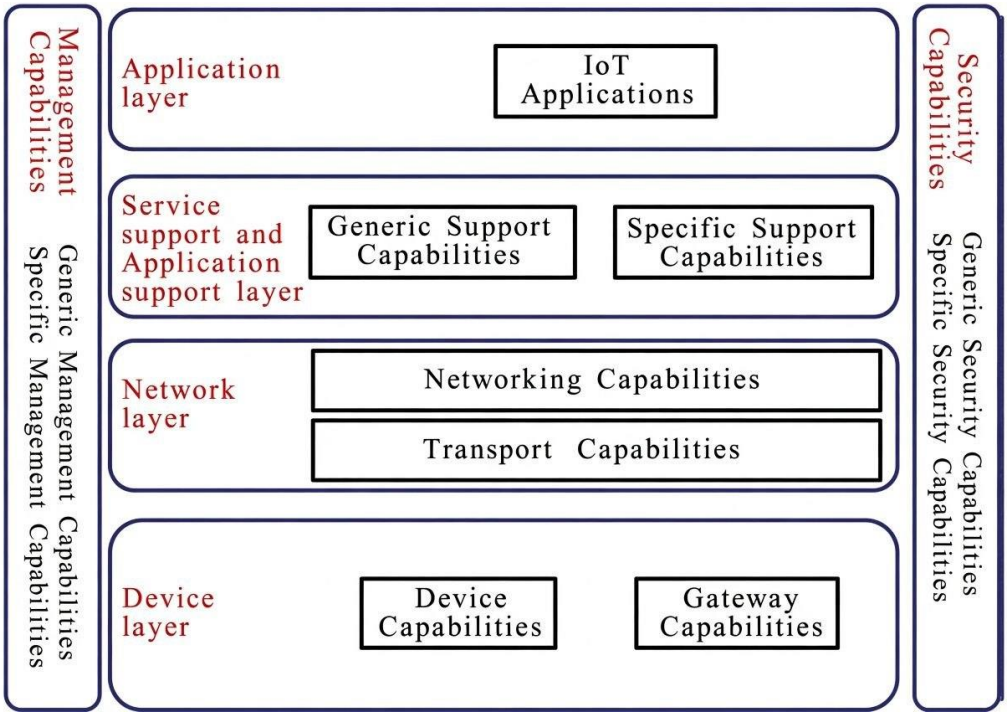


Рисунок 1.4 – Чотирирівнева архітектурна модель IoT, що рекомендована Рек. ITU-T Y.2060

Її нижнім рівнем є рівень пристроїв (Device Layer), до якого входять фізичні об’єкти, датчики, RFID-мітки, інтелектуальні пристрої, а також шлюзи доступу. Основне призначення цього рівня полягає у зборі даних про стан фізичних об’єктів та їх первинній обробці, а також автоматичному виконанні дій щодо інструкцій, що отримуються ззовні [13].

Цей рівень містить дві функціональні групи можливостей [13]:

- можливості пристроїв (Device Capabilities), що забезпечують вимірювання фізичних параметрів, ідентифікацію об’єктів, збір та попередню обробку даних;

- можливості шлюзів (Gateway Capabilities), що забезпечують агрегування даних, перетворення протоколів та взаємодію мережної інфраструктури об’єктів IoT із зовнішньою мережею ПД.

Треба зазначити, що шлюзи є важливим елементом системи IoT, оскільки дозволяють інтегрувати різнорідні сенсорні мережі та пристрої, що використовують різні технології зв’язку.

Задачі мережного рівня (Network Layer) наведеної архітектурної моделі є аналогічними рівню комунікаційної або мережної інфраструктури, що був розглянутий для архітектури на рис. 1.3. Тобто реалізуються механізми транспортування інформації між пристроями, шлюзами, сервісними платформами

та прикладними системами із забезпечення надійної передачі даних. На цьому рівні виділяють дві функціональні групи можливостей [13]:

- транспортні можливості (Transport Capabilities), які реалізують функції передачі інформації, маршрутизації, комутації та адресації;

- мережні можливості (Networking Capabilities), що забезпечують організацію мережної взаємодії між різними сегментами IoT-системи.

Для реалізації мережного рівня можуть також використовуватися як дротові, так і бездротові технології зв'язку.

На рівні підтримки сервісів і додатків (Service Support and Application Support Layer) забезпечується виконання функцій обробки даних та надання сервісів, що необхідні для функціонування IoT-систем. Цей рівень є сполучною ланкою між рівнем пристроїв та прикладним рівнем. Зокрема тут реалізується логіка роботи системи та здійснюється інтеграція різних прикладних сервісів. Функціональними можливостями цього рівня є [13]:

- загальні функціональні можливості (Generic Support Capabilities), які ґрунтуються на універсальних сервісах, які можуть використовуватися різними додатками незалежно від предметної області (див. Vertical Market на рис. 1.1). До них належать зберігання даних, управління пристроями і подіями, аналітична обробка інформації та підтримка сервісів взаємодії;

- спеціалізовані функціональні можливості (Specific Support Capabilities), що орієнтовані на реалізацію специфічних функцій для конкретної прикладної області, наприклад промислової автоматизації, енергетики або транспортних систем.

До рівня підтримки сервісів і додатків можуть входити периферійні обчислювальні ресурси, які забезпечують можливість обробки даних ближче до їх джерела, унаслідок чого мінімізується затримка та необхідна пропускна здатність. Також тут можуть використовуватися хмарні обчислення, платформи великих даних (Big Data) та системи штучного інтелекту [13].

Верхнім рівнем архітектурної моделі на рис. 1.4 є прикладний рівень (Application Layer). Він охоплює програмні додатки та сервіси, що використовують дані, які були отримані від IoT-пристроїв, для розв'язання практичних задач у різних сферах діяльності. До таких сфер належать енергетика, транспорт, промисловість, охорона здоров'я, освіта, торгівля та інші галузі. Прикладні рішення можуть бути вертикальними (рис. 1.1), тобто орієнтованими

на потреби конкретної галузі, або горизонтальними, що призначені для використання в різних сферах діяльності [3, 13].

Особливістю архітектурної моделі ITU-T Y.2060 є наявність наскрізних функцій управління (Management Capabilities), які охоплюють усі рівні системи. Ці функції забезпечують конфігурування пристроїв, моніторинг стану мережі, управління ресурсами, виявлення несправностей, контроль продуктивності та адміністрування сервісів. Ефективна реалізація механізмів управління є необхідною умовою функціонування масштабних IoT-систем, що можуть включати мільйони взаємопов’язаних пристроїв [13].

Оскільки системи Інтернету речей оперують значними обсягами даних і взаємодіють через відкриті мережі, важливу роль відіграють функції забезпечення інформаційної безпеки (Security Capabilities). Архітектурна модель Y.2060 передбачає реалізацію загальних і спеціалізованих механізмів захисту на всіх рівнях системи IoT, зокрема таких, як [13]:

- автентифікація користувачів і пристроїв;
- авторизація доступу до ресурсів;
- забезпечення конфіденційності даних;
- контроль цілісності інформації;
- захист від несанкціонованого доступу;
- виявлення та протидія мережним атакам.

1.2.3 Базова п’ятирівнева архітектурна модель IoT-системи

На сучасному етапі розвитку інфокомунікацій широке поширення у всіх сферах отримала мережа Інтернет, який використовує для зв’язку між мережними вузлами та надання користувачам безлічі різноманітних сервісів і додатків стек протоколів TCP/IP. Оскільки Інтернет речей з’єднує все і всіх для обміну інформацією між собою у тому числі через канали Інтернет, то трафік і обсяги зберігання даних у мережі також зростатимуть у геометричній прогресії. На цей час системи IoT об’єднують мільярди об’єктів, що вимагає вирішення також досить складних питань, що пов’язані з конфіденційністю та безпекою. Отже виникає потреба у новій архітектурній моделі, яка зможе збільшити деталізацію і абстрагування функціональних можливостей IoT-систем. Зокрема, така архітектурна модель IoT має враховувати багато факторів, таких як:

масштабованість, сумісність, надійність, QoS, тощо. Тобто, розвиток систем IoT тісно пов’язаний з розвитком Інтернет і залежить від технологічного прогресу та розробки різноманітних нових сервісів, додатків і бізнес-моделей. Відповідно з цим в рамках такої сучасної базової архітектурної моделі пропонується модель, в якій структура IoT складається з п’яти рівнів (рис. 1.5), які стисло розглядаються нижче [3, 14].

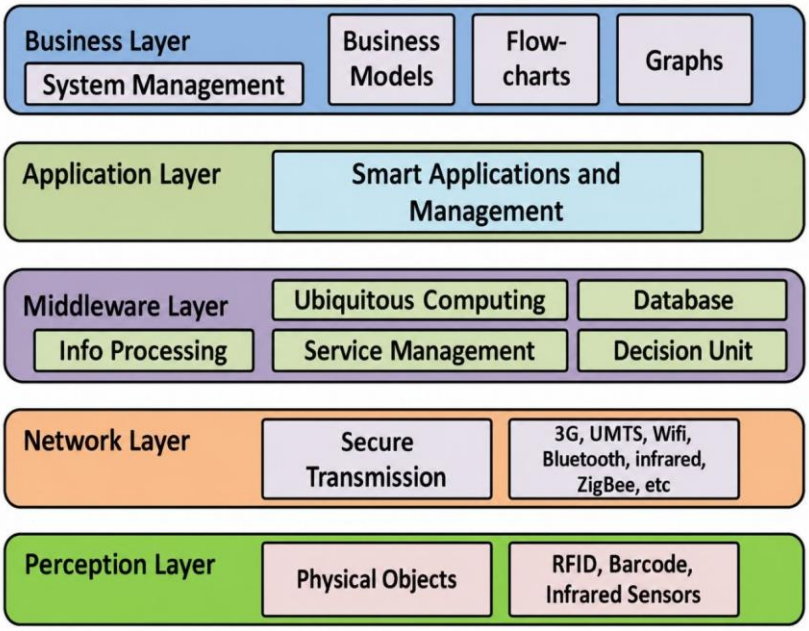


Рисунок 1.5 – П’ятирівнева архітектурна модель IoT

1) На рівні сприйняття (Perception Layer), що також відомий як «рівень пристроїв» (див. рис. 1.4), або «рівень фізичних об’єктів і датчиків» (див. рис. 1.3) містяться відповідно фізичні об’єкти та датчики, зокрема RFID, 2D-штрих-коди або інфрачервоні датчики, залежно від методу ідентифікації об’єктів. На цьому рівні в основному здійснюється ідентифікація та збір інформації про конкретні об’єкти за допомогою датчиків. Залежно від їх типу може збиратися інформація про місцезнаходження, температуру, рух, наявність вібрацій, швидкість руху, вологість, хімічні зміни у повітрі, тощо. Ця інформація потім передається вище на мережний рівень для подальшої безпечної передачі до систем обробки інформації [14].

2) На мережному рівні (Network Layer), який також можна назвати «рівнем передачі» або, по аналогією з моделлю на рис. 1.3, «Рівнем комунікаційної або мережної інфраструктури». Задачі і функції цього рівня є тотожними подібним рівням, що були розглянуті у попередніх моделях, тобто цей рівень забезпечує

безпечну передачу інформації від датчиків до системи обробки інформації. Таким чином, мережний рівень передає інформацію від рівня сприйняття до проміжного рівня [14].

3) На проміжному рівні (Middleware Layer) датчики та інші пристрої в IoT-системі реалізують різні типи послуг. Кожен пристрій з'єднується та взаємодіє лише з тими іншими пристроями, які реалізують той же самий тип послуги. Цей рівень відповідає за управління послугами та має зв'язок із базою даних (БД). Він отримує інформацію від мережного рівня та зберігає її в БД, а також на цьому рівні здійснюється обробка інформації та повсюдні обчислення (розподілені інтелектуальні обчислення), а також приймає автоматичні рішення на основі отриманих результатів [14].

4) Рівень додатків (Application Layer) забезпечує загальне управління додатком на основі інформації про об'єкти, що була оброблена на проміжному рівні. До додатків, які реалізовані за допомогою IoT, належать: інтелектуальна («розумна») охорона здоров'я, інтелектуальне («розумне») сільське господарство, «розумний» дім, «розумне» місто, інтелектуальні («розумні») транспортні системи, тощо [14].

5) Бізнес-рівень (Business Layer) рівень в цілому відповідає за управління системою IoT, включаючи додатки та сервіси. На цьому рівні створюються бізнес-моделі, формуються графіки, блок-схеми, тощо – на основі даних, що були отриманих від рівня додатків. Це необхідно тому, що успіх технологій інтернету речей залежить від наявності ефективних бізнес-моделей. На основі аналізу результатів функціонал цього рівня допоможе визначити подальші дії та бізнес-стратегії [14].

1.3 Технологічні особливості і архітектурна модель когнітивного IoT

Сама по собі ідея когнітивності стосовно властивостей радіоелектронних засобів (РЕЗ) була вперше сформульована ще у 1999 році, а згодом отримала розвиток у вигляді технології когнітивного радіо (Cognitive Radio, CR), сутність якої полягає в тому, що бездротові термінали користувачів, наприклад смартфони або планшети, а також мережі, що з ними пов'язані, можуть бути автономними та інтелектуально з гнучкою адаптацією (іншими словами «розумно») здійснювати вибір і використання доступних радіочастотних ресурсів та мережних

комунікацій. При цьому правила функціонування та взаємодії цих терміналів визначаються потребами їх користувачів щодо отримання певних послуг. Водночас РЕЗ мають ефективно та з потрібною завадостійкістю забезпечувати використання наявних радіоресурсів [15].

Пристрої CR за допомогою механізмів зондування радіочастотного середовища здатні виявляти тимчасово вільні ділянки радіочастотного спектра, які раніше були виділені для використання іншим РЕЗ. Виявивши такі вільні смуги частот або радіоканали, когнітивні пристрої CR можуть тимчасово їх використовувати для передачі та прийому інформації, не створюючи при цьому завад основним РЕЗ, що працюють у цьому спектрі. Зазначені вище властивості формують поняття когнітивних радіомереж (Cognitive Radio Network, CRN) і реалізуються насамперед завдяки застосуванню технологій програмного управління мережею та її компонентами [15].

