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

КВАЛІФІКАЦІЙНА РОБОТА

першого (бакалаврського) рівня вищої освіти

на тему:

«ПРОЕКТУВАННЯ СЕНСОРНИХ МЕРЕЖ IoT З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ BIGDATA»

Виконав: здобувач групи Кн-41
спеціальності 122 «Комп'ютерні науки»

_____ Макух В. А.
(прізвище та ініціали)

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

ДУБЛЯНИ-2025

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

Перший (бакалаврський) рівень вищої освіти
Спеціальність 122 «Комп'ютерні науки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

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

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Макуху Віктору Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи *«Проектування сенсорних мереж IoT з використанням технологій BigData»*
керівник роботи *к. т. н., доцент., Пташник В. В.*
(наук.ступінь, вч. звання, прізвище, ініціали)
затверджені наказом Львівського НУП *від 25.02.2025 року № 123/к-с.*
2. Строк подання студентом роботи *10 червня 2025 року*
3. Вихідні дані до роботи: *характеристика сучасних сенсорних мереж і протоколів зв'язку для IoT-систем; технічна документація на датчики, мікроконтролери та бездротові модулі (LoRa, NB-IoT тощо); специфікації та інструкції до платформ Big Data-аналітики (наприклад, Apache Hadoop, Spark); довідкова та науково-технічна література з проєктування енергоефективних IoT-рішень; вимоги до систем збору, обробки й аналізу телеметричних даних у розподілених мережах.*
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ
1. Основи функціонування та архітектури інтернету речей
2. Технології та методи реалізації високопродуктивних iot-систем
3. Розробка, моделювання та прогнозування енергоефективності IoT-системи
4. Охорона праці та безпека в надзвичайних ситуаціях
Висновки
Список використаних джерел
5. Перелік графічного матеріалу
Графічний матеріал подається у вигляді презентації

6. Консультанти розділів

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

7. Дата видачі завдання *28 листопада 2024 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Відмітка про виконання
1	*Аналіз основ функціонування та архітектури інтернету речей*	*28.11.2024 – 31.12.2024*	
2	*Вибір технології та методи реалізації високопродуктивних IoT-систем*	*01.01.2025 – 28.02.2025*	
3	*Розробка, моделювання та прогнозування енергоефективності IoT-системи*	*01.03.2025 – 30.04.2025*	
4	*Розгляд питань з охорони праці та безпеки у надзвичайних ситуаціях*	*01.05.2025 – 14.05.2025*	
5	*Завершення оформлення розрахунково-пояснювальної записки та презентаційного матеріалу*	*15.05.2025 – 31.05.2025*	
6	*Завершення роботи в цілому. Підготовка до захисту кваліфікаційної роботи*	*01.06.2025 – 10.06.2025*	

Здобувач _____ *Макух В.А.*
(підпис) (прізвище та ініціали)

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

УДК 681.521 / 681.518

Проектування сенсорних мереж IoT з використанням технологій BigData. Макух В. А. Кафедра інформаційних технологій – Дубляни, Львівський НУВМБ ім. С.З. Гжицького, 2025.

Кваліфікаційна робота: 57 сторінок текстової частини, 25 рисунків, 6 таблиць, 16 джерел літератури.

Мета кваліфікаційної роботи полягає розробці IoT-рішень для високопродуктивних сенсорних мереж з урахуванням можливостей обробки великих даних та підвищення енергоефективності.

Об'єктом дослідження є високопродуктивні бездротові сенсорні мережі в архітектурі IoT.

Предмет дослідження вивчає методи побудови енергоефективних IoT-систем з використанням технологій обробки великих даних

У першому розділі розглянуто концепцію Інтернету речей, архітектуру сенсорних мереж та принципи їх взаємодії з хмарними платформами. Описано вимоги до енергоефективності та особливості функціонування розподілених IoT-систем. У другому розділі проаналізовано основні технології бездротового зв'язку у контексті їх застосування в сенсорних мережах. Розглянуто архітектуру систем обробки великих даних та можливості інтеграції інтелектуальних методів обробки (ML/AI) для підвищення ефективності IoT-рішень. У третьому розділі наведено архітектуру системи моніторингу, виконано математичне моделювання енергоспоживання пристроїв. Розроблено комп'ютерну модель на основі нейромережі типу NARX для прогнозування енергоспоживання та підтверджено її ефективність експериментальними даними. Розглянуто питання безпеки під час проєктування, впровадження та експлуатації сенсорних мереж IoT, що працюють із великими обсягами даних.

Ключові слова: Інтернет речей, Big Data, енергоефективність.

ЗМІСТ

ВСТУП

Сучасний світ переживає стрімку цифрову трансформацію, в якій ключову роль відіграють технології Інтернету речей (IoT). Вони забезпечують автоматизований збір і передачу даних від фізичних об'єктів, що змінює підходи до управління процесами в різних галузях. Особливої актуальності набуває побудова високопродуктивних сенсорних мереж, здатних працювати у складних умовах з мінімальним енергоспоживанням.

Зі зростанням кількості підключених пристроїв постає потреба у використанні технологій великих даних (Big Data), що дозволяють ефективно обробляти великі обсяги інформації, які генеруються сенсорами в режимі реального часу. Big Data відкривають нові можливості для прогнозної аналітики, оптимізації ресурсів, підвищення точності прийняття рішень і виявлення аномалій у даних. Водночас інтеграція Big Data у структуру IoT-систем вимагає глибокого аналізу архітектурних рішень, методів обробки даних та енергозберігаючих алгоритмів.

Метою даної роботи є розробка методології створення IoT-рішень для високопродуктивних сенсорних мереж з урахуванням можливостей обробки великих даних та підвищення енергоефективності.

Для досягнення цієї мети були поставлені такі завдання:

- проаналізувати архітектуру, принципи функціонування та особливості побудови сенсорних мереж у середовищі IoT;
- дослідити застосування технологій Big Data у контексті обробки даних, що надходять від IoT-пристроїв;
- здійснити порівняльний аналіз сучасних технологій реалізації IoT у сенсорних мережах;
- сформулювати математичну модель роботи IoT-системи та розв'язати задачу енергоефективного функціонування.

РОЗДІЛ 1
ОСНОВИ ФУНКЦІОНУВАННЯ ТА АРХІТЕКТУРИ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Сутність та структура бездротових сенсорних мереж

Інтернет речей (IoT) — це система взаємопов'язаних комп'ютерних пристроїв, механічних і цифрових машин, об'єктів, тварин або людей, яким присвоєно унікальні ідентифікатори і які можуть передавати дані через мережу без участі людини [1]. На сучасному етапі розвитку IoT є високопродуктивною мережею з впровадженням бездротових технологій для організації передавання інформації в сенсорних мережах. На цьому етапі такі мережі отримали назву бездротових сенсорних мереж (WSN).

Бездротові сенсорні мережі WSN повинні мати можливість розгортати велику кількість дуже малих вузлів, які можна зібрати та налаштувати для досягнення спільної мети. Вони можуть динамічно адаптуватися до змін у середовищі розгортання та проактивно реагувати на зміни топології мережі.

Основними компонентами бездротової сенсорної мережі є: сенсорний модуль, процесорний модуль, модуль живлення, трансивер. Залежно від конкретного застосування бездротової сенсорної мережі до її складу можуть додаватися виконавчі пристрої (приводи), аналого-цифрові перетворювачі (АЦП) і монітори. На рисунку 1.1 представлено архітектуру вузла мережі.

Бездротові комунікаційні мережі формуються особливим чином, коли сенсорні вузли організовані без централізованої координації, що характерно для більшості застосувань WSN.

Джерелом живлення сенсорних вузлів є батареї, які зазвичай не підлягають перезарядженню або заміні, особливо в тих випадках, коли вузли мають працювати тривалий час без втручання людини [6, 19].

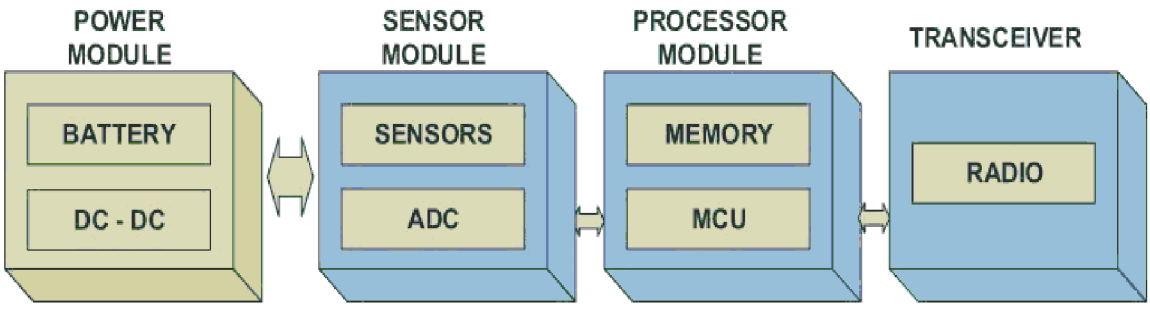

Рисунок 1.1 – Структура вузла високопродуктивної сенсорної мережі

Ретельне управління ресурсами є однією з ключових проблем при проєктуванні бездротових сенсорних мереж. Її можна вирішити за допомогою енергозберігаючих підходів, таких як оптимізація радіозв'язку, зменшення обсягу переданих даних, використання режимів сну й пробудження, енергоефективні протоколи маршрутизації та технології збору енергії.

1.2 Архітектурні рівні IoT-систем

Хоча кожна система IoT має свої особливості, основа архітектури IoT і загальний потік обробки даних є приблизно однаковими [7]. Архітектура IoT включає такі основні компоненти (рис. 1.2): гранична зона — ліворуч; обробка та аналіз подій — центр; термінальна програма — праворуч.

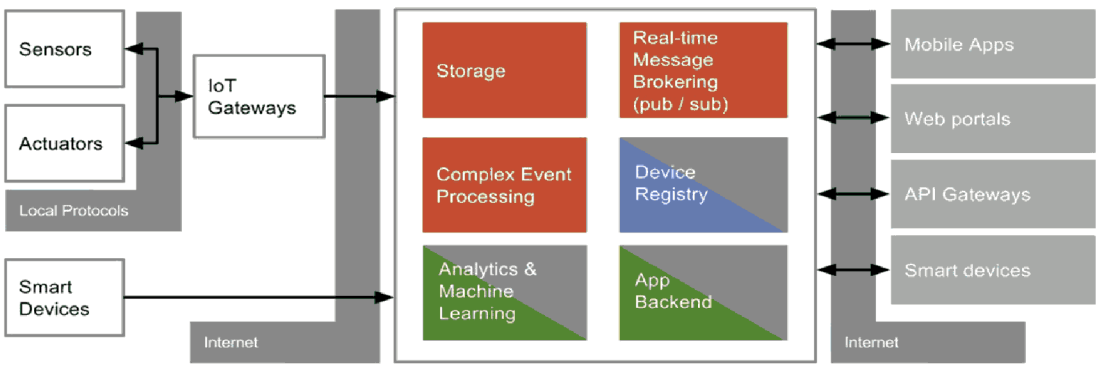

Рисунок 1.2 – Типова архітектура IoT-системи

В основі кожної системи IoT лежать підключені пристрої, які забезпечують отримання суттєвих даних для Інтернету речей. Для цього їм потрібні датчики, що реєструють фізичні параметри зовнішнього середовища або внутрішніх об'єктів. Ці датчики можуть бути вбудованими в сам пристрій або реалізованими як окремі компоненти, призначені для вимірювання та збору телеметричних даних. Наприклад, сільськогосподарські датчики вимірюють такі параметри, як температура й вологість повітря та ґрунту, рівень pH ґрунту або інтенсивність сонячного освітлення, що впливає на рослини.

Ще одним важливим елементом є актуатори. Вони тісно взаємодіють із датчиками, перетворюючи зібрані розумними об'єктами дані на фізичні дії. Уявімо собі розумну систему поливу, оснащену всіма необхідними датчиками. На основі отриманих даних система в реальному часі аналізує ситуацію та передає команду виконавчим механізмам відкрити вибрані водяні клапани там, де рівень вологості ґрунту нижчий за встановлене значення. Клапан залишається відкритим доки датчик не зафіксує нормалізацію вологості. Увесь процес відбувається без участі людини [7].

Не менш важливо, щоб підключені пристрої могли не лише обмінюватися двосторонніми даними зі шлюзами чи системами збору даних, а й розпізнавати один одного, спілкуватися між собою для збору, обміну інформацією та співпраці в режимі реального часу.

Досягнення такої взаємодії є складним завданням, особливо в умовах обмежених ресурсів та живлення від акумуляторів, адже для підтримки зв'язку потрібна висока обчислювальна потужність, що споживає цінну енергію та пропускну здатність. Надійна архітектура IoT повинна забезпечувати ефективне керування пристроями завдяки використанню відповідних, безпечних і малоресурсних протоколів зв'язку.

Таким чином, датчик розпізнає зміни, тобто фіксує вхідні дані. Вони присутні в різних пристроях і охоплюють широкі сфери застосування. Галузі застосування датчиків наведені на рисунку 1.3.