Для отримання послуг в CRN користувач може застосовувати термінальне обладнання, що функціонує з використанням принципів програмно-конфігурованого радіо (Software-Defined Radio, SDR). Такі пристрої забезпечують гнучке програмне управління протоколами та параметрами інтерфейсів радіодоступу. Завдяки цьому термінали з підтримкою принципів SDR мають широкі можливості щодо вибору різних інфокомунікаційних мереж для отримання необхідних сервісів. Зокрема вони можуть працювати в бездротових мережах на основі стандартів GSM, GPRS, EDGE, UMTS, Wi-Fi, LTE, а також використовувати телевізійні частотні діапазони відповідно із стандартом IEEE 802.22-2011. Слід зазначити, що принципи програмно-конфігурованого радіо та властивості когнітивності поширюються не лише на термінали користувачів, але й на обладнання базових станцій (БС), і на цей час можуть також бути використані в пристроях IoT, забезпечуючи тим самим більш ефективне використання радіочастотного спектра, підвищення гнучкості мереж та адаптацію до умов функціонування, які постійно змінюються [15].

Вважається, що когнітивний інтернет речей (Cognitive Internet of Things, CIoT) – це подальший розвиток платформи IoT, в якій речі (фізичні або віртуальні об’єкти, пристрої, датчики) пов’язані між собою та взаємодіють із мінімальним втручанням людини. В останній час підключені до IoT пристрої можуть використовувати штучний інтелект та машинне навчання. Об’єкти такої мережі можуть у разі потреби сформувати певне уявлення про свій стан та стан навколишніх об’єктів, також можуть сприймати і аналізувати інформацію про

навколишнє середовище, робити на основі аналізу цієї інформації логічні висновки, навчатися та здійснювати адаптацію до специфіки зовнішніх і внутрішніх умов [15].

Розглянемо основні принципи побудови архітектурної моделі CIoT. Платформа CIoT передбачає наявність у системах інтернету речей механізмів кооперації та інтелектуальної («розумної») взаємодії між мережними компонентами. У зв'язку з цим до складу архітектурної моделі CIoT входять такі інтелектуальні («розумні») компоненти, як когнітивні вузли (КВ) та когнітивні елементи (КЕ), які можуть автономно змінювати власні технічні параметри відповідно до поточних умов функціонування мережі та навколишнього середовища. Відмінність між КВ та КЕ полягає в тому, що до КВ можуть додатково підключатися так звані прості (ПВ) або некогнітивні вузли (рис. 1.6). Таким чином, КВ виконує не лише власні функції, але й також забезпечує взаємодію та координацію роботи інших підключених пристроїв [15].

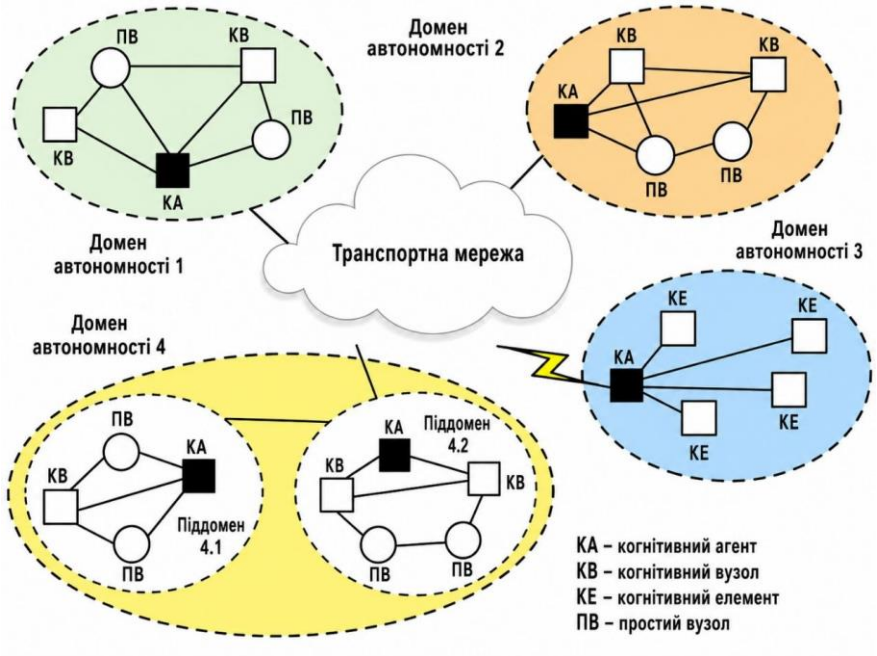


Рисунок 1.6 – Архітектурна модель організації платформи когнітивного IoT

Усі зазначені мережні компоненти об'єднуються в домени автономності (ДА), у межах яких між ними встановлюється тісна взаємодія, зокрема в межах певної території або функціональної області. У таких доменах когнітивні елементи та вузли можуть узгоджувати свою поведінку, кооперуватися та спільно приймати рішення щодо використання мережних і радіочастотних ресурсів.

Водночас кожний елемент, що входить до ДА, зберігає властивості автономності та певний рівень незалежності під час прийняття локальних рішень. Окремі домени автономності також можуть взаємодіяти між собою, утворюючи середовище мультидоменної кооперації**.** Така взаємодія забезпечує координацію функціонування великої кількості розподілених когнітивних пристроїв і мереж, що сприяє підвищенню ефективності використання ресурсів, адаптивності системи та якості надання інфокомунікаційних послуг [15].

Для організації взаємодії в межах кожного домену автономності використовується когнітивний агент (КА), який забезпечує координацію роботи КВ і КЕ. Завдяки цьому взаємодія може здійснюватися як між ДА в цілому, так і на рівні окремих КЕ. При цьому слід враховувати, що до складу ДА можуть входити також і ПВ (некогнітивні), функціонування яких контролюється та координується КВ [15].

У CIoT реалізується модель когнітивного управління, яка ґрунтується на концепції віртуального об’єкта, який є цифровим поданням відповідного фізичного об’єкта. Віртуальний об’єкт створюється, модифікується або видаляється програмними засобами динамічно, відповідно до змін стану фізичного об’єкта. Таким чином забезпечується відображення поточного стану реального фізичного об’єкта у цифровому середовищі. Для реалізації певних прикладних функцій або сервісів окремі віртуальні об’єкти можуть автоматично об’єднуватися між собою, утворюючи композитні (складені) віртуальні об’єкти (рис. 1.7). Таке об’єднання дозволяє інтегрувати інформацію від декількох фізичних об’єктів, забезпечуючи більш складну обробку даних, розширення функціональних можливостей системи та підтримку інтелектуальних («розумних») сервісів у середовищі CIoT [15].

Композитні віртуальні об’єкти являють собою сукупність семантично сумісних віртуальних об’єктів, які взаємодіють між собою та надають відповідні сервіси. Таке об’єднання дозволяє реалізовувати послуги IoT відповідно до заданих функціональних вимог. При цьому композитні об’єкти можуть повторно використовувати вже існуючі індивідуальні віртуальні об’єкти незалежно від їх початкової сфери застосування або домену функціонування. Важливою особливістю композитного об’єкта є можливість підтримки та узгодження характеристик окремих віртуальних об’єктів, а також динамічного налаштування їх параметрів відповідно до змін умов функціонування або контексту використання [15].

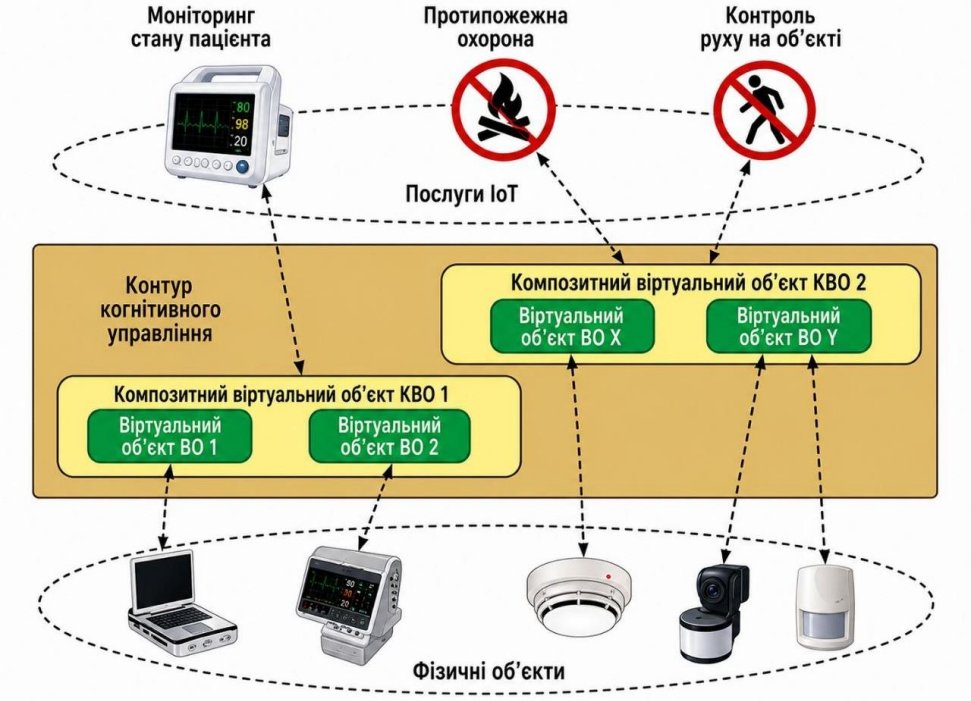


Рисунок 1.7 – Узагальнена модель управління в CIoT

Завершальним елементом моделі, що розглядається, є логіка послуг, призначення якої полягає у трансляції вимог прикладних додатків або користувачів IoT до відповідного композитного віртуального об'єкта, що забезпечує надання необхідної послуги [15].

Розглянемо приклад практичного застосування CIoT в аспекті вирішення задачі оптимізації часу у випадку надання невідкладної медичної допомоги пацієнту, що знаходиться за конкретною адресою. Зробимо припущення, що пацієнт перебуває під постійним дистанційним контролем, який реалізується системою медичного моніторингу на базі послуги IoT. Уявімо, що у певний момент система датчиків на тілі пацієнта зафіксувала погіршення його стану (наприклад, різке прискорення або переривчатість дихання, різку зміну пульсу, наявність серцевої аритмії, тощо) [15].

Показання датчиків (фізичних об'єктів) викликають відповідні зміни стану віртуальних об'єктів, які, як зазначалося, пов'язані із фізичним об'єктом через шлюз. Спеціальний додаток, який виконує обробку та трансляцію показань датчиків (наприклад, такий, що можна встановити на смартфон або планшет) здійснює обробку зазначену інформацію віртуального об'єкта і далі робить її перетворення у форму, що передається і використовується композитним

віртуальним об’єктом (в нашому прикладі – це центр швидкої медичної допомоги) [15].

У випадку, коли необхідний центр швидкої допомоги не був знайдений або немає вільного автомобілю скорої допомоги (у відповідності до бази знань – це необхідний фізичний об’єкт), то застосовується інший віртуальний об’єкт, що підходить для випадку, що виник, наприклад, датчик сигналізації якоїсь іншої служби. У результаті модель надання допомоги розширюється, шляхом включення нового композитного віртуального об’єкту – комплексна служба надання всебічної допомоги «112». Тобто швидка медична допомога може бути надана хворому не конкретним медичним центром, а, наприклад, службою порятунку, що буде викликана центром «112» , фахівці якої також мають навички надання першої медичної допомоги [15].

Якщо знову зробити припущення, що подія відбувається в «розумному місті», то медичні дані про стан хворого можуть одночасно пересилатися, як до медичного центру, так і до «розумного автомобіля» певної служби порятунку. Також паралельно інформативне повідомлення стосовно ситуації, що описується, може бути надіслане, наприклад, до служби регулювання дорожнього руху, яка зможе значно підвищити ефективність надання послуги, шляхом організації для автомобіля так званої «зеленої вулиці» у напрямку до помешкання хворого. Таким чином, наведений приклад щодо надання медичної допомоги наочно демонструє переваги когнітивності та когнітивного управління в аспекти вирішення задач практичного застосування інтернету речей [15].

1.4 Технології, що застосовуються у разі організації IoT-систем

Проведений аналіз концепції IoT та особливостей її архітектурних моделей показує, що ефективне функціонування IoT-систем в значній мірі залежить від способів організації взаємодії між пристроями, датчиками, інформаційними сервісами, тощо. Незважаючи на різноманітність архітектурних підходів, спільною вимогою для всіх систем IoT є забезпечення надійного, енергоефективного, безпечного та масштабованого обміну даними між великою кількістю розподілених об’єктів [3, 4, 8, 14].

У більшості сучасних реалізацій IoT основою побудови її мережної інфраструктури є бездротові технології зв’язку. Це пояснюється необхідністю

забезпечення мобільності пристроїв, спрощенням розгортання мереж, зменшенням витрат на кабельну систему і лінійні споруди та можливістю організації зв'язку у важкодоступних місцях або на територіально розподілених об'єктах. У зв'язку з цим особливої актуальності набуває дослідження технологій, які забезпечують ефективну взаємодію пристроїв у бездротових інфокомунікаційних системах.

На сьогодні для побудови IoT-систем використовується значна кількість технологій, що орієнтуються на підтримку бездротового доступу і забезпечують функціонування у середовищах бездротових інфокомунікаційних систем. Серед таких технологій важливе місце займають LoRaWAN, RFID та M2M. Кожна із цих технологій виконує свою власну функціональну роль у загальній концепції побудови інтернету речей і орієнтована на вирішення певного класу задач.

Технологія радіочастотної ідентифікації (RFID) фактично є однією з базових складових концепції IoT, оскільки забезпечує автоматичну ідентифікацію фізичних об'єктів. Основне призначення RFID полягає у безконтактному зчитуванні інформації з електронних міток, що прикріплюються до об'єктів. Це дозволяє однозначно і достовірно ідентифікувати пристрої, товари або інші матеріальні об'єкти. Завдяки цьому RFID широко використовується у логістиці, складському господарстві, транспортних системах, промисловості та системах контролю доступу. У контексті функціонування IoT радіочастотна ідентифікація реалізує початковий етап взаємодії із фізичним середовищем, зокрема автоматичну ідентифікацію об'єктів та отримання інформації про їх стан [6, 16].

Також в аспекті розвитку і підвищення ефективності IoT важливим є застосування технологій M2M, які забезпечують автоматизовану взаємодію між технічними пристроями без безпосередньої участі людини. Особливого значення застосування M2M набуває в концепції розвитку когнітивного інтернету речей, особливості і архітектурна модель якого була розглянута в попередньому підрозділі. На відміну від RFID, де основний акцент робиться на здійсненні ідентифікації об'єктів, технології M2M орієнтовані на організацію двостороннього обміну даними між машинами, датчиками, контролерами та інформаційними системами. M2M-технології широко застосовуються у системах промислової автоматизації, дистанційного моніторингу, телеметрії, енергетиці та транспортній галузі. Фактично M2M можна розглядати як одну з сучасних технологічних основ реалізації IoT (зокрема CIoT), що забезпечує автоматизоване функціонування розподілених технічних систем.

Іншою характерною технологією для IoT є широкозонна мережа великого радіуса дії (Long Range Wide Area Network, LoRaWAN), що належить до класу мереж з низьким енергоспоживанням (Low Power Wide Area Network, LPWAN). Звідси у спеціалізованих інформаційних джерелах та науково-технічних роботах найчастіше технологію LoRaWAN називають широкозонною мережею великого радіуса дії з низьким енергоспоживанням. Вона розроблена спеціально для забезпечення енергоефективного зв'язку між великою кількістю IoT-пристроїв, розташованих на значних відстанях один від одного [5]. Основними перевагами LoRaWAN є велика зона покриття, низьке енергоспоживання кінцевих пристроїв та можливість обслуговування значної кількості абонентських вузлів. Завдяки цим властивостям LoRaWAN активно використовується у системах «розумного міста», екологічного моніторингу, сільського господарства, енергетики та інфраструктурних системах.

Якщо порівняти вищеописані технології, то можна бачити, що зазначені технології мають різне функціональне призначення та не є взаємозамінними. Так, RFID найбільш ефективна для задач автоматичної ідентифікації об'єктів на невеликих відстанях, проте практично не використовується для організації мереж ПД. Технології M2M забезпечують автоматизований інформаційний обмін між пристроями та можуть використовувати різні мережні середовища, включаючи стільникові та локальні мережі. У свою чергу, LoRaWAN орієнтована на побудову масштабованих бездротових мереж з низьким енергоспоживанням і значною дальністю зв'язку, однак характеризується невисокою швидкістю передачі даних. Тобто вибір конкретної технології для організації взаємодії пристроїв у системах IoT визначається їх особливостями прикладного застосування, вимогами до дальності зв'язку, енергоспоживання, об'ємів даних, що передаються, кількості пристроїв та умовам їх експлуатації. Тому далі проаналізуємо зазначені технології, тому що це є важливим етапом дослідження реалізаціїї IoT у сучасних бездротових інфокомунікаційних системах.

2 ТЕХНОЛОГІЯ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ (RFID)

2.1 Загальні особливості технології RFID

Технологія RFID протягом останніх десятиліть пройшла шлях від спеціалізованої технології, яку використовували лише в окремих галузях, до одного із важливіших елементів сучасних систем IoT, в яких RFID широко застосовується для автоматизації процесів ідентифікації, обліку та контролю різноманітних об’єктів, що дозволяє суттєво підвищити ефективність логістичних, виробничих і складських процесів або застосовуватися для відстеження часу, наприклад, на спортивних змаганнях. Основною перевагою RFID є можливість дистанційної ідентифікації об’єктів за допомогою радіочастотного зв’язку. На відміну від традиційних технологій штрихового кодування (так званих штрих-кодів), RFID не потребує прямої видимості між ідентифікатором та зчитувальним пристроєм (рідером). Це дозволяє здійснювати автоматичне зчитування інформації навіть у випадках, коли RFID-мітка знаходиться всередині упаковки чи розташована поза прямою видимістю або серед інших подібних об’єктів [16].

Треба зазначити, що RFID-мітки не замінюють штрих-коди, а доповнюють їх можливістю дистанційного зчитування. Також вони у порівнянні із звичайними штрих-кодами забезпечують можливість використання значно більшої кількості унікальних ідентифікаторів. Крім ідентифікаційної інформації, у пам’яті RFID-міток можуть зберігатися додаткові дані, зокрема відомості про виробника, тип продукції, серійний номер, дату виготовлення та інші характеристики об’єкта. У деяких випадках RFID-мітки можуть взаємодіяти з датчиками та забезпечувати реєстрацію параметрів навколишнього середовища, наприклад температури, вологості або інших фізичних величин [16, 17].

Ще однією важливою особливістю RFID є можливість одночасного автоматичного зчитування великої кількості міток, що знаходяться в зоні дії рідера. На відміну від технології штрих-кодів, де кожний об’єкт необхідно окремо орієнтувати відносно сканера, RFID-система здатна без участі оператора виконувати ідентифікацію багатьох об’єктів одночасно. Завдяки цьому ця технологія значно підвищує швидкість обробки інформації та сприяє автоматизації процесів управління потоками фізичних об’єктів [16].

Зазначимо, що технологія RFID була створена ще в середині минулого століття, але її широке впровадження розпочалося лише останніми роками. Фактором, що тривалий час стримував масове застосування RFID, була відносно висока вартість електронних компонентів у порівнянні з традиційними засобами маркування. Однак розвиток мікроелектроніки та зниження вартості RFID-обладнання сприяли значному розширенню сфер її застосування. На сьогодні RFID досягла такого рівня техніко-економічної ефективності, який дозволяє використовувати її у великомасштабних системах IoT для обліку та управління товарами, транспортними засобами, виробничими ресурсами та іншими об’єктами

Таким чином, технологія RFID є важливою складовою систем IoT у разі розгортання сучасних бездротових інфокомунікаційних систем, забезпечуючи автоматичну ідентифікацію об’єктів, збір інформації та інтеграцію фізичних об’єктів у цифрове інформаційне середовище.

2.2 Компоненти і принцип дії системи RFID

Як вже стало зрозумілим із раніше викладеного, Система RFID складається із зчитувального пристрою (рідера) та спеціальної RFID-мітки (транспондера), в якій зберігається певна інформація, що записана в неї. Принцип роботи систем RFID є досить простим. Рідер передає електромагнітну енергію в навколишній простір. Мітка отримує сигнал від рідера і генерує відповідний сигнал, який приймається антеною рідера, обробляється електронним блоком і передається на термінал оператора через стандартизований інтерфейс (рис. 2.1) [17].

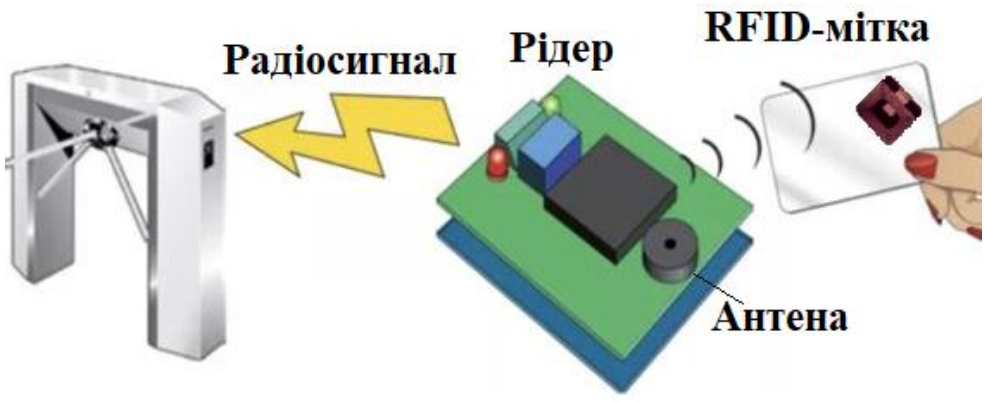


Рисунок 2.1 – Принцип функціонування системи RFID

Рідер має приймач та антену, яка надсилає сигнал до мітки та отримує відповідь; мікрочіп, який перевіряє та декодує дані, а також пам’ять, яка зберігає дані для подальшої передачі за потреби. Також у рідері є програмне забезпечення, яке дозволяє зчитувати, записувати та змінювати інформацію в мітці. Конструктивно рідер може бути як мобільним (переносний термінал), так і вбудованим у якийсь об’єкт (наприклад, у турнікет). Конструкція RFID-рідера наведена на рис. 2.2 [17].



Рисунок 2.2 – Конструкція рідера RFID

Основними компонентами RFID-мітки також є антена та мікрочіп, який є до неї підключений. Антена в основному визначає фізичні характеристики мітки. Кожна мітка повинна мати свій унікальний номер, який її ідентифікує. Без цього механізму ідентифікатори були б заплутаними, а інформація — спотвореною. Чіп має пам'ять, у якій зберігається ідентифікаційний код або інші дані. Мітка виявляє сигнал від рідера і починає передавати на нього дані, що зберігаються в пам’яті (рис. 2.1). Між рідером і міткою не потрібна лінія зв’язку, оскільки радіосигнал легко проникає крізь неметалеві матеріали. Таким чином, мітки можуть бути приховані в об’єктах, які необхідно ідентифікувати [16, 17].

Існує велика кількість різновидів RFID-систем, проте узагальнюючи їх можна поділити на два основні класи: активні та пасивні. Активні RFID-мітки потребують наявності власного джерела живлення. Таке живлення може забезпечуватися або шляхом підключення до зовнішньої енергетичної лінії, або за рахунок вбудованої акумуляторної батареї. Прикладом активної мітки є

транспондер, що встановлюється на літаку, який ідентифікує його національне походження. Іншим прикладом є пристрій LoJack, що встановлений на автомобілі, який використовує технологію стільникового зв'язку та GPS навігацію для визначення місцезнаходження автомобіля у разі викрадення. Але термін експлуатації активної мітки обмежується запасом енергії джерела живлення та інтенсивністю використання пристрою, також збільшується вартість і габаритні розміри. Це робить їх застосування економічно недоцільним для багатьох широких застосуваннях, зокрема у сфері торгівлі та логістики [16].

Тому найбільшого практичного поширення набули пасивні RFID-мітки, які не потребують власного джерела живлення, практично не вимагають технічного обслуговування і мають тривалий термін експлуатації. Вище, описуючи основні компоненти RFID-мітки, якраз і малася на увазі пасивна конструкція, тобто та, що складається з антени та мікрочіпа. Також може бути захисний корпус або оболонка. Захисна оболонка забезпечує механічну цілісність мітки та захищає її компоненти від впливу навколишнього середовища, механічних пошкоджень і хімічних речовин. Конструктивно така оболонка може бути виконана у вигляді герметичної скляної капсули (рис. 2.3а) або тонкої пластикової підкладки з клейовим шаром для зручного кріплення на об'єктах (рис. 2.3 б) [16].

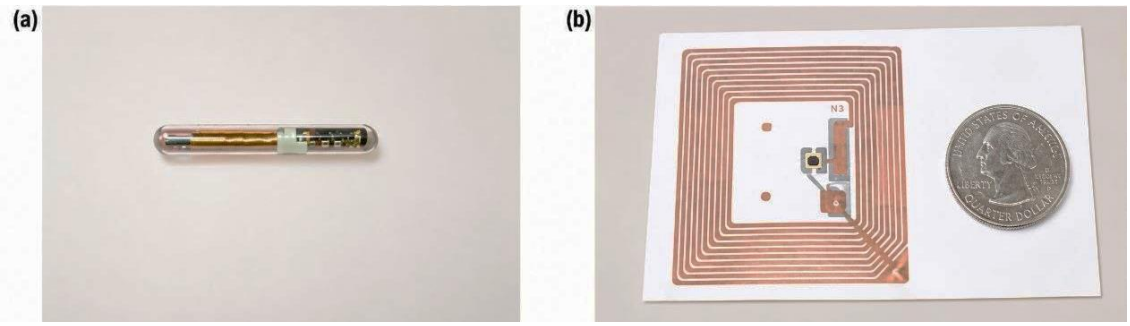


Рисунок 2.3 – Пасивні RFID-мітки: (а) Trovan – розміщена в скляному флаконі довжиною ~ 1 см; (б) Tiris – на ламіновані пластиковій основі (розмір ~ 5×5 см) з клейовим шаром для зручного кріплення до товарів

Для передачі енергії від рідера до пасивної RFID-мітки використовуються два принципово різні підходи: магнітна індукція і захоплення електромагнітної хвилі. Обидва підходи базуються на фізичних властивостях електромагнітного поля радіочастотної антени та використовують відповідно ближню зону (Near Field) і дальню зону (Far Field) її випромінювання. У ближній зоні передача

енергії здійснюється переважно за рахунок магнітного поля між антеною рідера та антеною мітки, подібно до принципу роботи трансформатора. У дальній зоні мітка отримує енергію безпосередньо з електромагнітної хвилі, що поширюється у просторі. Обидва методи забезпечують передачу достатньої кількості енергії для функціонування пасивної мітки. Залежно від типу RFID-пристрою потужність, яка передається до мітки, може становити приблизно від 10 Вт до 1 мВт. Крім передачі енергії, сигнали ближньої та дальньої зон використовуються також для двостороннього обміну даними між міткою та рідером, для чого застосовуються різні методи модуляції сигналів [16].

2.3 Технологія RFID ближньої зони

Принцип роботи RFID-систем ближньої зони ґрунтується на законі електромагнітної індукції Фарадея. У таких системах взаємодія між рідером і RFID-міткою реалізується за допомогою магнітного зв’язку. Зчитувач пропускає через свою антенну котушку змінний електричний струм великої амплітуди, внаслідок чого в навколишньому просторі формується змінне магнітне поле. Якщо в зоні дії цього поля знаходиться RFID-мітка, що буде містити антену у вигляді котушки меншого розміру (рис. 2.4), то на ній з’явиться змінна напруга. Після випрямлення цієї напруги та накопичення енергії в конденсаторі формується запас електричного заряду, який використовується для живлення електронної схеми RFID-мітки. Таким чином, пасивна RFID-мітка не потребує власного джерела живлення для мікрочіпа, оскільки необхідна енергія надходить від електромагнітного поля рідера [16].