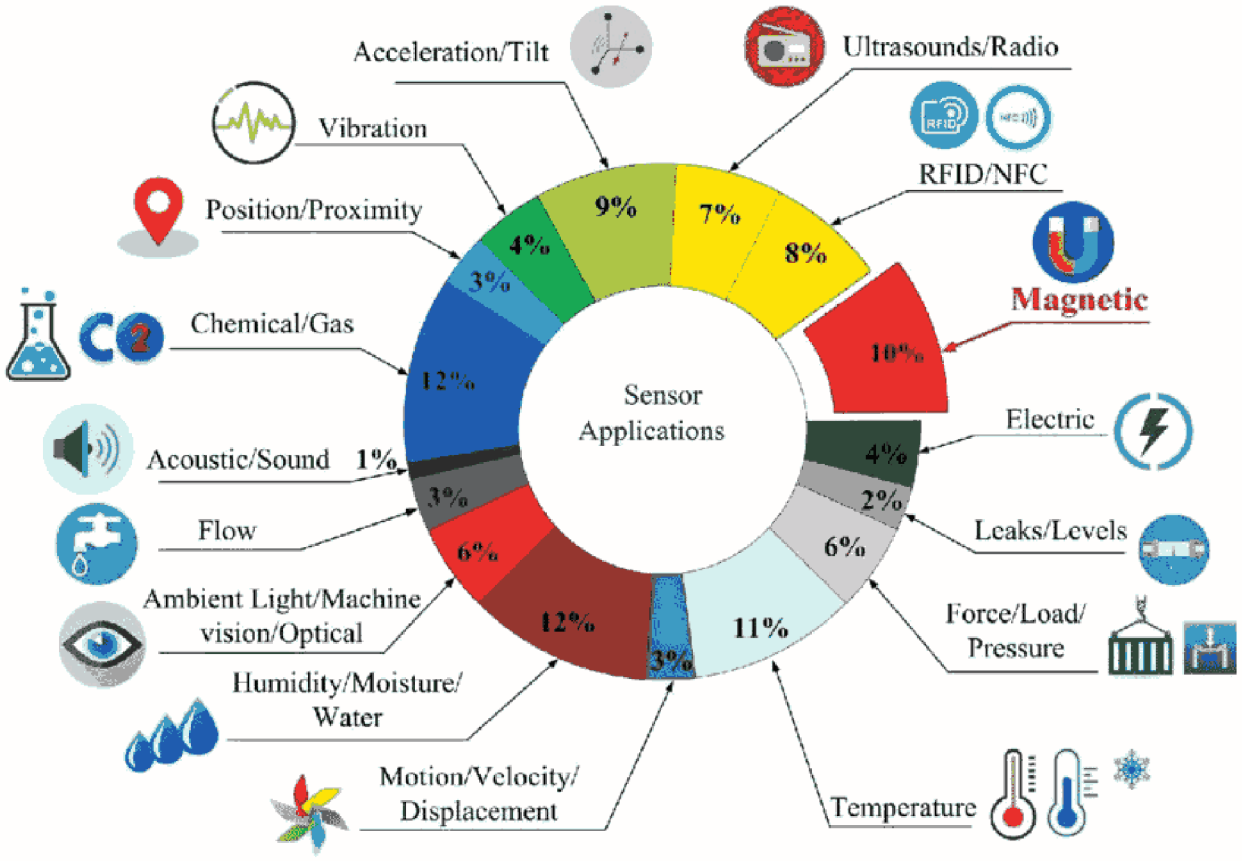

Рисунок 1.3 – Основні напрями застосування сенсорних пристроїв

Аналоговий датчик збирає потік даних, що можуть мінливо змінюватись. Однак передати такий тип даних по кабелю або бездротовим способом проблематично без попереднього перетворення сигналу на цифрову форму. Принцип обробки сигналу зображено на рисунку 1.4.

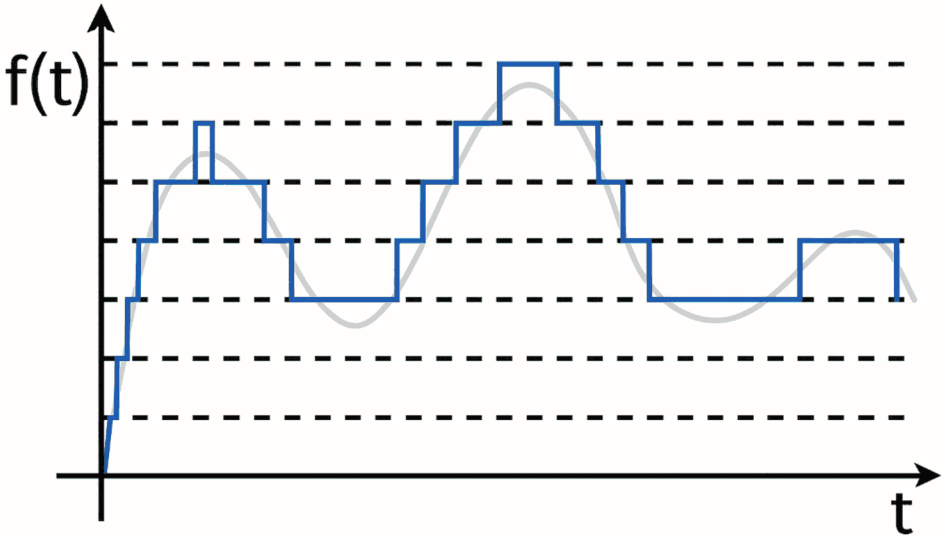

Рисунок 1.4 – Схема обробки цифрової інформації

Цифрові дані — це послідовність нулів і одиниць. Щоб перетворити аналогові дані на цифрові, безперервний аналоговий сигнал необхідно розбити на кілька окремих ділянок, кожній з яких призначається певне числове значення.

Хвиляста лінія на графіку представляє безперервний аналоговий сигнал, а червона пунктирна лінія — його цифрове представлення. Кожному кроку цифрового сигналу відповідає певне значення, закодоване у вигляді комбінації нулів і одиниць, що може передаватися як дротовими, так і бездротовими мережами.

Виконавчий механізм отримує вихідні дані. Людське тіло є найкращим прикладом системи, що включає як датчики, так і виконавчі механізми. Мозок людини виконує роль мікроконтролера, об'єднуючи дані, зібрані численними сенсорами, для формування надійних і точних рішень.

Шлюз. Незважаючи на те, що цей рівень все ще функціонує поблизу датчиків і виконавчих механізмів пристрою, його доцільно розглядати як окремий етап архітектури IoT, оскільки він має критичне значення для процесів збору, фільтрації та передачі даних до периферійної інфраструктури та хмарних платформ. Враховуючи величезний обсяг вхідних і вихідних даних, що може генеруватися в результаті розгортання мільйонів пристроїв, ключовими є процеси агрегації даних, їх відбір і передача [8].

Шлюзи та системи збору даних, виступаючи посередниками між підключеними об'єктами, хмарами та аналітичними платформами, забезпечують необхідні точки з'єднання, які поєднують основні рівні архітектури.

Шлюз полегшує обмін даними між датчиками та іншими компонентами системи, перетворюючи інформацію у формат, зручний для подальшого використання. Крім того, шлюзи можуть контролювати, фільтрувати та відбирати дані з метою мінімізації обсягу інформації, яка надсилається до хмари, що, у свою чергу, знижує витрати на передачу через

мережу. Таким чином, шлюз виконує попередню локальну обробку даних, стискаючи їх у корисні інформаційні пакети для подальшого аналізу.

Іншою важливою функцією шлюзу є забезпечення безпеки. Оскільки шлюз відповідає за керування двонаправленим потоком інформації, застосування відповідних методів шифрування й захисту допомагає запобігти витоку даних із хмари IoT та зменшити ризик зловмисних атак на IoT-пристрої.

Таким чином, шлюзи IoT виконують широкий спектр функцій: обробку та фільтрацію даних, забезпечення безпеки, підключення пристроїв, оновлення тощо. Вони не лише реалізують зазначені функції, а й можуть слугувати платформою для програм, що працюють на ПК або інших пристроях, забезпечуючи інтелектуальну обробку даних.

1.3 Периферійні та хмарні обчислення в IoT-інфраструктурі

Хоча периферійні обчислення не є обов'язковим елементом кожної архітектури IoT, вони можуть надавати суттєві переваги, особливо у великих проєктах. З огляду на обмеження пропускної здатності та затримки при передачі даних до хмари, периферійні системи здатні забезпечити швидший відгук і більшу гнучкість у процесах обробки та аналізу даних. Оскільки швидкість обробки інформації має вирішальне значення для низки застосунків у сфері промислового Інтернету речей (IIoT), популярність периферійних обчислень останнім часом суттєво зросла [8].

Оскільки периферійна інфраструктура фізично розміщується ближче до джерел даних, вона може швидше реагувати на події в режимі реального часу та забезпечувати миттєве виведення результатів. У таких випадках до хмари передається лише оброблена або агрегована інформація, тоді як «сирі» дані обробляються локально, що дозволяє ефективніше використовувати ресурси.

Безпеку можна суттєво підвищити шляхом мінімізації вразливостей мережі, а знижене енергоспоживання та оптимальне використання пропускної здатності сприяють ефективнішому використанню бізнес-ресурсів.

Якщо датчики — це нейрони, а шлюзи — основа Інтернету речей, то хмара — це мозок у тілі цієї системи. На відміну від периферійних рішень, центри обробки даних або хмарні платформи призначені для зберігання, обробки та глибокого аналізу великих обсягів інформації за допомогою потужних засобів аналітики та алгоритмів машинного навчання, які зазвичай не підтримуються периферійними пристроями.

Протягом останніх кількох років хмарні обчислення стали більш поширеними, особливо в промислових архітектурах Інтернету речей, сприяючи підвищенню продуктивності, зменшенню кількості незапланованих простоїв і зниженню енергоспоживання [7, 8].

Надаючи оптимальні рішення для прикладних задач користувача, хмара відкриває можливості для бізнес-аналітики та візуалізації, допомагаючи користувачам взаємодіяти з системами, контролювати та відстежувати їх роботу, а також ухвалювати обґрунтовані рішення на основі звітів, інформаційних панелей і даних у реальному часі.

РОЗДІЛ 2
ТЕХНОЛОГІЇ ТА МЕТОДИ РЕАЛІЗАЦІЇ ВИСОКОПРОДУКТИВНИХ IoT-СИСТЕМ

2.1 Взаємодія IoT-систем із Big Data: принципи обробки, архітектура та сенсорні мережі

Великі дані — це комбінація структурованих, напівструктурованих і неструктурованих даних, зібраних організацією, які можна використовувати у проєктах машинного навчання, прогнозному моделюванні та інших сучасних аналітичних застосуваннях [11].

Системи обробки та зберігання великих даних стали звичним компонентом архітектур управління даними в організаціях. Великі дані зазвичай характеризуються трьома основними властивостями:

- великим обсягом даних у різноманітних середовищах;
- широкою різноманітністю типів даних, що зберігаються;
- високою швидкістю генерації, збору та обробки даних.

Останнім часом до цих характеристик додано інші, зокрема: достовірність, цінність та мінливість [12].

Хоча великі дані не мають чітко визначеного обсягу, їх застосування зазвичай охоплює терабайти, петабайти або навіть ексабайти інформації, зібраної протягом певного періоду.

Компанії використовують великі обсяги даних, накопичених у своїх системах, для підвищення ефективності операцій, покращення обслуговування клієнтів, створення персоналізованих рекламних кампаній на основі конкретних уподобань споживачів і, в результаті, — підвищення прибутковості. Використовуючи клієнтські дані, можна проводити комплексний аналіз, що охоплює поведінку користувачів, реакції в соціальних мережах і ставлення до бренду. Це дає змогу порівнювати

компанію з конкурентами, точніше визначати цільову аудиторію, проектувати нові продукти та підвищувати рівень задоволеності клієнтів, вчасно реагуючи на проблеми та зберігаючи їхню лояльність.

Обсяг — це найчастіше згадувана характеристика великих даних. Хоча великі дані не завжди передбачають гігантські обсяги, у більшості випадків саме так і є через характер інформації, яка збирається та зберігається. Потоки кліків, системні журнали й потокові системи — одні з найпоширеніших джерел, що постійно генерують великі обсяги даних [14].

Швидкість — у контексті великих даних цей параметр стосується темпів, з якими генеруються великі обсяги інформації, що потребує обробки та аналізу. У багатьох випадках великі набори даних оновлюються в режимі реального або майже реального часу, на відміну від традиційних сховищ даних, які оновлюються щодня, щотижня або щомісяця. Програми для аналітики великих даних отримують, узгоджують і аналізують вхідні дані, а потім формують результати або відповіді на основі складних запитів. Це означає, що аналітики даних і дослідники повинні добре розуміти наявну інформацію та чітко усвідомлювати, які саме відповіді вони шукають, щоб забезпечити дійсність і актуальність отриманих результатів. На рисунку 2.1 представлено динаміку зростання обсягів великих даних.

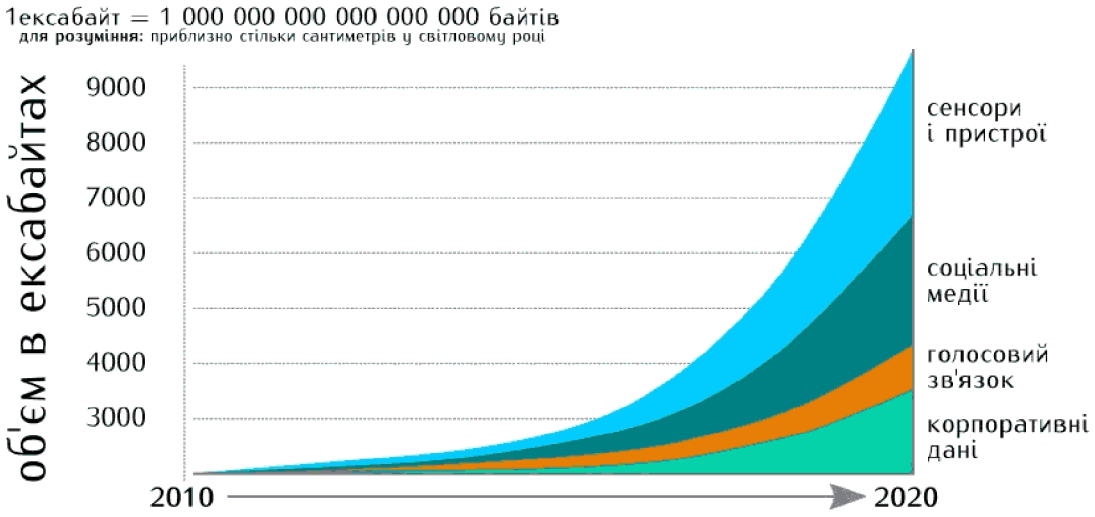

Рисунок 2.1 – Тенденції зростання обсягів Big Data

Достовірність даних означає надійність і якість набору даних. Невизначені або необроблені дані, зібрані з багатьох джерел, таких як соціальні мережі чи вебсторінки, можуть спричинити серйозні проблеми з якістю, які важко виявити та усунути.