Передача інформації від мітки до рідера в області ближньої зони здійснюється за допомогою методу модуляції навантаження. Суть цього методу полягає в тому, що зміна струму в антенній котушці мітки призводить до виникнення власного магнітного поля, яке впливає на магнітне поле рідера. У результаті в антені рідера спостерігаються незначні зміни струму, величина яких залежить від навантаження, що підключене до котушки мітки. Аналізуючи ці зміни, рідер може відновити інформацію, що передається RFID-міткою (звідси й назва «модуляція навантаження») [16].

Зазначений принцип аналогічний принципу роботи звичайного силового трансформатора, у якому передача енергії відбувається між первинною та

вторинною обмотками за рахунок магнітного поля. Проте на відміну від трансформатора, у RFID-системах відстань між антенами рідера та мітки може бути значно більшою. Таким чином, якщо електроніка мітки створює навантаження на власну антенну котушку та змінює його з часом, то сигнал можна закодувати у вигляді незначних коливань напруженості магнітного поля, що представляють ідентифікатор мітки. Зчитувач може потім відновити цей сигнал, відстежуючи зміну струму, що протікає через котушку зчитувача. Для передачі даних можуть використовуватися різні методи кодування та модуляції залежно від кількості бітів ідентифікатора, швидкості передачі даних та вимог щодо завадостійкості [16].

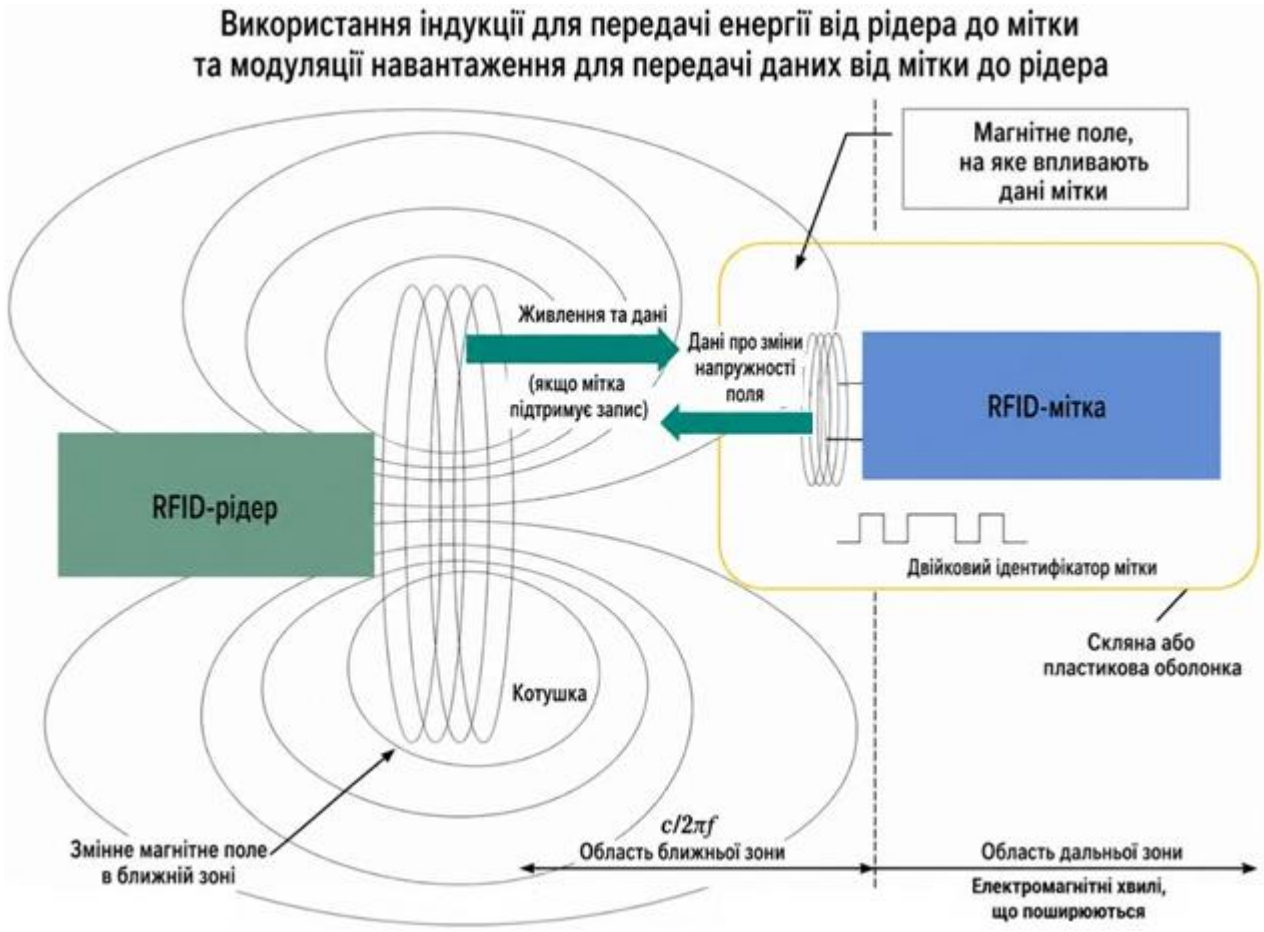


Рисунок 2.4 – Механізм передачі енергії та обміну даними в ближній зоні для RFID-міток, що працюють на частотах нижче 100 МГц

Використання магнітної індукції є найпростішим способом реалізації пасивних RFID-систем. Саме тому цей підхід був одним із перших, що знайшов широке практичне застосування, та став основою для створення ряду

міжнародних стандартів, зокрема ISO/IEC 15693 та ISO/IEC 14443, а також багатьох пропрієтарних RFID-рішень. Разом з тим RFID-системи ближньої зони мають певні фізичні обмеження. Максимальна відстань, на якій можливе ефективне використання магнітної індукції, приблизно визначається співвідношенням [16]:

$$R = \frac{c}{2\pi f}, \tag{2.1}$$

де c – щвидкість світла;

f – робоча частота системи.

Із підвищенням робочої частоти відстань, на якій може ефективно функціонувати система ближньої зони, зменшується. Крім того, інтенсивність магнітного поля швидко спадає зі збільшенням відстані між рідером і міткою. Магнітне поле слабшає пропорційно $1/r^3$, де r – це відстань між міткою та рідером уздовж центральної лінії, що є перпендикулярною до площини котушки. Треба також звернути увагу, що сучасні RFID-додатки вимагають використання більшої кількості ідентифікаційних бітів, а також одночасного зчитування багатьох міток та підвищення швидкості передачі даних. Це потребує збільшення робочої частоти системи, що, у свою чергу, обмежує ефективність магнітної індукції. Саме тому подальший розвиток RFID-технологій привів до появи систем, що використовують механізм передачі енергії та обміну даними в дальній зоні, у яких передача енергії та даних здійснюється за рахунок електромагнітних хвиль [16].

2.4 Технологія RFID дальньої зони

RFID-мітки, принцип роботи яких базується на використанні електромагнітного випромінювання дальньої зони (рис. 2.5), отримують енергію від електромагнітних хвиль, що випромінюються дипольною антеною рідера. Менша дипольна антена, що розташована в RFID-мітці, приймає електромагнітну енергію, внаслідок чого на її виводах виникає змінна різниця потенціалів, що виникає між плечима диполя. За допомогою випрямляча, який реалізований на основі діода, ця напруга перетворюється на постійну та накопичується в

конденсаторі, забезпечуючи живлення електронних компонентів мітки. Однак, на відміну від RFID-систем ближньої зони, у яких використовується магнітна індукція, мітки дальньої зони розташовуються поза межами ближньої зони антени рідера. Тому використання методу модуляції навантаження для передачі інформації від мітки до рідера є неможливим [16].

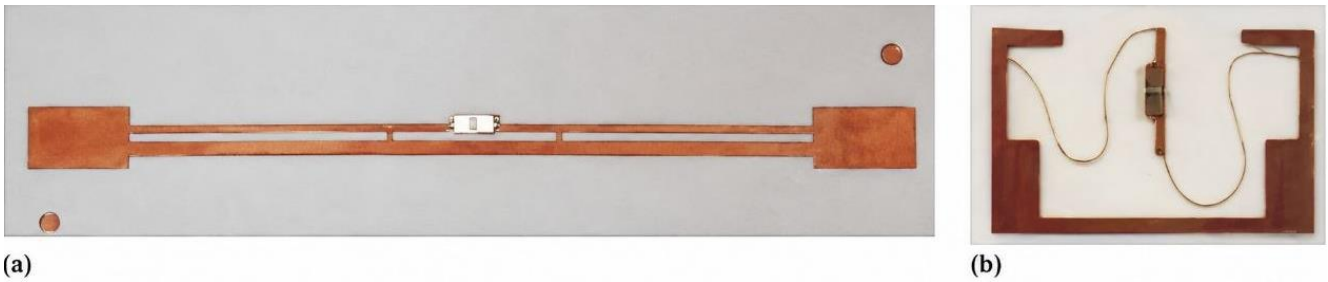


Рисунок 2.5 – RFID-мітки дальньої зони: (а) Alien на частоті 900 МГц (16×1 см), (б) Alien на частоті 2,45 ГГц (8×5 см)

Технологія, яку розробники використовують у комерційних RFID-системах дальньої зони називається зворотним розсіюванням (рис. 2.6). Принцип цієї технології полягає в тому, що антена RFID-мітки проєктується таким чином, щоб бути налаштованою на певну робочу частоту та максимально ефективно поглинати електромагнітну енергію, що надходить від рідера. Проте за наявності невідповідності імпедансів частина прийнятої енергії відбивається назад у напрямку рідера у вигляді слабкого електромагнітного сигналу, який рідер потім може виявити за допомогою чутливого приймача радіохвиль. Змінюючи в часі значення імпедансу своєї антени, RFID-мітка може змінювати величину відбитого сигналу, формуючи певну послідовність бітів, яка містить її ідентифікаційний код [16].

На практиці зміна імпедансу антени мітки може реалізовуватися шляхом підключення транзистора поперек її диполя та його періодичного перемикання між різними режимами роботи. У результаті відбувається модуляція коефіцієнта відбиття антени, що і забезпечує передачу інформації до зчитувача. Як правило, RFID-системи дальньої зони працюють на частотах, що перевищують 100 МГц, переважно у діапазоні ультрависоких частот (УВЧ), наприклад, на частотах 860 - 960 МГц або 2,45 ГГц. Нижче зазначених частот переважно використовуються RFID-системи, що функціонують на основі магнітної індукції та належать до систем ближньої зони [16].

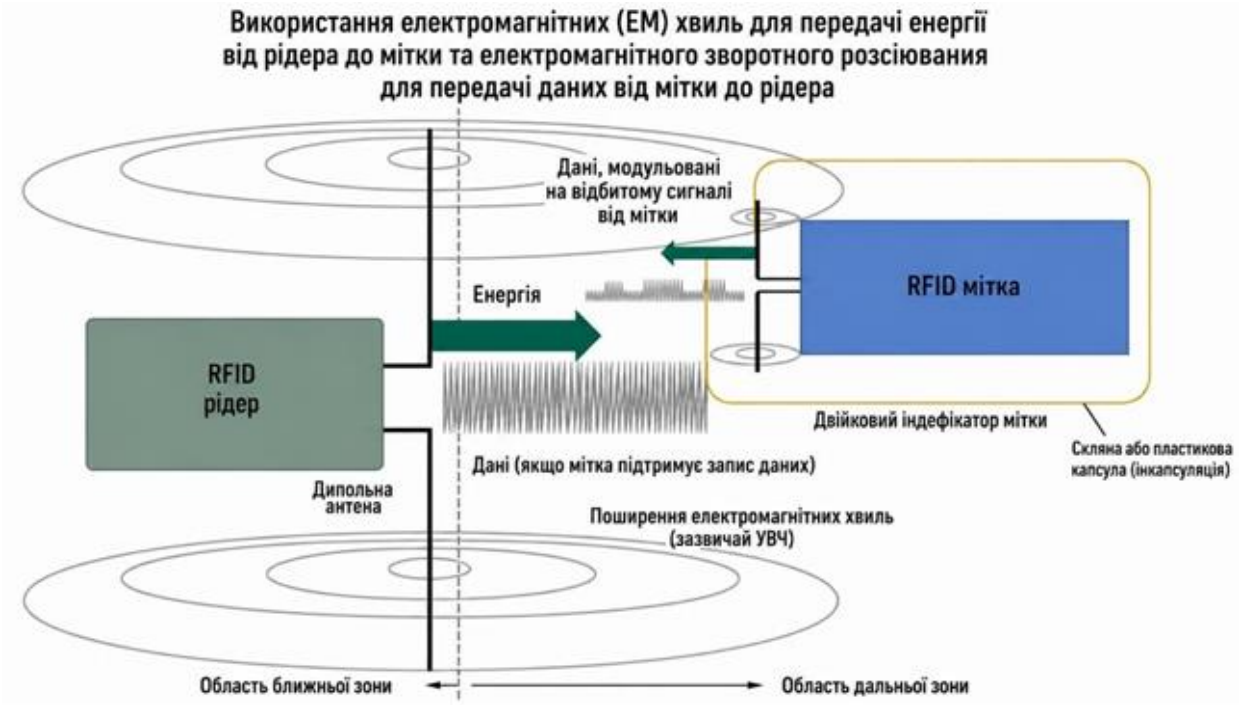


Рисунок 2.6 – Механізм передачі енергії та обміну даними в дальній зоні для RFID-міток, що працюють на частотах понад 100 МГц

Дальність дії RFID-систем дальньої зони визначається двома основними факторами: кількістю енергії, яка надходить від рідера до мітки, та чутливістю приймача рідера до слабкого відбитого сигналу. Слід ще раз акцентувати увагу, що енергія сигналу, який повертається від мітки до рідера, є дуже малою. Це пояснюється тим, що електромагнітний сигнал двічі зазнає ослаблення: під час поширення від рідера до мітки та під час поширення відбитого сигналу від мітки назад до рідера. Отже, енергія, що повертається, дорівнює $1/r^4$, де r – це відстань між рідером і RFID-міткою [16].