Низькоякісні дані призводять до недостовірного аналізу, що може знизити довіру до аналітики загалом. Тому важливо враховувати обсяг невизначених або нечітких даних в організації перед тим, як застосовувати їх у проєктах аналітики великих даних. ІТ-відділи та аналітики повинні переконатися, що доступні дані є достатньо точними для забезпечення надійних результатів.

Ще однією задачею є проєктування архітектури систем великих даних. Такі системи мають бути адаптовані до конкретних потреб організації, що вимагає від ІТ-команд та розробників програмного забезпечення самостійного підбору та впровадження відповідного набору інструментів серед широкого спектра доступних технологій.

Процес обробки великих даних у середовищі IoT проходить через чотири основні етапи. Спершу відбувається збір значного обсягу неструктурованих даних, що надходять від IoT-пристроїв і характеризуються високою швидкістю надходження та різноманітністю. Далі ці дані зберігаються у розподілених базах даних, організованих у відповідних файлових структурах. Після збереження здійснюється їхній аналіз за допомогою спеціалізованих інструментів, а завершальним етапом є формування аналітичних звітів і візуалізація результатів аналізу.

Схематичне зображення процесу обробки великих даних в Інтернеті речей наведено на рисунку 2.2. А на рисунку 2.3 зображено динаміку зміни кількості підключених IoT-пристроїв в Україні та деяких сусідніх країнах.

Оскільки IoT та великі дані дають змогу здійснювати дії на запит і в реальному часі, зростає актуальність розгортання цих технологій. У цьому контексті периферійні (граничні) обчислення стають дедалі більш популярними.

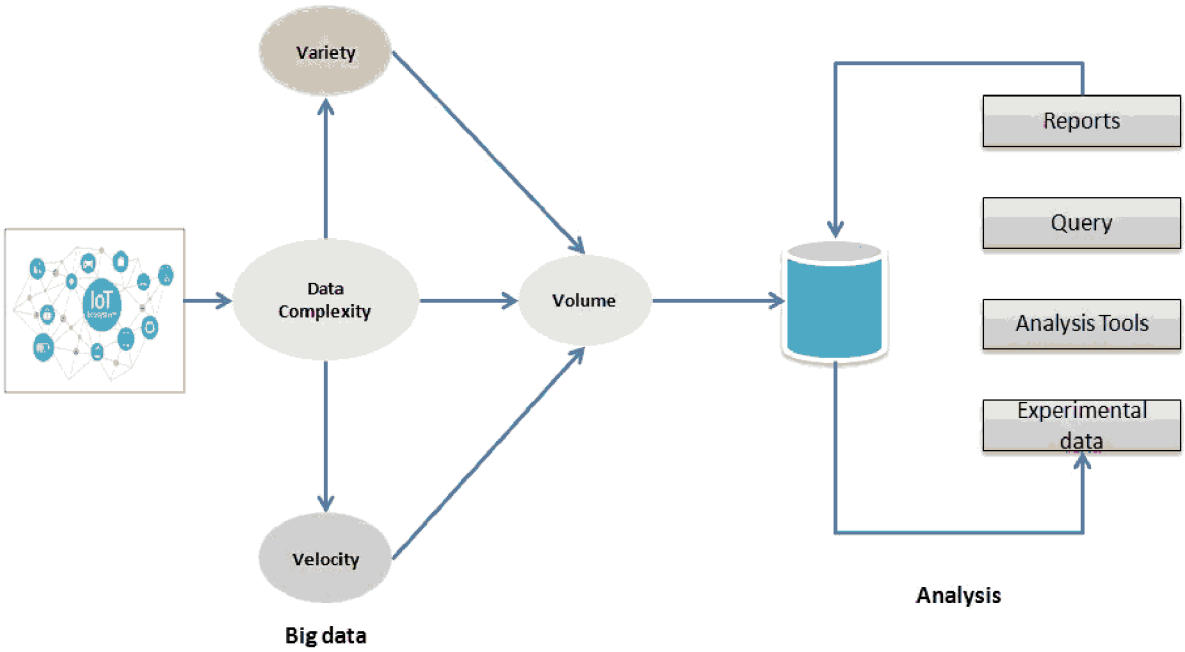

Рисунок 2.2 – Процес обробки Big Data у середовищі IoT

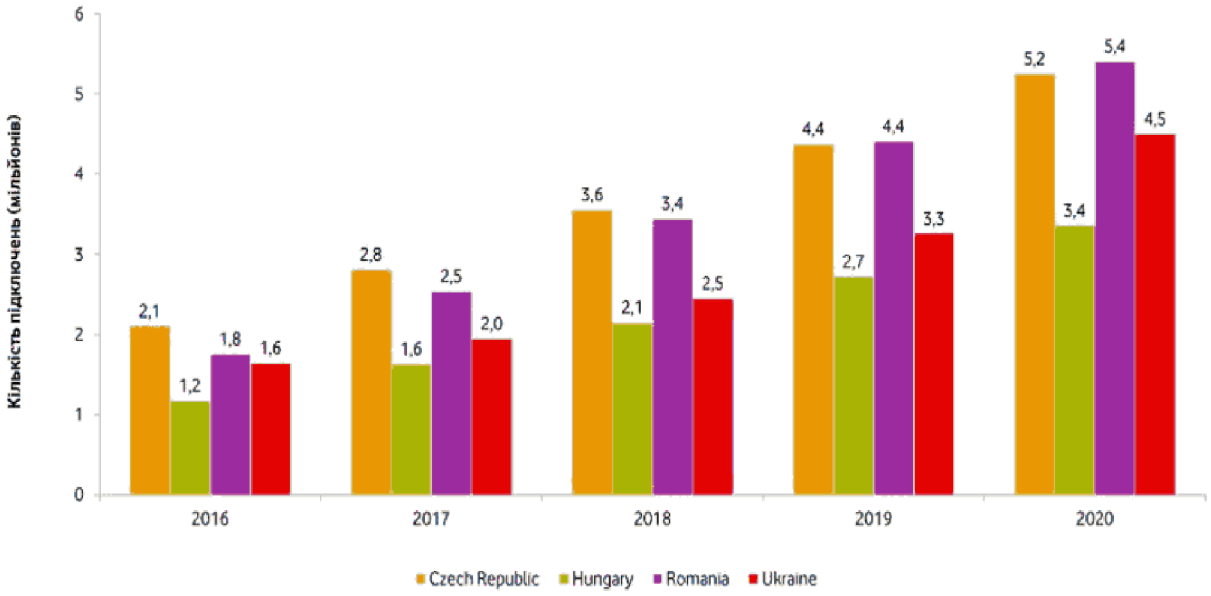

Рисунок 2.3 – Динаміка зростання кількості IoT-пристроїв

Тому інструменти, створені для роботи з великими даними та аналітикою, є корисними для обробки великого потоку даних, що надходять у режимі реального часу від пристроїв IoT. Розробники, які спеціалізуються на IoT, створюють платформи, програмне забезпечення та застосунки, які підприємства й організації можуть використовувати для керування своїми пристроями та даними, що ними генеруються.

Розвиток мікроелектроніки відкрив можливості створення компактних, енергоефективних сенсорних пристроїв, що привело до широкого впровадження бездротових сенсорних мереж (WSN). Вони забезпечують постійний збір і передачу даних про стан середовища чи об'єкта спостереження, що є основою для сучасних IoT-рішень, орієнтованих на обробку великих даних. Перехід на бездротову передачу даних значно підвищив гнучкість і масштабованість таких мереж, а також дозволив розгортати їх у важкодоступних або змінних умовах.

Типова бездротова сенсорна мережа складається з численних вузлів, які здатні самостійно виявляти зміни середовища, обробляти локальні дані та передавати результати на шлюз або сервер. Передача інформації здійснюється невеликими пакетами з підтвердженням доставки, що гарантує надійність обміну навіть за наявності перешкод.

Функціонування таких мереж залежить від обраної топології. Найчастіше застосовуються ієрархічні (кластерні) або однорангові архітектури. У першому випадку мережею керують спеціальні координатори, що збирають дані від сенсорних вузлів і передають їх далі. У другому – всі вузли мають однакові можливості, здійснюючи обмін даними без централізованого керування.

На рисунку 2.4 показано узагальнену функціональну модель WSN, яка включає сенсорні вузли, модулі передачі, елементи зберігання та обробки даних.

Особливу роль у мережі відіграють шлюзи. Вони виступають посередниками між вузлами збору даних та хмарною інфраструктурою, виконують первинну фільтрацію та агрегацію, а також реалізують базовий захист інформації. У разі спрацювання певного датчика, наприклад, пожежного, саме шлюз ініціює реакцію – запуск локальної тривоги або відправлення повідомлення у відповідну службу.

Сенсорні мережі можуть будуватись як на основі вже існуючих телекомунікаційних інфраструктур (з базовими станціями), так і в

автономному режимі — без централізованого керування. У першому випадку пристрої передають дані через комунікаційні мережі на обробку в центрах обробки даних, у другому — обмін інформацією відбувається безпосередньо між вузлами, що дозволяє працювати навіть за відсутності зовнішніх каналів зв’язку.

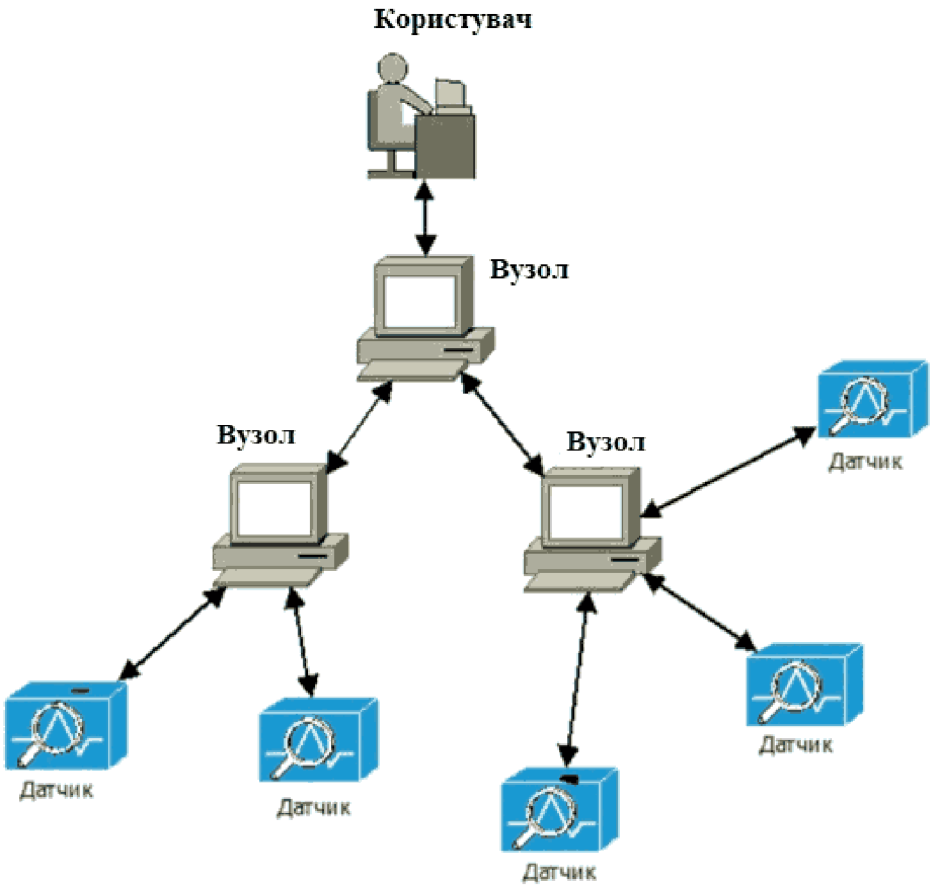

Рисунок 2.4 – Модель функціонування сенсорної мережі з Big Data

Кожен із варіантів має свої переваги. Централізована архітектура зручна для контролю і масштабування, проте залежить від інфраструктури. Одноранговi рішення забезпечують більшу автономність, але потребують складніших алгоритмів маршрутизації. Обидва підходи застосовуються у практиці проєктування WSN і можуть поєднуватися для досягнення балансу між стабільністю, автономністю та ефективністю. На рисунку 2.5 наведено приклади організації бездротової сенсорної мережі з урахуванням підтримки Big Data-аналітики.