Проте постійний розвиток мікроелектроніки, що відповідає закономірностям, відомим як закон Мура, сприяв істотному зменшенню енергоспоживання напівпровідникових компонентів. Сучасні RFID-мітки потребують для своєї роботи лише декілька мікроват потужності, що дозволило суттєво збільшити дальність їх зчитування порівняно з попередніми поколіннями пристроїв. Крім того, були розроблені недорогі радіоприймачі з підвищеною чутливістю, що здатні реєструвати сигнали з рівнем потужності близько –100 дБм у діапазоні 2,4 ГГц. Завдяки цьому сучасні RFID-рідери дальньої зони можуть надійно зчитувати інформацію з міток на відстанях до 3 м, а окремі комерційні рішення забезпечують дальність зчитування навіть до 6 м [16].

Таким чином, RFID-системи дальньої зони забезпечують більшу дальність зчитування порівняно із системами ближньої зони та є ефективним засобом автоматичної ідентифікації об’єктів в IoT сучасних бездротових інфокомунікаційних систем.

3 ТЕХНОЛОГІЧНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ ШИРОКОЗОННИХ МЕРЕЖ ВЕЛИКОГО РАДІУСА ДІЇ З НИЗЬКИМ ЕНЕРГОСПОЖИВАННЯМ (LORAWAN)

3.1 Загальні особливості технології LoRaWAN та принципи її функціонування

Інтенсивний розвиток систем IoT з потребою забезпечення кращих показників щодо доступності, енергоефективності, швидкості і вартості розгортання, оптимізації обслуговування, – привів до бурхливого розвитку енергоефективних мереж дальнього радіусу дії (LPWAN), одним із класів яких є широкозонні мережі великого радіуса дії (LoRaWAN). По своїй суті LoRaWAN є відкритим мережним протоколом для великих бездротових систем з високою пропускною здатністю (близько до 1 млн. пристроїв), що характеризується низьким енергоспоживанням. Він використовує на фізичному рівні технологію широкосмугової модуляції LoRa (Long Range), завдяки якій забезпечує дальність передачі даних (до 15 км – на відкритій місцевості, і до 5 км – у міській забудові). Крім того, реалізує високу проникаючу здібність у міській забудові (можливе використання в глибоких підвалах без додаткових витрат), а також забезпечує захист сигналу від перешкод. В аспекті підтримки концепції IoT, LoRaWAN є орієнтованим на задоволення основних найважливіших її вимог, зокрема двонаправлений обмін даними, наскрізна безпека, мобільність пристроїв та сервісів визначення їх місцезнаходження [5, 18].

Функціонування мережі LoRaWAN в бездротовій інфокомунікаційній системі полягає в наступному. Базова станція (БС) безперервно здійснює моніторинг радіоефіру у визначеному частотному діапазоні. Якщо від одного з кінцевих пристроїв надходить пакет даних, базова станція приймає його та, за необхідності, передає відповідь на відповідній частоті. Для передачі інформації зазвичай використовується канал шириною 125 кГц, а максимальна швидкість передачі даних становить трохи більше 5 кБіт/с. На перший погляд така швидкість може здаватися занадто малою, однак ця технологія не призначена для передачі великих обсягів мультимедійної інформації, наприклад потокового відео чи іншого мультимедійного контенту. Основним призначенням LoRaWAN є швидка, надійна та енергоефективна передача невеликих інформаційних повідомлень від датчиків або інших IoT-пристроїв до БС. Саме тому невисока

швидкість передачі компенсується значною дальністю зв’язку, високою завадостійкістю та мінімальним енергоспоживанням кінцевих пристроїв [19].

Для адаптації параметрів зв’язку до поточних умов розповсюдження радіосигналу в технології LoRaWAN використовується коефіцієнт розширення спектра (Spreading Factor, SF), що є її ключовим параметром. Він визначає основні параметри модуляції, від яких залежать швидкість передачі даних, тривалість передачі пакета та завадостійкість радіоканалу. У специфікації LoRaWAN передбачено значення цього коефіцієнта від 7 до 12. Зокрема зі збільшенням значення SF підвищується завадостійкість системи та покращується можливість приймання сигналів на великих відстанях або в складних умовах поширення радіохвиль. Проте одночасно зменшується швидкість ПД і збільшується тривалість перебування пакета в ефірі. Наприклад, у разі SF = 12 досягається максимальна дальність зв’язку та найвища завадостійкість, однак швидкість передачі становить лише близько 292 біт/с, а тривалість передачі одного пакета може досягати 2,47 с. Слід враховувати, що збільшення часу перебування пакетів у радіоефірі призводить до зростання навантаження на БС. Якщо велика кількість датчиків використовує один і той самий радіоканал, збільшується ймовірність виникнення взаємних завад і знижується пропускна здатність мережі. Тому за сприятливих умов для розповсюдження сигналу система автоматично використовує менші значення SF, що забезпечує вищу швидкість передачі даних і скорочує час зайнятості радіоканалу. Зокрема, у випадку, коли SF = 7, тобто має найменше значення, то досягається можливість максимально швидко передавати дані та економити енергію, але радіус дії сигналу та стійкість до шумів помітно зменшуються. Такий адаптивний підхід дозволяє одночасно підтримувати високу енергоефективність кінцевих пристроїв і забезпечувати ефективне використання радіочастотного ресурсу мережі LoRaWAN [19].

3.2 Архітектура системи IoT із застосуванням технології LoRaWAN

Архітектура системи IoT на базі технології LoRaWAN реалізована за принципом «зірка зірок» (Star-of-Stars), у центрі якої знаходиться мережний сервер, до якого підключено декілька шлюзів та безліч кінцевих пристроїв, в якості яких тут виступають бездротові датчики та інші IoT-пристрої, що займаються збором та передачею інформації різного призначення (рис. 3.1) [5, 20].

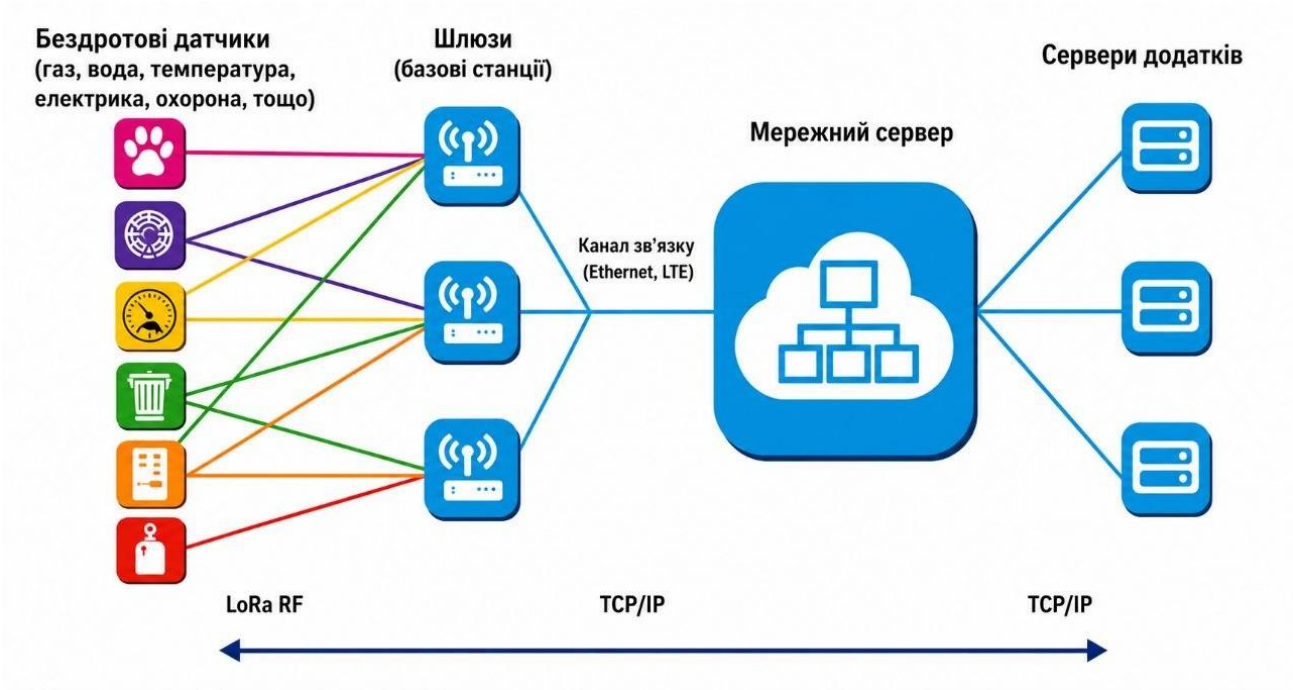


Рисунок 3.1 – Архітектурна модель системи IoT на базі технології LoRaWAN

Відповідно до принципів функціонування мережі LoRaWAN, який був розглянутий у попередньому підрозділі, пакети, що були сформовані датчиками, передаються по радіоканалу та приймаються БС, які в архітектурі LoRaWAN і виступають у якості шлюзів (див. рис. 3.1). При цьому вони не виконують обробку отриманої інформації, а лише забезпечують її передачу до мережного сервера. Шлюзи підключаються до мережного сервера за допомогою стандартних TCP/IP-з'єднань і функціонують як прозорий міст між радіомережою LoRaWAN та IP-мережею. Їх основне призначення полягає у перетворенні радіочастотних пакетів на IP-пакети для здійснення їх подальшої передачі мережею, а також у виконанні зворотного перетворення під час надсилання інформації від мережного сервера до датчиків [5, 18].

Мережний сервер координує роботу всіх шлюзів, контролює процес передачі повідомлень і визначає, через який шлюз доцільно здійснювати взаємодію з конкретним датчиком. Це особливо важливо у випадках, коли один і той самий пакет приймається одночасно кількома шлюзами. У такій ситуації мережний сервер виконує аналіз отриманої інформації, видаляє дублікати пакетів, обирає оптимальний маршрут передачі та реалізує інші функції управління мережею, зокрема адаптацію параметрів радіозв'язку, контроль автентифікації пристроїв та інші. Разом із тим мережний сервер не виконує обробку прикладних

даних, що містяться у пакетах. Ці функції покладаються на сервер додатків, який є завершальною ланкою архітектури LoRaWAN [19].

На сервері застосувань здійснюється розшифрування корисної інформації, що отримується від датчиків, її подальша обробка, зберігання та подання у вигляді, зручному для використання прикладними інформаційними системами. Залежно від призначення IoT-системи отримані дані можуть передаватися до систем диспетчерського управління, баз даних, білінгових систем, програмних інтерфейсів користувача, платформ моніторингу або інших інформаційних ресурсів, де вони використовуються для візуалізації, аналізу та прийняття відповідних рішень [19].

Бездротовий зв’язок у мережах LoRaWAN використовує переваги фізичного рівня LoRa, який забезпечує передавання даних на значні відстані. Завдяки цьому взаємодія між кінцевим пристроєм і мережною інфраструктурою здійснюється за один радіострибок (single-hop) через один або одночасно декілька шлюзів, що знаходяться в зоні його радіовидимості. Такий підхід спрощує реальну архітектуру мережі, зменшує енергоспоживання датчиків і підвищує надійність ПД. Наведена на рис. 3.1 архітектура LoRaWAN підтримує двосторонній обмін інформацією між датчиками та мережею, що дозволяє не лише приймати дані від датчиків, але й передавати до них команди управління або параметри конфігурації. Крім того, специфікація LoRaWAN передбачає підтримку багатоадресної передачі даних, яка забезпечує одночасне надсилання однакових повідомлень до групи датчиків. Використання такого багатоадресного режиму сприяє більш ефективному використанню радіочастотного спектра та зменшенню мережного навантаження під час виконання таких операцій, як дистанційне оновлення прошивки через бездротове середовище (Firmware Over-the-Air, FOTA), зміна параметрів їх роботи або передача інших службових повідомлень великій кількості датчиків [5].

У мережі LoRaWAN кожен датчик ідентифікується за допомогою набору унікальних параметрів, які забезпечують його автентифікацію, реєстрацію в мережі та захищений обмін даними. До основних ідентифікаційних параметрів належать унікальний 64-бітний ідентифікатор пристрою (DevEUI) та 32-бітна мережна адреса (DevAddr), яка призначається пристрою під час роботи в мережі та використовується для його адресації. Крім ідентифікації самого датчика, визначаються також параметри служби (додатку), з якою він взаємодіє. Для цього використовується 64-бітний ідентифікатор служби (AppEUI), який визначає

відповідну службу або мережу, а також 128-бітний ключ в цій службі (AppKey), що використовується для автентифікації датчика під час його реєстрації в мережі [20].

Специфікація LoRaWAN передбачає дві процедури активації та реєстрації датчиків у мережі: активація через бездротовий канал (Over-The-Air Activation, OTAA) та активація шляхом попереднього налаштування параметрів датчика (Activation By Personalization, ABP) [20].

Процедура OTAA є найбільш поширеним і рекомендованим способом реєстрації датчиків у мережі LoRaWAN. Для її виконання в пам'яті датчику та на мережному сервері мають бути у наявності параметри DevEUI, AppEUI та AppKey. Після першого підключення до мережі автоматично виконується процедура автентифікації, у результаті якої формуються два унікальні сеансові ключі шифрування [20]:

- NwkSKey (Network Session Key) – ключ мережного рівня, що використовується для захисту службових повідомлень та перевірки їх цілісності;

- AppSKey (Application Session Key) – ключ прикладного рівня, призначений для шифрування корисних даних, які передаються між датчиком і сервером додатків.

Автоматичне формування сеансових ключів підвищує рівень інформаційної безпеки та дозволяє періодично оновлювати криптографічні параметри без втручання користувача.

Процедура ABP передбачає попереднє налаштування всіх необхідних параметрів безпосередньо у датчику та на мережному сервері. У цьому випадку до пам'яті датчику заздалегідь записуються мережна адреса DevAddr, а також сеансові ключі NwkSKey і AppSKey. Завдяки цьому після ввімкнення датчик одразу готовий до роботи в мережі без виконання процедури активації через радіоканал. Після успішної реєстрації в мережі датчик може функціонувати в одному з трьох класів роботи, що визначені специфікацією LoRaWAN [20]:

1) Пристрої класу A – двонаправлені датчики з найменшою потужністю. Цей клас роботи має підтримуватися всіма датчиками мережі LoRaWAN за замовчуванням. Датчики у цьому класі більшу частину часу перебувають у пасивному режимі, але періодично за визначеним розкладом переходять в активний режим для передачі даних до сервера, і потім короткий час перебувають у режимі очікування підтвердження від нього. Після отримання підтвердження знову переходять у пасивний режим до наступного сеансу зв’язку. Такий режим роботи, з одного боку, забезпечує максимальне енергозбереження, а з іншого

боку, має недолік: у період між коротким обміном даними датчики недоступні для сервера, і він змушений чекати початку чергового сеансу зв’язку.

2) Пристрої класу B – двонаправлені датчики з певним часом очікування низхідного потоку від сервера. Тут датчики також, як і для класу A, більшу частину часу перебувають у пасивному режимі, але, тим не менш, між відправленнями даних регулярно переходять в активний режим і деякий час «слухають ефір». Ці часові інтервали «активності» суворо синхронізовані з сервером і реалізуються за рахунок деякого додаткового, хоча й досить низького, енергоспоживання датчиком. Таким чином, передача даних на датчик класу B буде здійснюватися значно швидше, ніж на датчик класу A, оскільки у цьому випадку не потрібно чекати на черговий сеанс ПД. Слід зазначити, що на сьогодні практично немає вільно розповсюджуваного серверного ПЗ, що підтримує роботу з датчиками класу B.

3) Пристрої класу C – двонаправлені датчики, що працюють з найменшою затримкою. Цей клас роботи датчиків характеризується тим, що більшу частину часу вони перебувають в активному режимі, що дає можливість у будь який час приймати дані від сервера. Однак за визначеним розкладом вони організовують короткі сеанси передачі своїх даних на сервер. Такі датчики споживають значно більше енергії, тому їх не рекомендується живити від акумулятора, але вони завжди доступні для сервера.

Слід зазначити, що для датчиків з акумуляторним живленням можна налаштувати тимчасові переходи між класами A і C, що дозволяє підвищити ефективність їх використання для виконання періодичних задач, які вимагають певного часу безперервної активності, наприклад, таких як оновлення прошивки через радіоканал.

Таким чином, можна бачити, що кожний із цих класів характеризується власними особливостями організації обміну даними, енергоспоживання та доступності пристрою для приймання повідомлень від мережі.

3.3 Переваги і недоліки технології LoRaWAN та її практичне застосування

У процесі аналізу, що був вище проведений було показано, що технологія LoRaWAN має низку особливостей, які визначають доцільність її використання для побудови бездротових систем IoT. Як і будь-яка інша технологія ПД,

LoRaWAN характеризується певними перевагами та обмеженнями, які необхідно враховувати під час розгортання та експлуатації мереж IoT [18].

Однією з основних переваг LoRaWAN є значна дальність бездротового зв'язку, яка суттєво перевищує аналогічні показники більшості бездротових технологій малого радіуса дії. Це дозволяє забезпечувати передачу інформації між датчиками та шлюзом на відстані від декількох до десятків кілометрів залежно від умов поширення радіохвиль.

Важливою особливістю технології є також висока проникна здатність радіосигналу, що забезпечує надійний зв'язок навіть у щільній міській забудові або всередині будівель. Завдяки цьому LoRaWAN може ефективно використовуватися в умовах, де інші бездротові технології демонструють обмежену дальність або нестабільну роботу.

Ще однією перевагою LoRaWAN є простота та швидкість розгортання мережі. Проаналізована вище архітектура типу «зірка зірок» (див. рис. 3.1) дозволяє одній базовій станції (шлюзу) обслуговувати велику територію без необхідності встановлення проміжних ретрансляторів або іншого допоміжного мережного обладнання. Це значно спрощує побудову мережі та зменшує витрати на її впровадження.

Суттєвою перевагою технології є також низьке енергоспоживання датчиків**.** Завдяки використанню енергоефективних алгоритмів ПД та особливостей протоколу LoRaWAN автономні датчики можуть працювати від одного елемента живлення протягом тривалого часу. Залежно від режиму функціонування, класу пристрою та інтенсивності передачі інформації термін автономної роботи може досягати до 10 років [18].

До переваг LoRaWAN також належать простота масштабування мережі та можливість підключення великої кількості датчиків без істотної зміни її структури. Крім того, у порівнянні з багатьма іншими системами бездротового моніторингу, технологія характеризується відносно невисокою вартістю як шлюзів, так і кінцевих IoT-пристроїв, що сприяє її широкому практичному застосуванню.

Разом із перевагами технологія LoRaWAN має і певні обмеження. Одним із них є порівняно велика затримка передачі інформації від датчика до сервера додатків. Залежно від режиму роботи мережі та параметрів зв'язку ця затримка може становити від кількох секунд до кількох десятків секунд. Іншим обмеженням є невисока пропускна здатність мережі. Швидкість передачі даних у

LoRaWAN змінюється від кількох сотень біт за секунду до кількох десятків кБіт за секунду залежно від вибраного коефіцієнта SF, ширини каналу та інших параметрів радіозв'язку. Тому технологія, як зазначалося вище, не призначена для передачі великих обсягів інформації або мультимедійних даних і використовується переважно для передачі коротких інформаційних повідомлень від датчиків.

Незважаючи на зазначені обмеження, сукупність технічних характеристик LoRaWAN робить її однією з найефективніших технологій побудови бездротових систем IoT. Велика дальність зв'язку, висока енергоефективність, добра проникна здатність радіосигналу та простота розгортання дозволяють використовувати LoRaWAN у багатьох галузях економіки та інфраструктури.Зокрема на практиці технологія широко застосовується для автоматизованого збору показників приладів обліку електроенергії, газу та води, моніторингу технічного стану інженерних систем, виявлення протікань, задимлення та аварійних ситуацій, контролю параметрів навколишнього середовища, відстеження місцезнаходження персоналу, транспортних засобів і матеріальних цінностей, управління системами зовнішнього освітлення, а також моніторингу умов вирощування рослин і утримання тварин у сільському господарстві. Крім того, LoRaWAN ефективно використовується для дистанційного контролю технічного стану промислового обладнання, інженерних споруд та інших об'єктів, що потребують здійснення безперервного моніторингу [18].

Такий широкий спектр практичних застосувань підтверджує, що LoRaWAN є однією з базових технологій реалізації сучасних систем інтернету речей, що орієнтовані на побудову масштабованих, енергоефективних і економічно доцільних бездротових інфокомунікаційних мереж.

4 ТЕХНОЛОГІЯ МІЖ МАШИННОЇ ВЗАЄМОДІЇ (M2M)

4.1 Загальні особливості технології M2M, її взаємозв’язок з IoT та принцип роботи

Технологія M2M є на цей час поширеною технологічною платформою організації IoT, тобто вона є однією із складових, на якій може ґрунтуватися концепція інтернету речей в цілому. Водночас M2M також в якості свої складових може підтримувати вище розглянуті технології RFID і LoRaWAN. Зокрема RFID взагалі стала першою технологією, яка була використана для реалізації концептуальних принципів M2M. Як зазначалося, це технологія обміну даними між різними пристроями та датчиками в IoT, тобто реалізує конкретний процес взаємодії між машинами без втручання людини і може використовувати різні мережні середовища, зокрема стільникові мережі різних стандартів (GSM/2G/3G/4G LTE/5G), мережі LoRaWAN, бездротові мережі (Wi-Fi, Zigbee), локальні мережі, тощо. Ця технологія широко використовується в системах охорони та безпеки, охороні здоров’я, промислових телеметричних і моніторингових системах, системах стеження, тощо [21, 22].

Якщо порівнювати, то M2M та інтернет речей мають багато спільних рис, оскільки обидві призначені для організації автоматизованого обміну інформацією між технічними пристроями. Проте, незважаючи на подібність, ці поняття не є тотожними та не можуть розглядатися як взаємозамінні. У багатьох аспектах інтернет речей є біль ширшим по своєму значенню терміном (з точки зору того, що підключається), а M2M – це, у деякому сенсі, невід’ємна частина IoT (тобто з точки зору як підключається, за допомогою яких інструментів). Технологія M2M передбачає саме реалізацію взаємодії машин між собою, тобто – це система організації прямого зв’язку між двома пристроями, тоді як IoT – це система підключення інтелектуальних («розумних») пристроїв до телекомунікаційних мереж для збору даних, здійснення їх аналізу та прийняття рішень на будь-якій відстані (рис. 4.1). Таким чином, концепція IoT об'єднує засоби зв'язку, обчислювальні ресурси, програмні платформи та прикладні сервіси в єдину екосистему. Іншими словами, будь-яка система інтернету речей обов'язково використовує механізми M2M-комунікації, оскільки саме вони забезпечують передачу інформації між пристроями. Проте наявність M2M-взаємодії ще не означає, що така система належить до IoT.

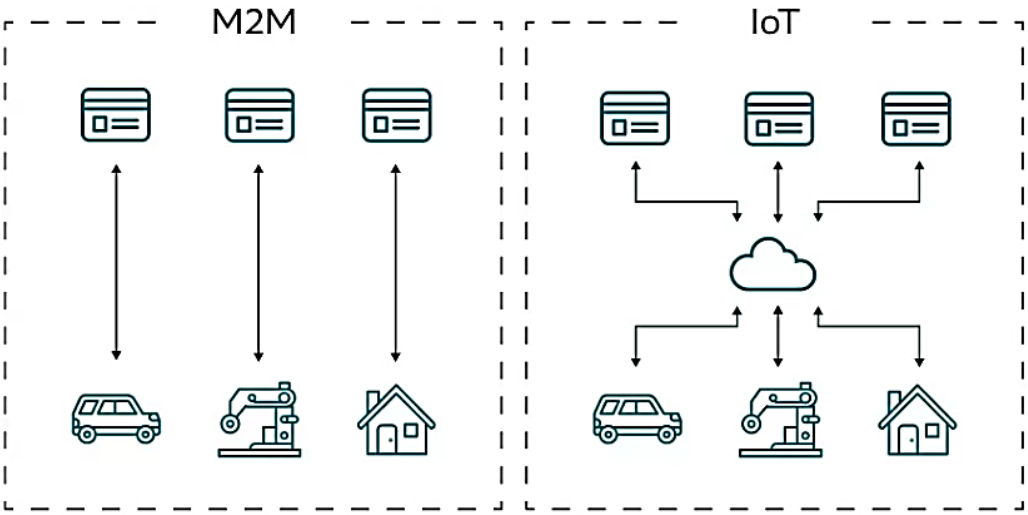


Рисунок 4.1 – Порівняння підходів взаємодії пристроїв на основі M2M та IoT

Наприклад, система визначення місцезнаходження транспортних засобів, у якій GPS-трекер автоматично передає координати на диспетчерський сервер, є прикладом реалізації технології M2M, оскільки забезпечує лише автоматизований обмін даними між технічними пристроями. Якщо ж ці дані додатково аналізуються інформаційною системою, використовуються для прогнозування дорожньої ситуації, побудови оптимальних маршрутів, автоматичного управління транспортними потоками або формування рекомендацій користувачам, то така система вже відповідає концепції Інтернету речей IoT [21, 22].

Таким чином можна сформулювати основні технологічні особливості M2M, що визначають її принципи побудови та функціонування [23]:

1) Автоматизована взаємодія між пристроями. Основою технології M2M є безпосередній обмін інформацією між технічними пристроями без участі людини. Для передачі даних можуть використовуватися різні канали зв'язку, зокрема дротові і бездротові інфокомунікаційні системи або Інтернет-з’єднання. Вибір способу передачі інформації залежить від вимог конкретної системи, умов експлуатації та необхідної дальності зв'язку.

2) Використання інтелектуальних («розумних») пристроїв. У технології M2M широко застосовуються спеціалізовані технічні засоби, зокрема датчики, виконавчі механізми, мікроконтролери, програмовані контролери, модулі збору даних та інші електронні пристрої. Вони забезпечують вимірювання фізичних параметрів, формування повідомлень та автоматичну передачу інформації до інших елементів системи M2M.

3) Програмні додатки для управління системою. Здійснення ефективного функціонування M2M-систем неможливе без наявності спеціалізованих додатків, яке забезпечує управління пристроями, конфігурацію параметрів роботи, обробку отриманих даних, контроль технічного стану обладнання та взаємодію із зовнішніми інформаційними системами.

4) Сервери та системи зберігання даних. У більшості систем M2M для накопичення, зберігання та обробки інформації використовуються локальні сервери або хмарні платформи. Це дозволяє централізовано здійснювати управління великою кількістю пристроїв, аналізувати отримані дані, формувати звіти та підтримувати функціонування прикладних сервісів.

5) Використання стандартів і протоколів ПД. Для забезпечення сумісності обладнання різних виробників у M2M використовуються стандартизовані мережні протоколи і технології, зокрема такі як TCP/IP, HTTP, а також інші більш спеціалізовані протоколи, що забезпечують надійний і захищений обмін інформацією між мережними пристроями [3, 23]:

- MQTT (Message Queuing Telemetry Transport) – енергоефективний мережевий протокол прикладного рівня, що створений спеціально для взаємодії пристроїв IoT та M2M. Цей протокол ідеально підходить для мереж із низькою пропускною здатністю або нестабільним зв’язком;

- служба распространения данных (Data Distribution Service, DDS) – протокол міжмашинної взаємодії від Object Managment Group (OMG), який використовує архітектуру «видавець-підписник» щоб забезпечити миттєву передачу критично важливих даних у системах реального часу завдяки високій надійності та з мінімальними затримками;

- IEEE 802.15.4 – базовий технічний стандарт для пристроїв IoT та M2M, що визначає фізичний рівень та рівень управління доступом до середовища для бездротових мереж з низьким енергоспоживанням та низькою швидкістю ПД, та інші протоколи.

Слід також звернути увагу на те, що під час проєктування та експлуатації систем M2M необхідно враховувати питання інформаційної безпеки. Зокрема, особливу увагу слід приділяти захисту каналів передачі даних, автентифікації пристроїв, забезпеченню конфіденційності інформації та протидії несанкціонованому доступу, оскільки зі збільшенням кількості взаємопов'язаних пристроїв зростає і кількість потенційних загроз [23].