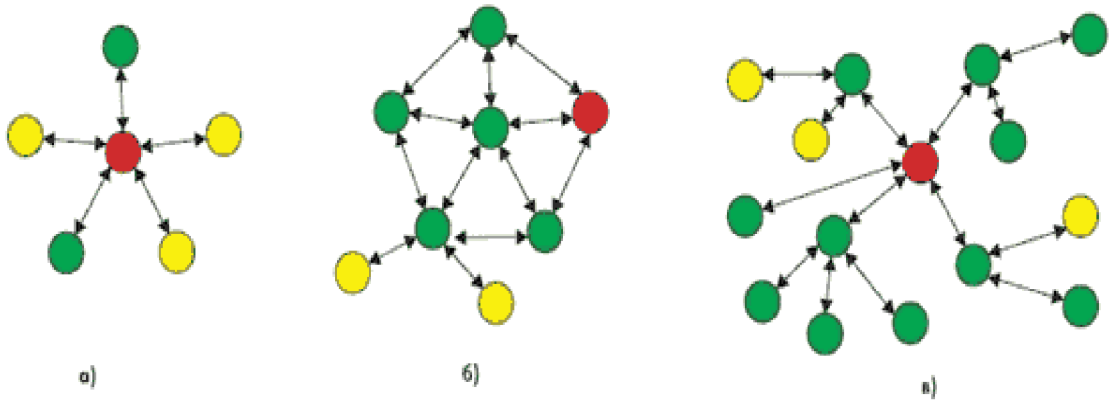

Рисунок 2.5 – Приклади організації сенсорних мереж з підтримкою великих даних

Широкі можливості бездротових сенсорних мереж дозволяють ефективно розгортати їх у побуті, промисловості, охороні здоров'я, енергетиці, а також у системах моніторингу навколишнього середовища. Завдяки низькому енергоспоживанню, малим розмірам і можливості самоконфігурації, такі мережі не потребують складного монтажу, а обслуговування зводиться до мінімуму.

Незважаючи на численні переваги, зростаючий обсяг зібраної інформації створює нові виклики. Частина даних є дубльованою або неінформативною, що вимагає впровадження механізмів фільтрації, стискання й оптимізації передавання. Особливо це актуально в реальному часі, коли затримки або перевантаження можуть впливати на швидкість реагування.

У деяких прикладних задачах, зокрема в медичних або енергетичних системах, обсяг і швидкість обміну даними постійно зростають. Для обробки таких потоків інформації традиційні підходи вже не є ефективними, тому все ширше застосовуються гібридні архітектури, які поєднують сенсорні мережі, локальні шлюзи та хмарні обчислення з використанням технологій Big Data.

2.2 Порівняльний аналіз технологій зв'язку для IoT-мереж

У сучасних умовах побудови високопродуктивних сенсорних мереж особливого значення набувають технології передачі даних, що забезпечують низьке енергоспоживання, високу дальність зв'язку та масштабованість. До таких технологій належать LoRa, SIGFOX, NB-IoT і Weightless-P. У цьому підрозділі наведено порівняльний аналіз їх архітектурних особливостей, технічних параметрів і практичного застосування.

LoRa (Long Range) — це технологія радіозв'язку для мереж LPWAN, заснована на модуляції Chirp Spread Spectrum (CSS), яка забезпечує високу завадостійкість. Основними перевагами LoRa є гнучке налаштування швидкості передавання, великий радіус дії (до 15–45 км на відкритій місцевості) та можливість використання трьох класів пристроїв: клас A (асинхронне передавання), клас B (синхронізовані часові вікна) і клас C (максимальна доступність до мережі).

На рисунку 2.6 зображено категоризацію пристроїв у мережі LoRa, що дозволяє реалізовувати як періодичну передачу невеликих пакетів, так і постійний моніторинг подій у реальному часі.

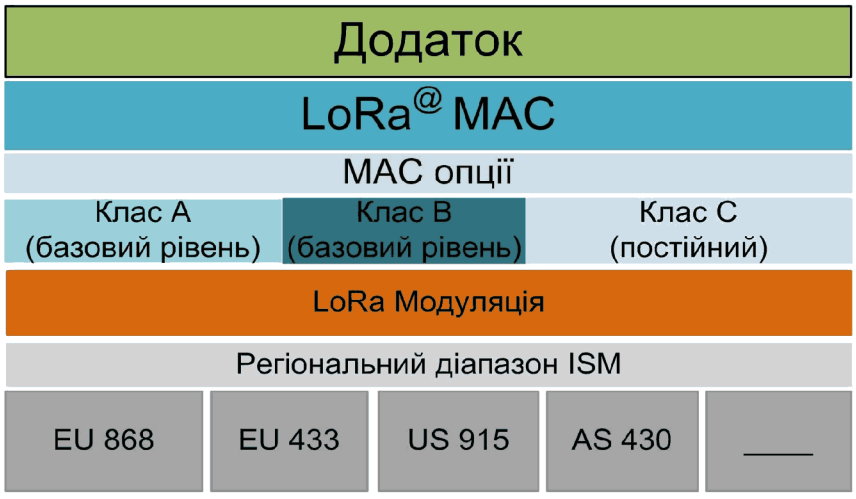

Рисунок 2.6 – Категоризація пристроїв у мережах LoRa

SIGFOX — це хмароорієнтована платформа для малопотужного зв'язку, яка використовує ультравузькосмугову модуляцію (UNB). SIGFOX дозволяє передавати дані на великі відстані за допомогою дуже простих і недорогих пристроїв. Основна перевага — мінімальне енергоспоживання при передаванні малих пакетів даних, що робить цю технологію ідеальною для моніторингових рішень. Топологія мережі SIGFOX має зіркоподібну архітектуру, де кожен пристрій зв'язується з кількома базовими станціями, що забезпечує надійність і гнучкість мережі.

NB-IoT (Narrowband IoT) — це стільникова технологія, розроблена на базі стандарту LTE. Вона використовує вузьку смугу пропускання (180–200 кГц) і забезпечує глибоке покриття, високу щільність підключень та до 10 років автономної роботи. Технологія підтримується мобільними операторами, що забезпечує легку інтеграцію в існуючу інфраструктуру. Цей підхід ідеальний для «розумних» лічильників, охоронних систем, тощо.

Weightless-P — це відкритий стандарт для LPWAN, який дозволяє двосторонній зв'язок, підтримує адаптивну модуляцію та працює в неліцензованих діапазонах. Його перевага — висока масштабованість: одна базова станція може обслуговувати велику кількість кінцевих пристроїв з мінімальним споживанням енергії. На рисунку 2.7 представлено архітектуру протоколу LoRaWAN, що демонструє підхід до організації передачі даних, аналогічний до Weightless.

Для системного аналізу виконано узагальнення ключових характеристик у таблиці 2.1. У ній наведено порівняння за критеріями: частотний діапазон, смуга пропускання, тип модуляції, швидкість передавання, рівень безпеки, автономність пристроїв і дальність дії. Такий аналіз дозволяє зробити висновки щодо доцільності застосування тієї чи іншої технології залежно від вимог до мережі. Наприклад, LoRa і Weightless-P підходять для приватних розгортань з високою гнучкістю, SIGFOX – для простих автономних датчиків, а NB-IoT – для комплексних систем, що потребують централізованого управління й високого рівня безпеки.

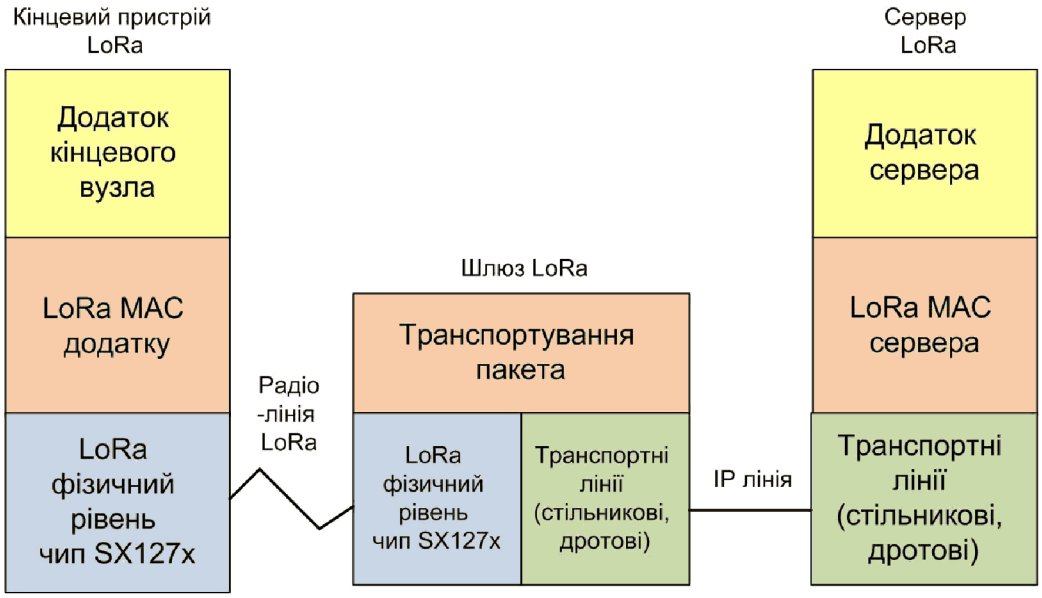

Рисунок 2.7 – Організація архітектури відкритого протоколу LoRaWAN

Таблиця 2.1 – Порівняльна характеристика технологій побудови високопродуктивних сенсорних IoT-мереж із Big Data

Характеристика	**LoRa**	**SIGFOX**	**NB-IoT**	**Weightless-P**
Тип модуляції	Chirp Spread Spectrum (CSS)	ультравузькосмугова	OFDMA / DSSS	FDMA / TDMA
Діапазон частот	ISM: 433 / 868 / 915 МГц	ISM: 868 / 915 МГц	ліцензований: 700–900 МГц	ISM: 169 / 433 / 470 / 780 / 868 / 915 / 923 МГц
Ширина смуги	до 500 кГц	100 кГц	200 кГц	12,5 кГц
Швидкість передавання даних	0,3–50 кбіт/с	До 100 кбіт/с	UL: 1–144, DL: 1–200 кбіт/с	0,2–100 кбіт/с (адаптивна)
Тип зв'язку	двосторонній	односторонній (зворотній канал обмежений)	двосторонній	двосторонній
Дальність дії	до 2,5 км у місті, до 45 км поза містом	до 10 км у місті, до 50 км поза містом	до 15 км	до 2 км у місті
Автономність пристроїв	>10 років	до 10 років (залежно від режиму)	до 10 років	3–5 років
Безпека	AES-64 / 128 біт	AES із HMAC	SIM-рівень захисту (3GPP стандарт)	AES-128 / 256
Організації підтримки	LoRa Alliance, Semtech, Cisco, IBM, Actility	SIGFOX, Samsung	3GPP, Huawei, Nokia, Ericsson, Intel	Ubiik, Weightless SIG

2.3 Методи штучного інтелекту в задачах IoT

У сучасних IoT-системах важливу роль відіграють інтелектуальні алгоритми, здатні адаптивно обробляти великі обсяги даних, виявляти приховані закономірності та робити точні прогнози. Серед таких підходів особливе місце посідають штучні нейронні мережі (ШНМ), які широко застосовуються в задачах класифікації, регресії, виявлення аномалій та прогнозування параметрів середовища.

Нейромережеві моделі дозволяють значно підвищити ефективність аналітики в IoT-середовищах, зокрема — в умовах високої динаміки вхідних даних і великої кількості параметрів. Їх здатність до навчання, узагальнення і самокорекції робить ці методи потужним інструментом обробки інформації, що надходить від сенсорних пристроїв у режимі реального часу.

Далі розглянемо базові принципи функціонування нейронних мереж, їх переваги, обмеження та особливості побудови, що мають значення для побудови інтелектуальних IoT-рішень.

Кожного разу, коли дані завантажуються в нейронну мережу, алгоритм аналізує ці дані, пропускаючи їх через мережу та призначаючи вагові коефіцієнти вузлам у прихованих шарах, що впливає на результати на виході. Приклад структури нейронної мережі наведено на рисунку 2.8.

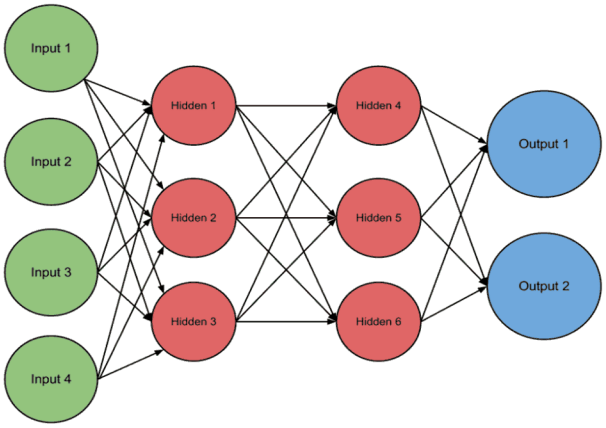

Рисунок 2.8 – Структурна схема штучної нейронної мережі

Наприклад, передбачення на основі нейронних мереж відрізняються від лінійної регресії (яка також є інструментом прогнозування, що застосовується в багатьох галузях, де потрібен аналіз), оскільки модель лінійної регресії є значно простішою. Розглянемо нейронну мережу лише з одним вхідним вузлом, одним вихідним вузлом і одним прихованим шаром.

Якщо видалити приховані шари з нейронної мережі, залишаться лише вхідні та вихідні вузли. У такому випадку мережа намагається передбачити вихідне значення, використовуючи лише вхідні параметри. Саме так працюють моделі лінійної та логістичної регресії, які також виконують прогнозування.

Приховані шари роблять нейронні мережі набагато потужнішими й точнішими, ніж традиційні інструменти прогнозування, оскільки вони «навчаються» аналогічно до людського мозку — запам'ятовують закономірності у даних і використовують цю інформацію в наступних ітераціях навчання.

Висока точність нейронних мереж викликає закономірне питання: чому їх не використовують частіше? Як і очікується, нейронні мережі мають певні недоліки. Вони потребують значно більшої обчислювальної потужності порівняно з традиційними методами, що робить їх дорожчими у реалізації. Крім того, для ефективного навчання нейронним мережам потрібні великі обсяги даних, які не завжди є доступними.

Ще одним обмеженням є так звана природа «чорної скриньки»: ми можемо спостерігати вхідні дані та результати, однак не можемо точно інтерпретувати, як приймаються внутрішні рішення. Це ускладнює налаштування алгоритмів і прогнозування поведінки мережі в нових ситуаціях. Втім, для завдань прогнозування енергоефективності систем IoT ці недоліки не є критичними.