У загальному випадку модель взаємодії M2M складається з трьох основних компонентів (рис. 4.2). Першим компонентом є цифровий пристрій або кінцевий вузол (A), який здійснює збір інформації за допомогою датчиків або інших засобів. Другим компонентом виступає канал зв'язку (B), що забезпечує передачу отриманих даних між пристроями. Третім компонентом є приймальний пристрій або сервер (C), який виконує приймання, зберігання, аналіз отриманої інформації та, за необхідності, формує управляючі команди. Залежно від функціонального призначення та умов експлуатації M2M-систем обмін даними може здійснюватися в односторонньому або двосторонньому режимі. Односторонній обмін передбачає передачу інформації лише від кінцевого пристрою до сервера або іншого вузла мережі, наприклад під час дистанційного збору показників датчиків. Двосторонній обмін, крім передачі даних, забезпечує можливість надсилання до пристрою команд керування, зміни параметрів його роботи або отримання службової інформації про його поточний стан [21, 23].



Рисунок 4.2 – Схема організації взаємодії пристроїв за технологією M2M

Така організація забезпечує автоматизований обмін даними між технічними пристроями без безпосереднього втручання людини та є базовим принципом побудови більшості сучасних систем за технологією M2M.

4.2 Архітектура M2M

На сьогодні для організації систем M2M використовується багато стандартів і технологій ПД, які забезпечують автоматизований обмін інформацією

між пристроями. Вибір конкретної технології визначається вимогами до швидкості ПД, дальності зв'язку, енергоспоживання, пропускної здатності мережі та особливостями практичного застосування системи. Найбільшого поширення в M2M-системах набули такі технології [23]:

- GSM (Global System for Mobile Communications) – технологія цифрового стільникового зв'язку, яка, окрім надання традиційних послуг стільникового зв'язку, також широко використовується для організації систем M2M завдяки значній зоні покриття та розвиненій мережній інфраструктурі;

- 3G (Third Generation) – технологія мобільного зв'язку третього покоління, що забезпечує вищу пропускну здатність і кращу якість передачі даних у порівнянні з GSM. Це дозволяє використовувати цю технологію для розгортання M2M, які потребують передачі більших обсягів інформації або роботи з більшою швидкістю;

- 4G LTE (Long Term Evolution) – технологія мобільного широкосмугового зв'язку четвертого покоління, яка характеризується ще вищою швидкістю ПД, меншою затримкою та більшою пропускною здатністю у порівнянні з мережами 3G. Завдяки цьому LTE широко застосовується в сучасних M2M-системах і є на цей час однією з провідних технологій реалізації IoT;

- LPWAN – клас широкозонних бездротових мереж з низьким енергоспоживанням, що призначені для підключення великої кількості автономних пристроїв IoT. Характерним представником технології LPWAN є мережі LoRaWAN, що були проаналізовані у третьому розділі, та які забезпечують передачу невеликих обсягів даних на значні відстані при мінімальному споживанні енергії, що робить їх ефективними для систем дистанційного моніторингу інженерної інфраструктури, «розумного» міста, екологічного контролю, транспортних систем та інших застосувань, де необхідна тривала автономна робота датчиків.

Важливою умовою розвитку технологій M2M є використання єдиних стандартів взаємодії між пристроями. Стандартизація забезпечує сумісність обладнання різних виробників, спрощує інтеграцію нових пристроїв у вже існуючі системи та створює можливість централізованого обміну інформацією між різними інфокомунікаційними платформами. Разом із тим існування великої кількості стандартів M2M може ускладнювати взаємодію обладнання різних виробників, що негативно впливає на масштабованість систем та швидкість їх впровадження. Тому дуже важливим є створення універсальних стандартів і протоколів обміну даними та відповідних програмних інтерфейсів. Це сприятиме

підвищенню сумісності обладнання, спрощенню інтеграції різнорідних пристроїв та подальшому розвитку концепції IoT на основі технології M2M [23].

Одним із таких рішень є архітектурна модель M2M, що розроблена Європейським інститутом стандартів телекомунікацій (European Telecommunications Standards Institute, ETSI). Ця архітектура визначає функціональну структуру мереж M2M, основні компоненти, принципи їх взаємодії та стандартизовані інтерфейси обміну даними. Архітектура ETSI побудована за багаторівневим принципом і складається з трьох основних рівнів: додатків M2M, сервісів і послуг та мережного, які у свою чергу входять до домену мережі. Також до домену мережі також входять функціональні модулі управління: функції управління системою M2M та функції управління мережею. Нижня частина архітектурної моделі відповідає домену пристроїв і шлюзів (рис. 4.3). Взаємодія між окремими компонентами наведеної архітектурної моделі здійснюється через відповідні інтерфейсні точки [23].

На верхньому рівні додатків створюються різноманітні додатки M2M, які реалізують прикладні функції системи відповідно із її призначенням. Саме на цьому рівні виконуються задачі моніторингу, диспетчерського управління, збору телеметричної інформації, автоматизації технологічних процесів, контролю інженерної інфраструктури, систем «розумного будинку», транспортних систем та інших прикладних сервісів. Треба зазначити, що додатки M2M можуть розташовуватися як у мережному домені, так і безпосередньо на кінцевих пристроях (датчиках) або шлюзах. Вони використовують сервіси і послуги нижнього рівня для обміну інформацією з обладнанням та отримання необхідних даних.

На рівні сервісів і послуг формуються та впроваджуються різноманітні сервісні можливості M2M (M2M Service Capabilities). Цей рівень є проміжною ланкою між додатками та мережною платформою, на якій розгорнута M2M, і забезпечує виконання універсальних функцій, які можуть використовуватися різними прикладними системами. Зокрема до основних функцій рівня сервісів і послуг належать [22, 23]:

- реєстрація та автентифікація пристроїв;
- управління з'єднаннями;
- маршрутизація повідомлень;
- зберігання та доставка інформації;
- управління подіями;
- забезпечення інформаційної безпеки;
- підтримка взаємодії між прикладними додатками та мережею.

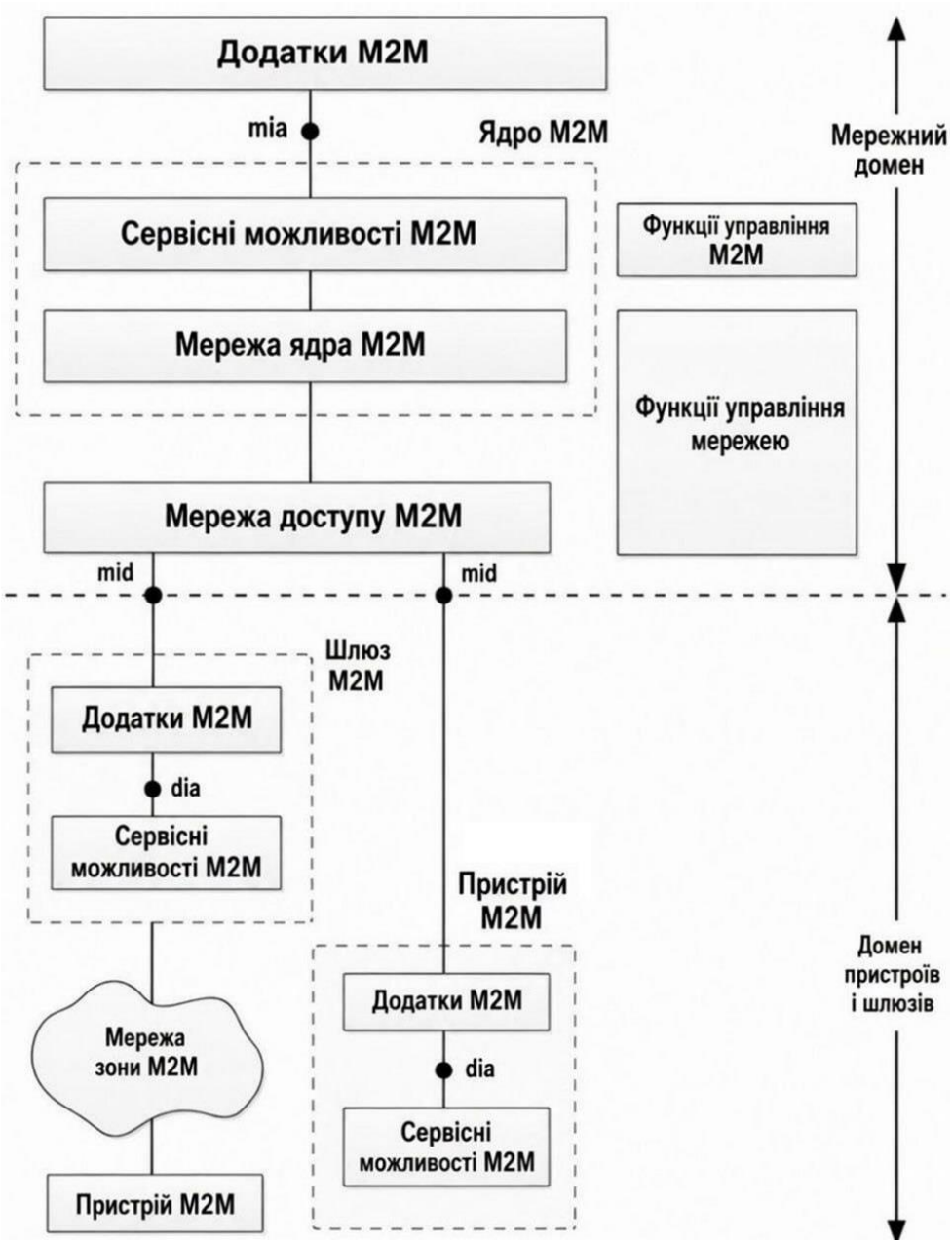


Рисунок 4.3 – Багаторівнева архітектурна модель M2M, що розроблена ETSI

Наявність рівня сервісів і послуг дозволяє уникнути дублювання однакових функцій у різних додатках і забезпечує уніфікований механізм доступу до ресурсів M2M-системи.

Базовою основою архітектури є її мережний рівень, який забезпечує обмін інформацією між усіма компонентами системи M2M. До його складу також входить модуль мережі доступу M2M, що забезпечує можливість підключення кінцевих пристроїв (датчиків) до телекомунікаційної мережі. В якості мереж доступу можуть використовуватися різні технології зв'язку, зокрема такі як: Ethernet, Wi-Fi, стільникові мережі GSM, UMTS, LTE, 5G, технологія LoRaWAN,

а також супутникові або інші телекомунікаційні системи. Передача інформації здійснюється до модуля ядра мережі M2M (M2M Core Network). Завдяки мережному ядру M2M забезпечується транспортування даних між мережами доступу та серверами додатків [23].

Основними компонентами домену пристроїв і шлюзів є M2M-пристрої, які виконують функції збору інформації від датчиків, управління виконавчими механізмами або безпосередньої взаємодії з фізичними об'єктами. Кожний пристрій може містити власні додатки та локальні сервісні можливості. У випадках, коли використовується група датчиків, що утворюють свою спеціалізовану локальну мережу, між нею та мережею доступу встановлюється M2M-шлюз, функціями кого є [23]:

- збір інформації від датчиків;
- агрегування даних;
- перетворення протоколів;
- забезпечення взаємодії між локальною мережею та зовнішньою телекомунікаційною мережею.

До шлюзу може підключатися мережа зони M2M, що об'єднує різноманітні датчики у групи, контролери та виконавчі пристрої.

Окреме місце в наведеній архітектурній моделі займають функції управління системами M2M та функції управління мережею). Функції управління системами M2M забезпечують конфігурування пристроїв, контроль їх працездатності, реєстрацію нових вузлів, оновлення ПЗ та централізоване адміністрування сервісів. Функції управління мережею відповідають за підтримку працездатності телекомунікаційної інфраструктури, моніторинг стану мережі, управління мережними ресурсами та забезпечення необхідних показників QoS.

Для забезпечення сумісності обладнання різних виробників архітектурна модель ETSI визначає точки інтерфейса, через які здійснюється взаємодія між окремими компонентами системи.

Існує кілька категорій точок інтерфейсу, які можуть застосовуватися в різних контекстах, наприклад [23]:

- агрегуючі вузли інтерфейсу – це пристрої, що відповідають за збір і ПД від пристроїв системи M2M до зовнішніх систем;
- брокерські вузли інтерфейсу – це пристрої, що сприяють обміну інформацією між пристроями;

- проксі-вузли інтерфейсу – це пристрої, що задіяні у забезпеченні безпеки та конфіденційності під час ПД між пристроями системи M2M та зовнішніми системами.

Інтерфейсні точки функціональної архітектури M2M є важливими у забезпеченні виконання функцій системи M2M, таких як збір та аналіз даних, управління пристроями, надання послуг тощо. Через них надається можливість пристроям M2M здійснювати взаємодію із зовнішніми системами та управляти ними, що забезпечує реалізацію широкого спектру додатків і сервісів, що орієнтовані на M2M-технології. Крім того, інтерфейсні точки є важливими у забезпеченні безпеки та конфіденційності обміну даними в системах M2M. Вони можуть застосовуватися для здійснення шифрування та автентифікації даних, а також для здійснення контролю доступу до пристроїв і до мережі. В залежності від наявних вимог до системи M2M можуть бути застосовані різні типи інтерфейсних точок, як окремо, так і в поєднанні один з одним [23]:

- mia (M2M Application Interface) – забезпечує взаємодію між M2M-додатками та сервісними можливостями мережного домену;

- dia (Device Application Interface) – використовується для взаємодії додатків, що працюють на M2M-пристроях або шлюзах, із локальними сервісними функціями;

- mid (M2M Interface for Device Domain) – забезпечує обмін інформацією між сервісними можливостями домену пристроїв і мережуим доменом через мережу доступу.

Наявність інтерфейсних точок забезпечує інтероперабельність обладнання, незалежність ПЗ від конкретних виробників та можливість побудови масштабованих M2M-систем.

Таким чином проаналізований підхід щодо організації архітектурної моделі M2M забезпечує модульність, масштабованість, сумісність обладнання різних виробників і спрощує інтеграцію систем M2M у сучасні інфокомунікаційні мережі у тому числі і бездротові та екосистеми інтернету речей.