Ключовою особливістю нейронних мереж є ітеративний процес навчання, під час якого записи (рядки) подаються в мережу по черзі, і вагові коефіцієнти, пов'язані з вхідними значеннями, коригуються кожного разу.

Після обробки всіх прикладів процес зазвичай повторюється. Упродовж цієї фази навчання мережа навчається, налаштовуючи ваги так, щоб правильно передбачити мітку класу для кожного вхідного зразка.

До основних переваг нейронних мереж належать висока стійкість до зашумлених даних і здатність класифікувати шаблони, з якими мережа не була навчена раніше. Після створення архітектури мережі її можна навчити для розв'язання конкретного завдання.

На початку процесу навчання початкові ваги задаються випадковим чином, після чого запускається процес навчання. Мережа обробляє кожен запис із навчальної вибірки, використовуючи ваги та функції в прихованих шарах, і порівнює отримані вихідні значення з очікуваними. Помилка розповсюджується назад мережею, змушуючи її коригувати ваги під час обробки наступного запису. Цей процес повторюється багаторазово, а вагові коефіцієнти поступово уточнюються.

Під час навчання один і той самий набір даних може опрацьовуватися багаторазово, що дозволяє досягти точнішого налаштування ваг з'єднань.

Важливими параметрами є кількість шарів і кількість обчислювальних елементів (нейронів) у кожному шарі. У випадку прямого з'єднання (feedforward) з алгоритмом зворотного поширення помилки ці параметри визначають топологію мережі та вважаються найменш формалізованими — їх вибір значною мірою залежить від досвіду і підходу розробника, і тому часто називається «мистецтвом проєктування мережі».

З часом сформувалося лише три загальні правила, яких дотримуються більшість дослідників та інженерів, що застосовують цю архітектуру до вирішення практичних задач.

Правило 1: зі зростанням складності взаємозв'язку між вхідними даними та бажаним результатом має зростати і кількість елементів обробки у прихованому шарі.

Правило 2: якщо модельована задача може бути поділена на кілька послідовних етапів, може виникнути потреба у використанні додаткових

прихованих шарів. Якщо ж процес не піддається такому поділу, додаткові рівні можуть призвести лише до запам’ятовування навчального набору, а не до формування узагальненого розв’язку.

Правило 3: обсяг доступних навчальних даних встановлює верхню межу кількості елементів обробки в прихованому шарі. Щоб її визначити, слід розділити кількість прикладів у навчальному наборі на суму кількості вузлів у вхідному та вихідному шарах мережі. Отримане значення додатково ділиться на масштабний коефіцієнт у межах від п’яти до десяти. Для даних із низьким рівнем шуму рекомендується використовувати більший коефіцієнт масштабування. Якщо використовується занадто багато штучних нейронів, мережа схильна до перенавчання — вона запам’ятовує навчальні дані, але втрачає здатність до узагальнення, що робить її непридатною для роботи з новими наборами даних.

Алгоритм нейронної мережі може бути використаний для побудови моделі, яка забезпечує добру точність прогнозування на нових даних. Хоча можна аналізувати статистичні показники та матрицю помилок поточної моделі, це не дає гарантії, що ця модель є найкращою з усіх можливих.

Методи ансамблю дозволяють об'єднувати декілька слабких нейронних мереж у єдину сильну модель. Ці методи працюють шляхом створення кількох гетерогенних мереж на основі різних підмножин вихідного набору даних з подальшим об'єднанням їхніх результатів. Вихідні дані можуть комбінуватися різними способами — наприклад, методом голосування більшості для задач класифікації або методом усереднення для задач регресії.

РОЗДІЛ 3
РОЗРОБКА, МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ЕНЕРГОЕФЕКТИВНОСТІ IOT-СИСТЕМИ

3.1 Проєктування архітектури та математична формалізація IoT-системи

На рисунку 3.1 зображено базову структуру системи роботи з великими даними на основі WSN, яка слугує основою архітектури такої системи.

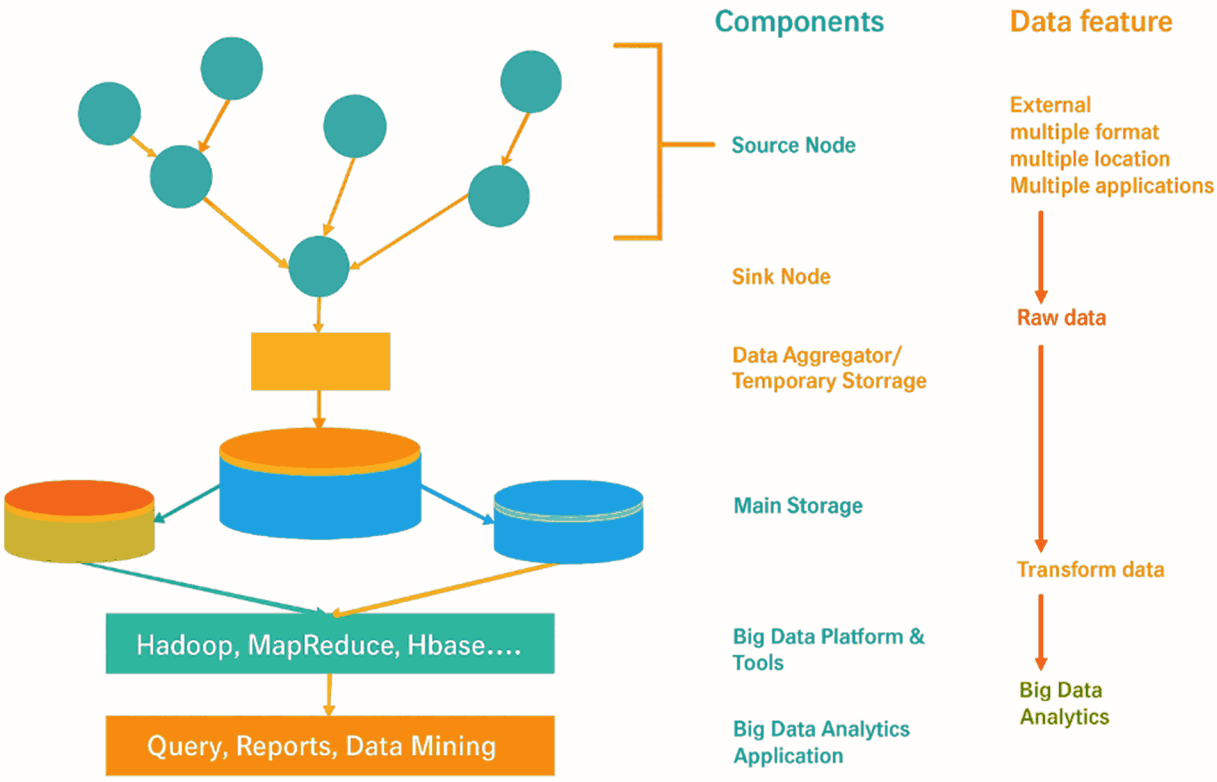

Рисунок 3.1 – Базова архітектура IoT-рішення

Як показано на рисунку 3.1, приймальний вузол збирає дані з сенсорних вузлів, а потім передає їх до тимчасового сховища для подальшого агрегування. Після завершення цього етапу зведеними даними можна

керувати через інфраструктуру великих даних із використанням основного сховища. Трансформовані дані обробляються платформами та застосунками для роботи з великими даними.

Швидке зростання обсягів даних призвело до зростання попиту на високопродуктивні та енергоефективні системи NB-IoT. Це вимагає постійного моніторингу та інтелектуальної обробки даних вимірювань і спостережень – завдань, що виконуються за допомогою рішень IoT.

Інформація, отримана шляхом вимірювань певних параметрів, слугує вхідними даними для спеціалізованої системи керування технологічним процесом. Для збору та комплексної обробки даних інтеграція Інтернету речей і бездротових високопродуктивних сенсорних мереж (WSN) у нові архітектури може значно підвищити ефективність, зокрема сприяти збільшенню врожайності.

Для такої системи недостатньо лише аналізу й обробки звичайних даних — потрібні великі обсяги даних. Подібна система моделюється як чітко визначене агентно-орієнтоване рішення з використанням датчиків. Хоча індивідуальний внесок IoT, великих даних і WSN у підвищення ефективності є доведеним і значущим, очікується, що подальша інтеграція цих компонентів у структуру IoT значно покращить рішення для моніторингу, моделювання виробництва, прогнозування та прийняття рішень.

WSN виконують кілька функцій: збір даних про різні параметри (наприклад, температуру, вологість, рівень сонячного випромінювання, концентрацію поживних речовин), розподілену обробку даних із досягненням консенсусу (якщо це передбачено), встановлення зв’язків між пов’язаними даними та їх зберігання, об’єднання даних нижчого рівня та передавання їх до центральних вузлів.

Big Data та IoT не лише взаємодоповнюють, а й взаємовпливають. Чим активніше розвивається Інтернет речей, тим вищим стає попит на можливості аналізу великих даних. Наприклад, у міру стрімкого зростання обсягу даних,

які генерує IoT, традиційні технології зберігання вже не справляються з навантаженням. Для обробки таких зростаючих обсягів потрібні сучасні й інноваційні рішення, що, у свою чергу, сприяє модернізації інфраструктури зберігання великих даних у межах організацій. Це підтверджує, що використання лише традиційних підходів до моніторингу, енергоменеджменту та прийняття рішень уже не є ефективним.

Як і в багатьох інших випадках, зокрема при моніторингу великих територій, датчики об'єднуються у високопродуктивні сенсорні мережі для зв'язку або локальної обробки даних. Така WSN включає вимірювальні вузли (датчики) та вузли збору, обробки й передавання інформації (приймачі або головні вузли кластера).

У подібних завданнях постає проблема дослідження та оптимізації параметрів енергоефективності системи. Це зумовлено тим, що для таких задач, як моніторинг певної території або енергоменеджмент, кінцеві пристрої IoT мають працювати автономно тривалий час. Тому питання дослідження енергоефективності цих пристроїв є надзвичайно актуальним.

Усе вищезазначене підтверджує, що використання великих даних та забезпечення високої енергоефективності рішень IoT є необхідною умовою сучасного технічного розвитку.

Розглянемо математичну модель IoT-рішення. Наведено спрощену схему взаємодії компонентів. Нехай досліджувана IoT-система складається з N входів та M виходів, загалом $P = N + M$ функціональних елементів. У цьому випадку N і M є змінними параметрами, які можна подати у вигляді математичного виразу:

$$Nt = f(SRt) \leq P, \tag{3.1}$$

$$Mt = f(SRt, PRt, Nt) \leq P, \tag{3.2}$$

де Nt – кількість входів;

Mt – кількість виходів;

P – сумарна кількість виводів;

SRt – масив поточних даних.

Функції (3.1) і (3.2) для кожного окремого рішення можна описати шляхом визначення станів, які може приймати рішення:

$$Pri = \{\text{двонаправлений, лише вхід, лише вихід, }\} \quad (3.3)$$

Графічну математичну модель системи IoT показано на рисунку 3.2. Блоки *PR*1–*PR*B у цій моделі представляють собою кінцеві пристрої IoT, для яких особливо важливими є зниження енергоспоживання та збільшення часу автономної роботи.

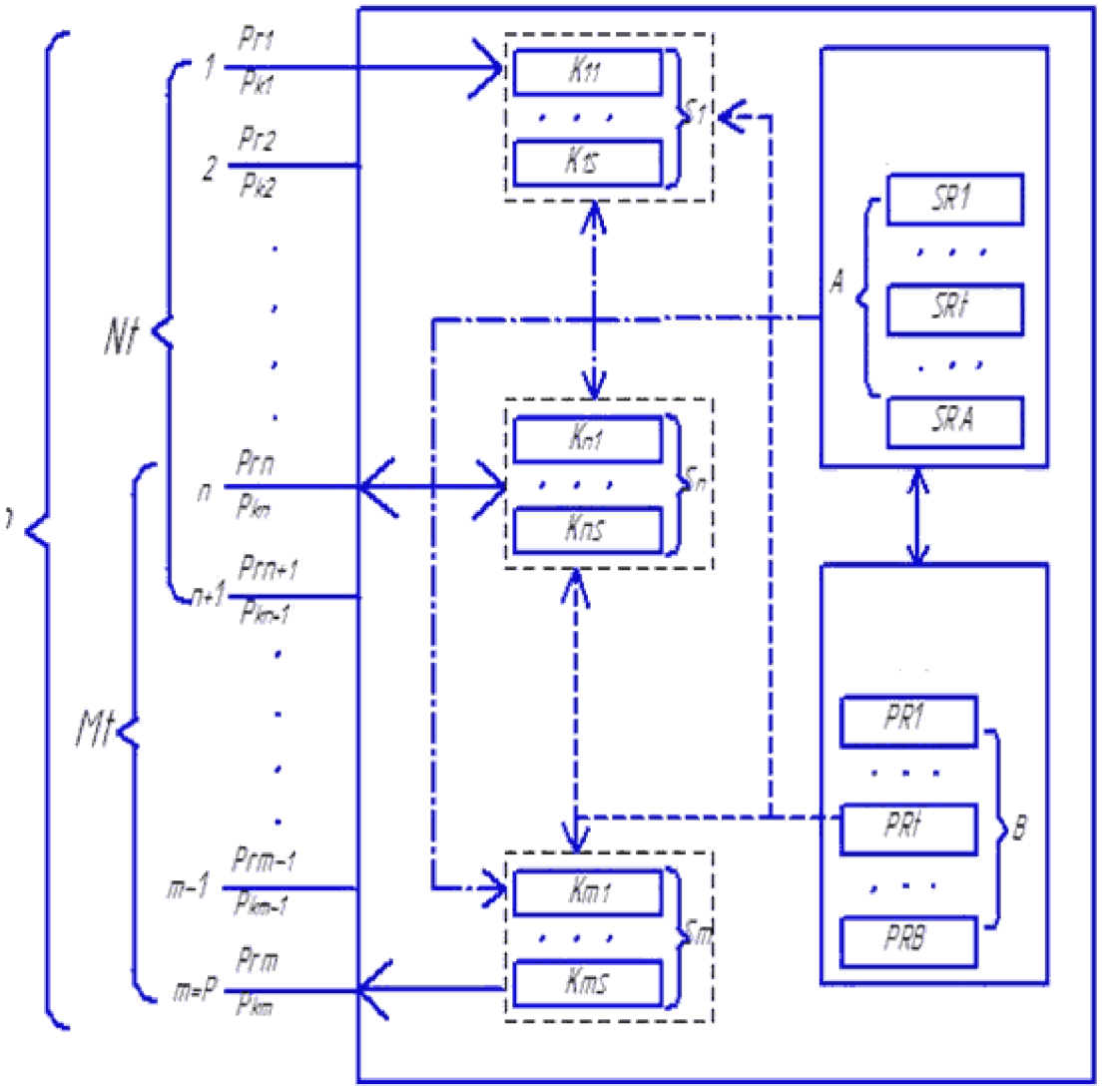

Рисунок 3.2 – Візуалізація IoT-моделі у вигляді графічної схеми

3.2 Аналіз енергоефективності та моделювання підключення IoT-пристроїв

Кожен пристрій, підключений до мережі, повинен пройти процедуру встановлення з'єднання між базовою станцією оператора та кінцевим пристроєм — незалежно від того, чи це смартфон, чи датчик. Цей процес передбачає аутентифікацію та називається процедурою довільного доступу (рис. 3.3).

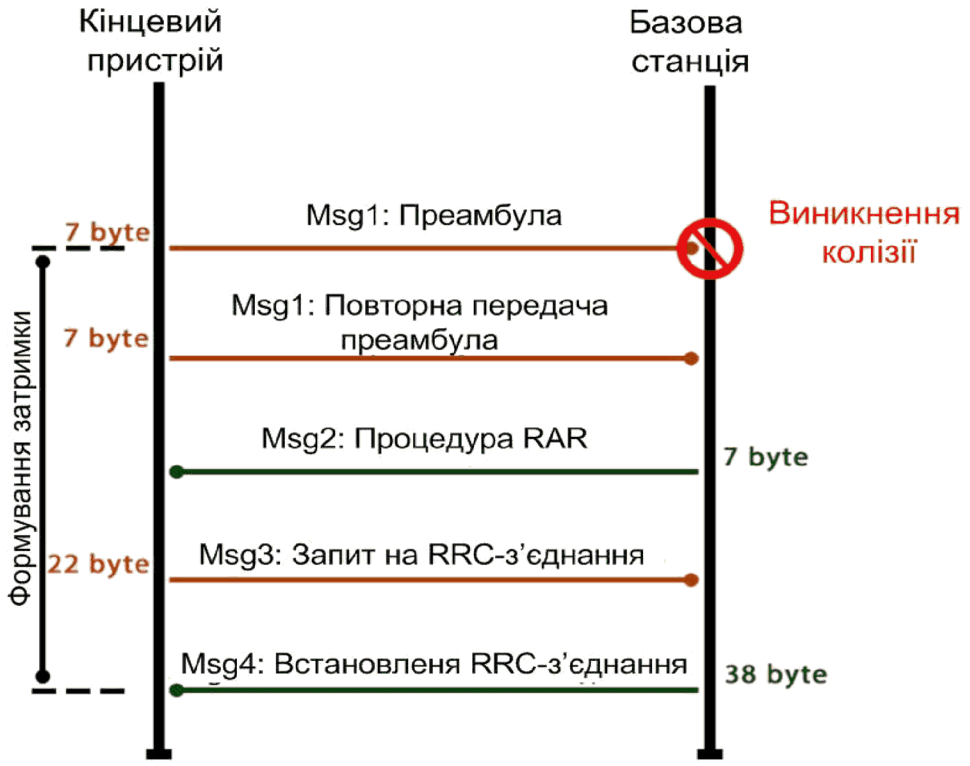

Рисунок 3.3 – Механізми реалізації процедури випадкового доступу

Спочатку термінальний пристрій надсилає преамбулу (Msg1) до станції через фізичний канал довільного доступу (PRACH), щоб розпочати процес підключення. Преамбула вибирається випадковим чином із 64 доступних послідовностей. Саме ця особливість і становить основну проблему дослідження. Зі збільшенням кількості термінальних пристроїв, які підключаються до мережі одночасно, можуть виникати конфлікти під час встановлення з'єднання, що призводить до затримок у каналі зв'язку.

Якщо преамбулу прийнято коректно, станція повинна підтвердити її, надіславши відповідь RAR (Random Access Response) (Msg2) у відповідному часовому вікні для приймання преамбули пристроєм UE. Після успішного отримання перших двох повідомлень термінальний пристрій надсилає повідомлення RRC через фізичний спільний канал висхідної лінії зв'язку (PUSCH), використовуючи ресурси, надані в Msg2, щоб ініціювати процедуру встановлення з'єднання (Msg3). Коли UE отримує повідомлення про встановлення з'єднання RRC (Msg4) від eNB, процес завершено успішно.

Особливістю передавання інформації термінальними пристроями IoT є її періодичність, тобто пристрої не постійно перебувають у мережі, а підключаються лише тоді, коли накопичену інформацію потрібно передати на сервер обробки. Враховуючи характеристики описаного процесу з'єднання, а також специфіку передавання інформації термінальними пристроями IoT, можна зробити висновок, що обмежена кількість преамбул у процесі з'єднання є «вузьким місцем». Якщо два пристрої починають підключення до мережі, використовуючи одну й ту саму преамбулу одночасно, один із них буде відхилений мережею та повторюватиме спроби встановлення з'єднання доти, доки не завершиться таймер або процедура не завершиться невдало.

Ця проблема може бути не критичною за невеликої кількості пристроїв закріплених за базовою станцією. Проте, зі зростанням кількості термінальних пристроїв, що є характерним для розвитку концепції Інтернету речей, вона набуває значної актуальності. У разі надзвичайної ситуації, коли спрацьовує група датчиків, можлива масова колізія, що спричиняє серйозні затримки або перевантаження мережі.

Ще одним важливим фактором роботи термінальних пристроїв IoT є їх автономність, тобто здатність тривалий час працювати без втручання людини. У межах цього дослідження запропоновано модель споживання енергії обчислювальним пристроєм. Вона дозволяє передбачити тривалість автономної роботи пристрою з урахуванням описаних затримок у зв'язку.

Розрахунок затримки встановлення з'єднання та ймовірності колізій ґрунтується на методиці з [9]. Вхідними даними для обчислень є стандартизовані параметри сигналу згідно з вимогами стандартів IoT. Модель також дає змогу розрахувати параметри за критеріями BSM. Основні вихідні дані впорядковано відповідно до специфікацій, як показано в таблиці 3.1.

Таблиця 3.1 – Початкові дані для математичного моделювання

Символ	Параметр	Величина
-	Ширина смуги	200 кГц
s	Повне число преамбул	64
L_1	Максимальне число передач преамбули	10
-	Розмір вікна очікування преамбули	5 мс
-	Таймер ContentionResolution	(у 48мс)
W_{max}	Індикатор Backoff	(у 200 м)
π_3	Імовірність успішної доставки Msg3	0.9
π_4	Імовірність успішної доставки Msg4	0.9
L_3	Максимальна кількість повідомлень HARQ T_x для повідомлень Msg3 та Msg4	5
M	Кількість кінцевих пристроїв у мережі	100/150/200
b	Частота PRACH	5 мс
K	Вікно очікування RAR	5 мс
K_1	Час передачі преамбули	1 мс
K_0	Час обробки преамбули на eNB	2 мс
t_{pr}	Час обробки перед передачею Msg3	5 мс
t_x	Час обробки Msg3 і прийом Msg4	6 мс

Під час обчислень дуже важливим є так званий індекс конфігурації PRACH — він визначає, у скількох часових інтервалах (підкадрах) пристрій може спробувати надіслати початковий сигнал (преамбулу), а також як довго цей сигнал триватиме. Інший важливий параметр — таймер ContentionResolution — визначає, скільки часу пристрій чекатиме на відповідь після надсилання наступного повідомлення Msg3, перш ніж система вирішить, що з'єднання не встановлено.

Коли пристрій має дані для надсилання, він намагається вийти на зв’язок через спеціальний канал PRACH. Але оскільки багато пристроїв можуть робити це одночасно, між ними виникає конкуренція. Після надсилання певної кількості підкадрів (K_0) пристрій робить паузу, щоб уникнути перетину з відповіддю Msg2. У цей час формується так зване вікно відповіді — часовий проміжок, протягом якого базова станція надсилає Msg2. Якщо пристрій не отримає Msg2 (через перешкоди чи конфлікти з іншими пристроями), він запускає процедуру з'єднання заново, але вже після випадкової затримки, яка визначається таймером W.

Коли пристрій все ж отримує відповідь RAR, він переходить до наступного кроку — готує та надсилає повідомлення Msg3 за час t_{pr}, а потім очікує певний проміжок часу t_{tx}, щоб передати Msg4. Проте доставка цих повідомлень не гарантована — кожне має свою ймовірність успішної передачі (π_3 і π_4). Якщо Msg3 не доставлено з першої спроби, пристрій може пробувати ще кілька разів, максимум — L_3 разів.

Загальна затримка встановлення з’єднання розраховується як сума затримок на етапах Msg1, Msg2 та RRC Msg3.

$$E[\tau] = E\left[\tau^{(1)}\right] + E[\tau^{(2)}], \tag{3.4}$$

де $E[\tau^{(1)}]$ – це час очікування від активації кінцевого пристрою до завершення процесу надсилання коду преамбули Msgl і відповіді Msg2;

$E[\tau^{(2)}]$ є часом очікування для встановлення з’єднання RRC.

Очікувана затримка Msg3/Msg4 розраховується за формулою:

$$E\left[\tau^{(2)}\right] = t_{pr} + t_{tx} \cdot n_3, \tag{3.5}$$

де n_3 – середня кількість передач між Msg3 та Msg4 і підраховується:

$$\overline{n_3} = \pi_{tx} \sum_{n=1}^{L_3} n(1-\pi_{tx})^{n-1} = \frac{1}{\pi_{tx}}[1-(1-\pi_{tx})^{L_3}]. \quad (3.6)$$

Для розрахунку затримки Msg1/Msg2 можна знехтувати зіткненнями при створенні з'єднання, тоді:

$$E[\tau^{(1)}] = c_1(K_1 + K_0 + K + \overline{w}), \quad (3.7)$$

де w – середнє очікування повторної відправки преамбули.

Для того, щоб врахувати при розрахунку вплив колізій на затримку слід використати формулу:

$$E[\tau^{(1)}] = \sum_{j=1}^{M} \theta_j \frac{1}{\pi+\mu_j} \quad (3.8)$$

де θ – ймовірність перебування пристрою у режимі зіткнення:

$$\theta_j = \frac{(M-1)!}{(j-1)!(M-1)!}\rho^{j-1}(1-\rho)^{M-j} \quad (3.9)$$

Цей алгоритм розрахунку дозволяє визначити середній час пересилання інформації пристроєм, що перебуває в різних станах. Це дає змогу коректно обчислити його енергоспоживання.

Для оцінки енергоспоживання кінцевого пристрою слід зосередитися на випадках, коли відбуваються колізії. Результати чисельного аналізу затримки підключення наведено в таблиці 3.2.

Отримані дані свідчать про те, що зі збільшенням кількості пристроїв у мережі зростає ймовірність колізій зв’язку, а отже, збільшується затримка з’єднання. Кінцевий пристрій (наприклад, датчик чи смартфон) може перебувати у двох основних станах:

- RRC_IDLE – пристрій не використовує мережеві ресурси і споживає мінімум енергії, оскільки приймач здебільшого вимкнений;
- RRC_CONNECTED – пристрій отримує ресурси для передачі даних.

Для продовження автономної роботи пристрої IoT часто використовують режим енергозбереження (PSM). При його активації запускаються два таймери TAU. Перший визначає час перебування у стані RRC_IDLE або DRX, а другий відраховує загальний час у режимах DRX і PSM.

Таблиця 3.2 – Затримка сигналів Msg3 та Msg4 у системі

Параметр	Позначення	Значення		
Затримка Msg3/Msg4				
Середня кількість спроб передачі преамбули	n	1,233		
Середня затримка	$E[\tau^{(2)}]$, мс	12,398		
Очікувана затримка Msg1/Msg2 без колізій				
Середня затримка при передачі преамбули з першої спроби	$E[\tau^{(1)}$, спроба], мс	8,5		
Очікувана затримка Msg1/Msg2 з колізіями				
		Число пристроїв M2M		
		100	150	200
Ймовірність колізії	π_{kol}	0,0025%	0,006%	0,008%
Середнє число спроб передачі преамбули	n	1,026	1,035	1,038
Середня затримка	$E[\tau^{(2)}]$, мс	15,87	16,71	17,42

Після завершення передачі TAU-запиту мережа переводить пристрій у режим очікування, знову активуючи таймер. Цей період називають активним часом, коли пристрій ще можна досягнути. Після його завершення пристрій переходить у PSM, де споживання енергії мінімальне, і залишається там до закінчення другого таймера.

Аналіз енергоспоживання кінцевого обладнання буде проводитися в двох режимах: без використання режиму PSM (рисунок 3.4) та з його використанням (рис. 3.6). Спочатку необхідно визначити енергоспоживання пристрою (табл. 3.3). Необхідна автономність пристрою становить 24 години на добу. Розрахунки проведено за сценаріями, наведеними на рисунках 3.4 та 3.5, з урахуванням затримок, визначених у попередніх обчисленнях.