ВИСНОВКИ

У кваліфікаційній роботі бакалавра проведено загальний аналіз концепції інтернету речей, а також технологічних особливостей організації і функціонування найбільш поширених технологій, що підтримуються цією концепцією, зокрема RFID, LoRaWAN та M2M, які визначають способи організації взаємодії в IoT між пристроями, датчиками, інформаційними сервісами, тощо. Розглянуто архітектурні моделі, як безпосередньо концепції IoT, так і зазначених технологій, проаналізовані принципи організації взаємодії між пристроями, датчиками, мережевою інфраструктурою та прикладними сервісами. Проведений аналіз дозволив визначити роль цих технологій у побудові сучасних систем, оцінити особливості їх практичного застосування та відповідні функціональні можливості у разі розгортання IoT у бездротових інфокомунікаційних системах.

У першому розділі розглянуті загальні технологічні особливості та архітектурні рішення концепції IoT. Показано, що функціонування IoT ґрунтується на трьох основних принципах: наявності розвиненої комунікаційної інфраструктури, яка забезпечує взаємодію пристроїв незалежно від їх місця розташування; унікальній ідентифікації кожного об'єкта для його однозначного розпізнавання в мережі, а також можливості обміну даними через мережу зв'язку або Інтернет, що забезпечує передачу інформації, взаємодію пристроїв та автоматизоване прийняття рішень.

Також показано, що базовою основою організації надійних і масштабованих IoT-систем є трьох-, чотирьох- та п’ятирівневі архітектурні моделі [13, 14]:

- трирівнева модель IoT забезпечує повний цикл функціонування системи: від збору та ідентифікації інформації на рівні фізичних об’єктів, через передачу даних мережею, до інтелектуальної обробки інформації та автоматизованого прийняття рішень. Така архітектура є основою побудови сучасних систем моніторингу, автоматизації та управління в інфокомунікаційних мережах;

- чотирирівнева архітектурна модель (ITU-T Y.2060) забезпечує комплексний підхід до побудови систем IoT, починаючи від збору інформації фізичними пристроями і завершуючи наданням прикладних сервісів користувачам, одночасно забезпечуючи необхідний рівень керованості та інформаційної безпеки;

- п’ятирівнева архітектурна модель ґрунтується на збільшенні деталізації і абстрагування функціональних можливостей IoT-систем. Зокрема вона дозволяє враховувати багато факторів, таких як: масштабованість, сумісність, надійність, QoS, тощо.

Також у цьому розділі розглянуті основні принципи побудови та архітектурна модель когнітивного інтернету речей (CIoT), який вважається подальшим розвитком платформи IoT, де «речі» (фізичні або віртуальні об’єкти, пристрої, датчики) пов’язані між собою та взаємодіють із мінімальним втручанням людини. Ця платформа передбачає наявність у системах IoT механізмів кооперації та інтелектуальної («розумної») взаємодії між мережними компонентами і, відповідно, її архітектурна модель показує можливості щодо забезпечення інтелектуальної взаємодії між фізичними та віртуальними об’єктами, автоматизованого формування послуг і прийняття рішень, а також надає підходи щодо адаптації системи до змін умов функціонування та потреб користувачів [15].

Результати аналізу концепції IoT та її архітектурних моделей свідчать про те, що ефективне функціонування IoT у значній мірі визначається організацією взаємодії між її пристроями і компонентами. У більшості сучасних реалізацій IoT основою побудови її мережної інфраструктури є бездротові технології зв’язку. Зокрема для побудови сучасних IoT-систем широко використовуються технології бездротового зв'язку RFID, LoRaWAN та M2M, кожна з яких пропонує свої власні підходи до реалізації взаємодії пристроїв в IoT-системах. RFID призначена для автоматичної ідентифікації об'єктів, M2M забезпечує автоматизований обмін даними між пристроями, а LoRaWAN використовується для побудови енергоефективних бездротових мереж великого радіуса дії. Вибір конкретної технології визначається вимогами прикладного застосування, зокрема необхідною дальністю зв'язку, енергоспоживанням, обсягом даних, що передаються, кількістю пристроїв та умовами їх експлуатації.

У відповідності з цим у другому розділі роботи було розглянуто і проаналізовано загальні особливості, компоненти, принципи дії і організації технології RFID. Ця технологія є важливою складовою сучасних бездротових інфокомунікаційних систем та систем Інтернету речей, забезпечуючи автоматичну ідентифікацію об’єктів, збір інформації та інтеграцію фізичних об’єктів у цифрове інформаційне середовище. Для передачі енергії від зчитувача до пасивної RFID-мітки використовуються два принципово різні підходи:

магнітна індукція і захоплення електромагнітної хвилі. Обидва підходи базуються на фізичних властивостях електромагнітного поля радіочастотної антени та використовують відповідно ближню і дальню зони її випромінювання. У ближній зоні передавання енергії здійснюється переважно за рахунок магнітного поля між антеною зчитувача та антеною мітки, подібно до принципу роботи трансформатора. У дальній зоні мітка отримує енергію безпосередньо з електромагнітної хвилі, що поширюється у просторі. Показано, що RFID-системи дальньої зони забезпечують більшу дальність зчитування порівняно із системами ближньої зони та є ефективним засобом автоматичної ідентифікації об’єктів у сучасних бездротових інфокомунікаційних системах і системах IoT [16, 17].

У третьому розділі роботи було розглянуто і проаналізовано загальні особливості та принципи функціонування технології LoRaWAN, а також архітектурна модель цієї технології. Зазначено, що архітектура LoRaWAN забезпечує чіткий розподіл функцій між окремими елементами мережі: кінцеві пристрої виконують збір інформації, шлюзи забезпечують її транспортування між радіомережею та IP-мережею, мережний сервер здійснює централізоване управління мережею, а сервер додатків відповідає за обробку, зберігання та використання даних відповідно до вимог конкретного IoT-застосування. Також у розділі наведений широкий спектр прикладного застосування технології LoRaWAN, що говорить про те, що вона є однією з ключових для реалізації сучасних систем IoT, які є орієнтованими на побудову масштабованих, енергоефективних і економічно доцільних бездротових інфокомунікаційних мереж [18 - 20].

Четвертий розділ кваліфікаційної роботи був присвячений розгляду загальних особливостей технології M2M та аналізу її взаємозв’язку з концепцією IoT. Крім того, також, як і в попередніх розділах проаналізована архітектурна модель M2M. Зазначено, що M2M ґрунтується на побудові мережі взаємопов'язаних пристроїв, які автоматично обмінюються інформацією за допомогою різних засобів зв'язку без безпосереднього втручання людини, що є базовим принципом [21, 22].

Показано, що технологія M2M та концепція IoT є взаємопов'язаними, але не тотожними поняттями. Встановлено, що головною відмінністю IoT від M2M є наявність інтелектуального рівня обробки інформації. Якщо технологія M2M забезпечує автоматизований обмін даними між технічними пристроями, то Інтернет речей реалізує повний цикл роботи з інформацією, що включає її збір,

передачу, аналіз, автоматизоване прийняття рішень і керування об'єктами. У зв'язку з цим M2M розглядається як одна з базових технологій, що забезпечує взаємодію між пристроями в системах IoT. Також обґрунтовано, що архітектурна модель ETSI є універсальною багаторівневою моделлю побудови M2M-систем, у якій функції збору інформації, передачі даних, надання сервісів, управління та прикладної обробки чітко розподілені між окремими рівнями. Такий підхід забезпечує модульність, масштабованість, сумісність обладнання різних виробників і спрощує інтеграцію M2M-систем у сучасні інфокомунікаційні мережі та екосистеми інтернету речей [23].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ITU. Internet of Things Global Standards Initiative [Електронний ресурс] // International Telecommunication Union. – Доступ здійснено 26.05.2026. – Режим доступу до ресурсу: https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx?utm_source=chatgpt.com.

2. Ashton K. That ‘Internet of Things’ Thing [Електронний ресурс] / K. Ashton // RFID Journal. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/expert-views/that-internet-of-things-thing/73881/?utm_source=chatgpt.com.

3. Al-Fuqaha A. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications [Електронний ресурс]/ A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash// IEEE Communications Surveys & Tutorials. – 2015. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7123563?utm_source=chatgpt.com.

4. Madakam S. Internet of Things (IoT): A Literature Review [Електронний ресурс] / S. Madakam, R. Ramaswamy, S. Tripathi // Journal of Computer and Communications – Vol.3, №5. – 2015. – Режим доступу до ресурсу: https://www.scirp.org/journal/paperinformation?paperid=56616&utm_source=chatgpt.com. DOI: 10.4236/jcc.2015.35021.

5. LoRa Alliance. What is LoRaWAN® Specification [Електронний ресурс] // LoRa Alliance. – Доступ здійснено 26.05.2026. – Режим доступу до ресурсу: https://lora-alliance.org/about-lorawan-old/?utm_source=chatgpt.com.

6. Scarfone K. Securing Radio Frequency Identification (RFID) Systems [Електронний ресурс]/ Karen A. Scarfone // National Institute of Standards and Technology (NIST). – 2017. – Режим доступу до ресурсу: https://www.nist.gov/publications/securing-radio-frequency-identification-rfid-systems?utm_source=chatgpt.com.

7. LTE Cat.1: идеальный баланс скорости, энергоэффективности и стоимости для IoT [Електронний ресурс] // блог компании «ЕМ Групп». – 2025. – Режим доступу до ресурсу: https://www.euromobile.ru/m2m-resheniya/lte-cat-1-idealnyy-balans-skorosti-energoeffektivnosti-i-stoimosti-dlya-iot/.

8. Max Rokatansky Что такое IoT и что о нем следует знать [Електронний ресурс] // Habr: блог компании OTUS. – 2021. – Режим доступу до ресурсу: https://habr.com/ru/companies/otus/articles/549550/.

9. Курушин М. Что такое Интернет вещей: полное объяснение и примеры [Електронний ресурс] / Миша Курушин // блог компанії «Timeweb Cloud». – 2025. – Режим доступу до ресурсу: https://timeweb.cloud/blog/chto-takoe-internet-veshchey-iot.

10. ITU Internet Reports 2005: The Internet of Things [Електронний ресурс] // International Telecommunication Union (ITU), Geneva. –2005. – 212 p. – Режим доступу до ресурсу: https://www.itu.int/net/wsis/tunis/newsroom/stats/The-internet-of-Things-2005.pdf.

11. Боронин П.Н. Интернет вещей как новая концепция развития сетей связи / П.Н. Боронин, А.Е. Кучерявый // Информационные технологии и телекоммуникации. – № 3 (7). – 2014. – С. 7 - 30.

12. Что такое Интернет вещей (IoT)? [Електронний ресурс] // SAP. – 2026. – Режим доступу до ресурсу: https://www.sap.com/central-asia-caucasus/resources/what-is-iot.

13. Платонов В. Обзор архитектур приложений для интернета вещей. Часть 1. [Електронний ресурс] / Валерий Платонов // Электронные компоненты. – №8. – 2025. – С. 41 - 48. – Режим доступу до ресурсу: https://elcomdesign.ru/uncategorized/obzor-arhitektur-prilozhenij-dlya-interneta-veshhej-chast-1/.

14. Khan R. Future Internet: The Internet of Things architecture, possible applications and key challenges [Електронний ресурс] / S. U. Khan, R. Zaheer, and S. Khan // in Proc. 10th Int. Conf. FIT. – 2012. – pp. 257 - 260. – Режим доступу до ресурсу: https://pureadmin.qub.ac.uk/ws/files/81384964/PID2566391.pdf.

15. Самсонов М. Когнитивный интернет вещей. Вещи все лучше адаптируются к людям [Електронний ресурс] / Михаил Самсонов, Александр Росляков, Александр Гребешков // ИКС. – №11. – 2014. – Режим доступу до ресурсу: https://www.iksmedia.ru/articles/5144194-Kognitivnyj-internet-veshhej-Veshhi.html?utm_referrer=https%3a%2f%2fwww.google.com%2f.

16. Want R. *An Introduction to RFID Technology* [Електронний ресурс] / R. Want // IEEE Pervasive Computing. – №5 (1) – 2006. – PP. 25 – 33. – Режим доступу до ресурсу: https://www.researchgate.net/publication/3437143_An_introduction_to_RFID_technology. DOI: 10.1109/MPRV.2006.2.

17. RFID-технологии и магнитные метки [Електронний ресурс] // All Technical Assistance. – Доступ здійснено 03.07.2026. – Режим доступу до ресурсу: http://allta.com.ua/what-is-rfid.

18. Огляд технології LoRaWAN [Електронний ресурс] // блог компанії Atiko. – Доступ здійснено 04.07.2026. – Режим доступу до ресурсу: https://www.atiko.com.ua/articles-ua/obzor-tekhnologii-lorawan-ua/.

19. Плотников О. Что такое LoRaWan Електронний ресурс] / Олег Плотников // Habr. – 2017. – Режим доступу до ресурсу: https://habr.com/ru/companies/nag/articles/371067/.

20. Гаевский С. Построение корпоративной сети LoRaWAN / Сергей Гаевский // Беспроводные технологии. – №3. – 2017. – С. 52 – 55.

21. Куконенко И. От машины к машине. Что такое M2M и как это применяют в бизнесе [Електронний ресурс] / Ирина Куконенко – руководитель проектов «M2M и кибербезопасность» МТС. – 2025. – Режим доступу до ресурсу: https://sber.pro/publication/ot-mashini-k-mashine-chto-takoe-m2m-i-kak-eto-primenyayut-v-biznese/.

22. Что такое технология M2M? [Електронний ресурс] // Top Connect (Эстония). – Доступ здійснено 05.07.2026. – Режим доступу до ресурсу: https://topconnect.com/ru/связь-m2m-и-iot/что-такое-технология-м2м/.

23. Лебедев М. Применение технологии M2M для автоматизации и управления системами: обзор и примеры приложений [Електронний ресурс] / Иван Лебедев, Антон Гонзиков, Джал Джангаев, Нарвик Тагиров, Бийарслан Забитов // Инновации и инвестиции. – №6. – 2023. – С. 160 – 164.