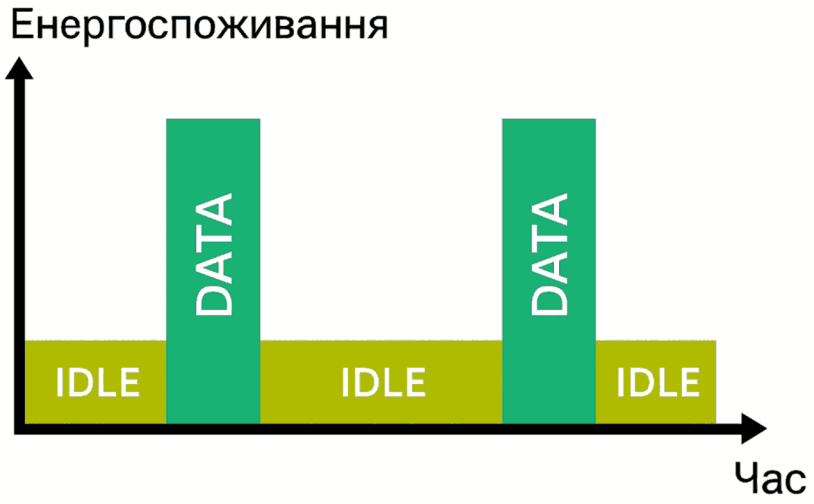

Рисунок 3.4 – Енергоспоживання кінцевих пристроїв без режиму PSM

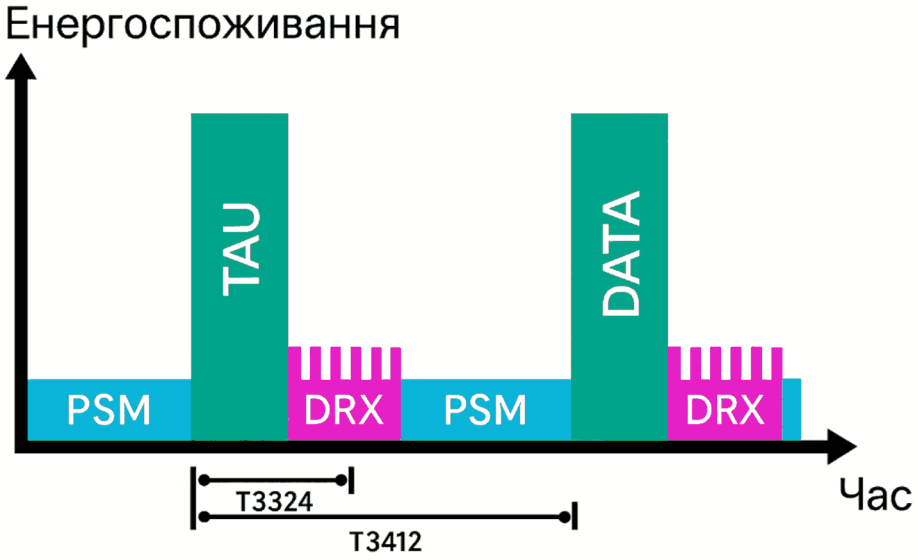

Рисунок 3.5 – Енергоспоживання кінцевих пристроїв з активованим режимом PSM

Таблиця 3.3 – Параметри енергоспоживання кінцевих пристроїв

Символ	Варіант	Значення
P_0	витрати потужності в режимі PSM	0 МВт
P_1	витрати потужності в режимі	0,05 мВт
P_2	витрати потужності на обробку та прийом	50 мвт
P_3	витрати потужності на передачу	50 мвт

Для оцінки енергоефективності роботи IoT-пристрою був розроблений алгоритм, що включає визначення відсотка часу, витраченого пристроєм у різних режимах роботи, розрахунок загальної потужності навантаження та постійного струму розряду. Основна мета – оцінити енергоспоживання пристрою протягом року та визначити термін його автономної служби.

Розрахунок починається з визначення частки часу, яку пристрій проводить у режимах передачі, прийому та очікування (DRX). З урахуванням параметрів передачі повідомлень Msg1/Msg3 та прийому Msg2/Msg4, обчислюються відповідні значення часу. Для кожного режиму виводяться окремі вирази, що враховують затримки, ймовірність передачі, кількість спроб доступу до мережі та інші параметри. Отримані частки часу підсумовуються, щоб отримати загальну частку часу активної роботи пристрою:

$$Q = q_3 + q_2 + q_1. \quad (3.10)$$

Далі визначається час, необхідний для передачі одного пакета даних. Він включає час передачі інформаційного блоку та сигналізаційних повідомлень, які супроводжують процес

$$T_{пакету} = T_{пер} + 2 \cdot T_{сиг}. \quad (3.11)$$

Знаючи цей час та потужність, споживану в режимах передачі та обробки, розраховується енергія, необхідна для однієї повної передачі:

$$\in_{пакету} = T_{пакету} \cdot P_2 + t_{обр} \cdot P_1. \quad (3.12)$$

До цієї енергії додається також споживання, пов’язане з іншими активними процесами (підключення до мережі, ініціалізація тощо), що в сукупності дає повну витрату енергії для однієї передачі.

$$\in_{full} [1 \text{ передача}] = \in_{пакету} + \in. \quad (3.13)$$

Річне енергоспоживання пристрою обчислюється на основі добового числа передач, множеного на кількість днів у році, а також часу перебування пристрою у стані очікування між передачами. Загальне енергоспоживання визначається як сума витрат у режимі передачі та режимі очікування (вставити ε_full[IDLE] = ε_full[рік] + ε_IDLE[рік]).

$$\in_{\text{full}} [IDLE] = \in_{\text{full}} [\text{рік}] + \in_{IDLE} [\text{рік}]. \quad (3.14)$$

Знаючи повне енергоспоживання за рік і ємність акумулятора пристрою, розраховується тривалість автономної роботи. У звичайному режимі очікування вона визначається за співвідношенням ємності до річного енергоспоживання

$$T_{\text{work}}[IDLE] = \frac{P_{bat}}{\in_{\text{full}}[IDLE]}. \quad (3.15)$$

Водночас у режимі PSM (Power Saving Mode), коли пристрій не здійснює передач і майже не споживає енергії, автономна робота подовжується

(вставити T_work[PSM] = P_bat / ε_full[PSM]).

$$T_{\text{work}}[\text{PSM}] = \frac{P_{bat}}{\in_{\text{full}}[\text{PSM}]}. \quad (3.16)$$

Таким чином, сформований підхід дозволяє комплексно оцінити витрати енергії на всі етапи роботи пристрою, що є критично важливим для планування терміну служби автономних IoT-систем.

На основі викладеної теорії проведемо чисельний аналіз часу автономної роботи термінального обладнання за таких умов. Для сигнальних повідомлень необхідно 59 байт для передавання по висхідній лінії зв'язку та 136 байт для отримання по низхідній лінії, без урахування 100 байт, які передаються по висхідній лінії зв'язку.

У розрахунках припускається, що всі кінцеві пристрої живляться від трьох батарей типу AAA (1,25 В) ємністю 1000 мА·год. Пристрій передає 100 байт інформації тричі на день. Результати наведено в таблиці 3.4.

На основі цієї таблиці можна зробити висновок, що зі збільшенням кількості пристроїв і обсягу даних у мережі енергоспоживання пристрою зростає лінійно, особливо тоді, коли розмір пакета досягає 1 Кбайт, а кількість пристроїв у мережі становить 150. На підставі отриманих результатів можна спрогнозувати орієнтовну тривалість автономної роботи кінцевих пристроїв за умов великого навантаження мережі.

Таблиця 3.4 – Чисельний аналіз автономної роботи пристроїв

Параметр	Число NB-IoT пристроїв	Розмір блоку даних		
		100 байт	500 байт	1 кбайт
Енергоспоживання на процедуру RA, Вт*с	100	$0,827*10^{-3}$		
	150	$0,828*10^{-3}$		
	200	$0,829*10^{-3}$		
Енергоспоживання на передачу блоку даних, Вт*с	100	$0,20*10^{-3}$		
	150	$0,99*10^{-3}$		
	200	$2,0*10^{-3}$		
Енергоспоживання за рік, Вт*с	100	2719,28	4772,39	7461,99
	150	2721,34	4774,46	7464,05
	200	2722,88	4775,94	7465,53
Час роботи пристрою в режимі IDLE, років	100	2,095	1,418	0,996
	150	2,094	1,417	0,995
	200	2,093	1,417	0,995
Час роботи пристрою в режимі PSM, років	100	3,310	1,886	1,206
	150	3,307	1,885	1,206
	200	3,305	1,884	1,205

Порівняємо час роботи термінальних пристроїв, що використовують режим PSM, із традиційними алгоритмами функціонування обладнання. Результати візуалізовано у графічній формі, як показано на рисунку 3.6. Діаграма відображає споживання ємності акумулятора пристрою впродовж певного періоду (у днях).

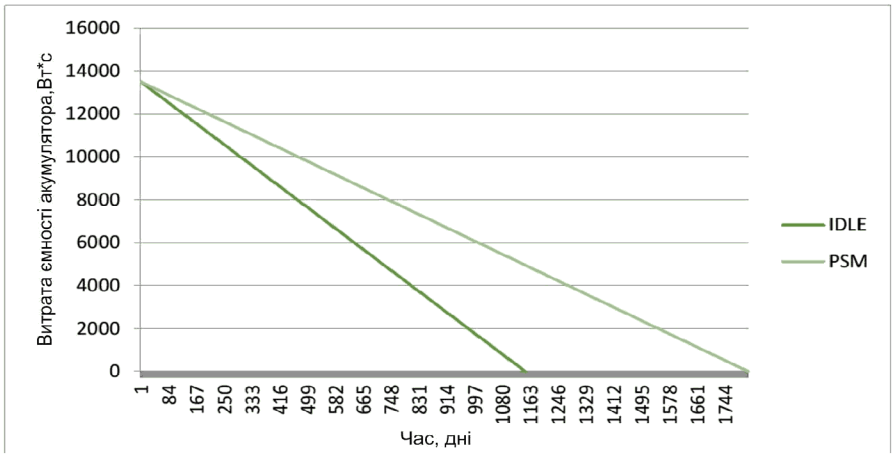

Рисунок 3.6 – Залежність ємності акумулятора від часу роботи пристрою

На основі поданого графіка можна зробити висновок, що використання режиму PSM у кінцевих пристроях подовжує термін служби батареї на 49% порівняно з традиційним режимом роботи пристроїв IoT у режимі BSM.

3.3 Розробка комп'ютерної моделі прогнозування енергоефективності

Під час розробки комп'ютерних математичних моделей рекомендується використовувати нейронні мережі та середовище моделювання Matlab/Simulink.

Нейронні мережі – це метод прогнозної аналітики, який застосовується для класифікації або прогнозування змінних. Вони є формою машинного навчання: система намагається передбачити значення змінних подібно до того, як це робить людський мозок.

Нейронна мережа функціонує шляхом формування структури з вхідних вузлів (вихідна точка), вихідних вузлів (результати/прогнози, сформовані після обробки даних) та прихованих шарів між ними.

Під час формування прогнозної моделі була побудована архітектура мережі, що враховує основні фактори, які впливають на точність прогнозування в умовах використання великих даних [27].

Побудована модель реалізує нейронну мережу типу NARX, яка дозволяє враховувати не лише поточні значення вхідних параметрів, а й затримки попередніх станів. Такий підхід дає змогу моделювати часові залежності між споживанням енергії та конфігурацією сенсорної мережі, що критично для реалістичного прогнозування в IoT-системах. Архітектура представлена на рисунку 3.7.

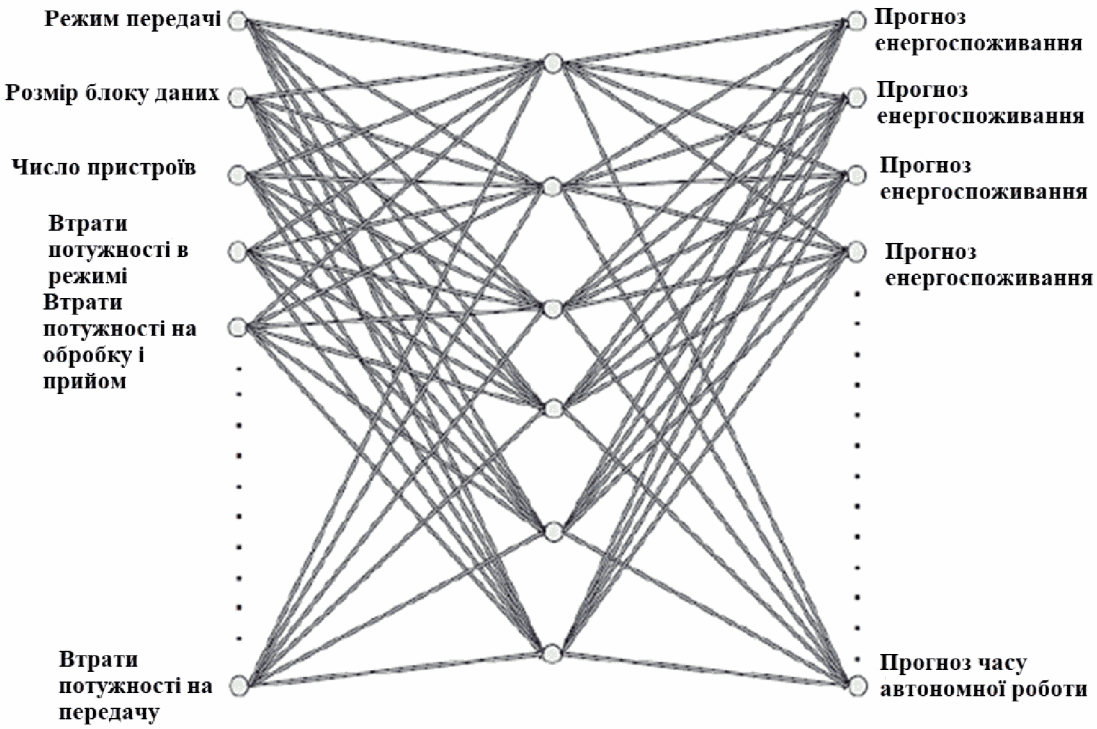

Рисунок 3.7 – Архітектура нейронної мережі для прогнозування енергоефективності

Навчання нейронної мережі здійснювалося в середовищі Matlab/Simulink на основі наявних даних та проведених обчислень. На рисунку 3.8 подано використані для навчання функції.

```
[y1,xf1,xf2] = myNeuralNetworkFunction(x1,x2,xi1,xi2)

takes these arguments:
    x1  = 8xTS matrix, input #1
    x2  = 1xTS matrix, input #2
    xi1 = 8x2 matrix, initial 2 delay states for input #1
    xi2 = 1x2 matrix, initial 2 delay states for input #2

and returns:
    y1  = 1xTS matrix, output #1
    xf1 = 8x2 matrix, final 2 delay states for input #1
    xf2 = 1x2 matrix, final 2 delay states for input #2

where TS is the number of timesteps.
```

Рисунок 3.8 – Програмна реалізація навчального процесу

Архітектура ПЗ представлена на рисунку 3.9. Вона включає модулі збору даних, попередньої обробки, обчислювального ядра на основі нейромережевої моделі та блок візуалізації результатів. Кожен модуль забезпечує окремий етап обробки — від первинного прийому телеметрії до формування остаточних висновків щодо енергоефективності. Діаграма класів представлена на рисунку 3.10.

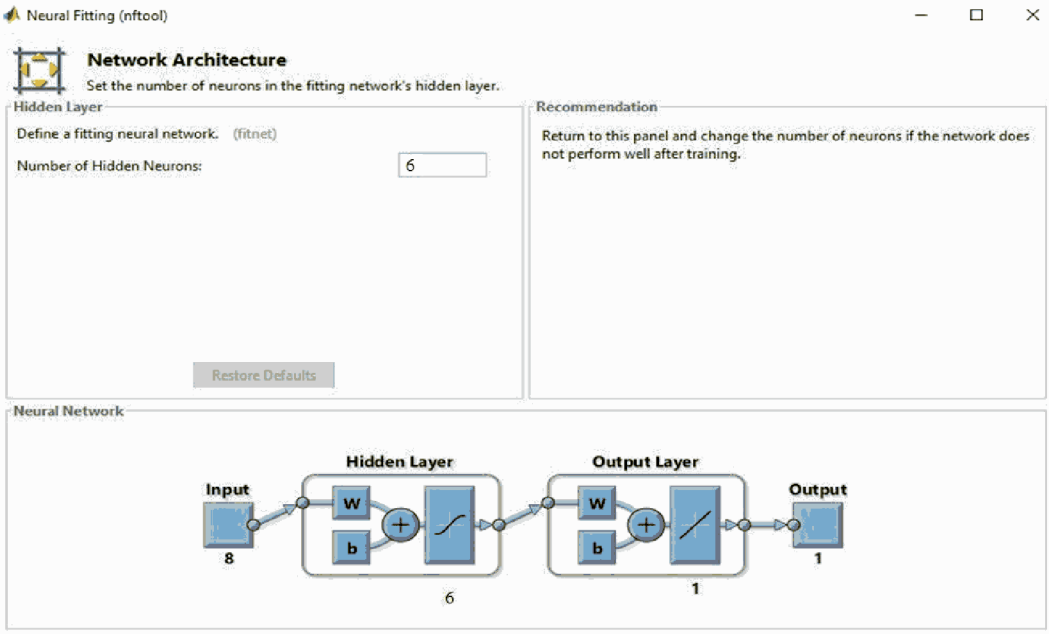

Рисунок 3.9 – Структура програмного забезпечення IoT-системи

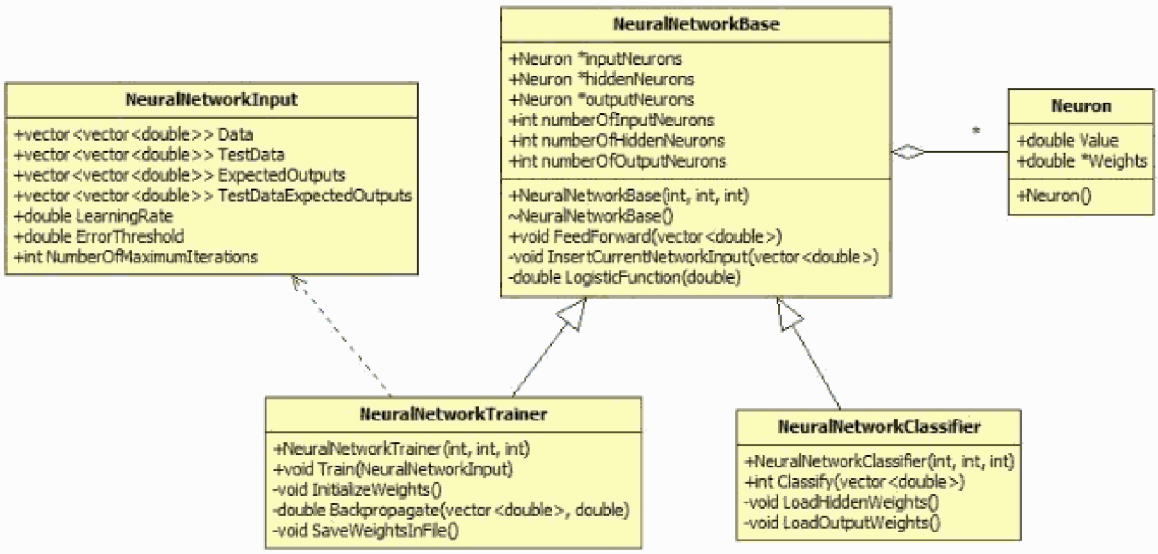

Рисунок 3.10 – Діаграма класів у розробленому програмному забезпеченні

Прогнозна модель представлена на рисунку 3.11. Побудована модель реалізує систему, яка враховує вплив кількох змінних: кількість пристроїв, частота передачі даних, режим енергозбереження (PSM) тощо. Вона дозволяє не лише розрахувати поточний стан, а й прогнозувати параметри енергоспоживання протягом заданого інтервалу часу.

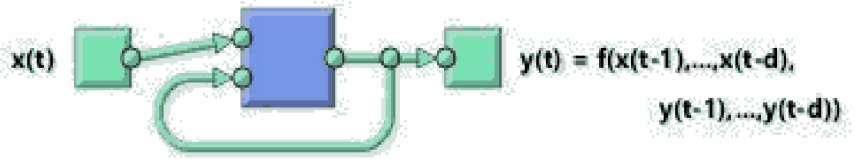

Рисунок 3.11 – Прогнозна модель оцінки енергоефективності

На рисунку 3.12 представлено результат симуляції роботи нейронної мережі типу NARX (Nonlinear Autoregressive Network with Exogenous Inputs) у середовищі MATLAB Simulink. Головна синя лінія на графіку відображає зміну вихідного значення моделі y1 у часі — це прогнозований показник, наприклад, значення енергоспоживання або стану пристрою в сенсорній мережі.

Графік має сходинкоподібну форму, що свідчить про реакцію моделі на зміни вхідних параметрів. Така поведінка характерна для систем, які переходять між дискретними режимами роботи, наприклад — зміна частоти передачі, активація режиму енергозбереження тощо.

У нижній частині графіка також відображено всі вхідні сигнали (x1(1)...x1(8), x2), однак їх значення візуально близькі до нуля (через масштабування), тому вони зображені у вигляді тонких ліній. Ці входи були використані мережею для формування відповідного прогнозу.

Симуляція засвідчує, що мережа успішно відтворює зміну вихідного параметра на основі часових рядів вхідних даних. Це підтверджує правильну побудову моделі та її здатність до узагальнення, що важливо для задач оцінки енергоефективності в IoT-системах.

Рисунок 3.12 – Візуалізація симуляції роботи програмного забезпечення

На рисунку 3.13 представлено завершальний етап моделювання роботи нейронної мережі NARX у середовищі Logic Analyzer. Графік демонструє зміну вихідного сигналу (NARX Neural Network) протягом симуляції, а також значення вхідних параметрів x1 та x2.

Візуалізація здійснена на чорному фоні з горизонтальними лініями, які відображають рівні сигналів у часі, а вертикальна жовта лінія вказує на момент часу 7.41 с, на якому було поставлено курсор для детального аналізу.

Значення вихідного сигналу (≈ 7.7872) свідчить про стабілізацію моделі, що підтверджує завершення процесу навчання та досягнення цільового рівня точності. Незначне коливання кривих демонструє адаптацію моделі до вхідних параметрів без явних стрибків чи розбалансування. Це вказує на відсутність перенавчання та достатню узагальнюючу здатність мережі. Таким чином, модель готова до використання для подальших прогнозів енергоефективності IoT-систем на основі нових вхідних даних..

Порівняємо результати, отримані аналітичними (обчислювальними) методами та за допомогою нейронних мереж, для прогнозування часу роботи кінцевих пристроїв IoT у високопродуктивних сенсорних мережах із використанням великих даних (таблиця 3.5).

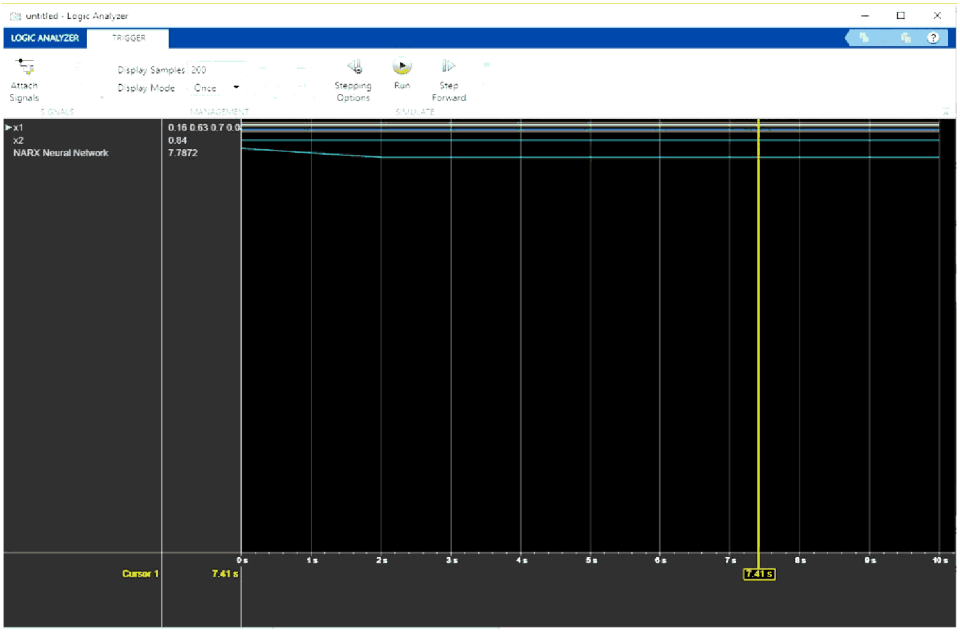

Рисунок 3.13 – Завершення процесу навчання нейронної мережі

Таблиця 3.5 – Порівняння результатів моделювання IoT-рішень

Параметр	Число NB-IoT пристроїв	Аналітичні результати	Прогнозування за допомогою НМ
Енергоспоживання на передачу блоку даних, Вт*с	100	$0,20*10^{-3}$	$0,1876*10^{-3}$
	150	$0,99*10^{-3}$	$0,9789*10^{-3}$
	200	$2,0*10^{-3}$	$2,0364*10^{-3}$
Енергоспоживання за рік, Вт*с	100	7461,99	7458,3686
	150	7464,05	7460,4859
	200	7465,53	7451,3689
Час роботи пристрою в режимі IDLE, років	100	0,996	0,98891
	150	0,995	0,98997

Із порівняльної таблиці видно, що похибка не перевищує 5 %, що свідчить про ефективність використання нейронних мереж для прогнозування часу роботи термінальних пристроїв IoT. Крім того, запропонований обчислювальний підхід можна застосовувати для оцінки енергоефективності високопродуктивних сенсорних мереж із використанням великих даних. Для досягнення високої енергоефективності доцільним є оптимальне застосування технології NB-IoT у таких сенсорних мережах [28].

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Загальні вимоги до безпеки при проектуванні сенсорних мереж IoT

Проектування сенсорних мереж IoT з використанням технологій BigData вимагає врахування ряду важливих аспектів, пов'язаних з безпекою на всіх етапах розробки та експлуатації. Сенсорні мережі часто використовуються для збору та обробки великої кількості даних, що можуть містити конфіденційну або чутливу інформацію, тому питання забезпечення безпеки є критично важливими. Одним з основних вимог є забезпечення надійної ідентифікації пристроїв та користувачів, що мають доступ до мережі. Всі пристрої сенсорної мережі повинні бути надійно захищені від несанкціонованого доступу, що досягається за допомогою криптографії, протоколів автентифікації та шифрування даних.

Важливим елементом є також безпечний обмін даними між пристроями в мережі та центром обробки даних. Дані, що передаються в межах сенсорної мережі, повинні бути зашифровані, що дозволить уникнути їх перехоплення чи спотворення під час транспортування. Крім того, необхідно враховувати захист даних на етапі зберігання в базах даних або хмарних платформах, де вони обробляються з використанням технологій BigData. У цьому контексті важливо забезпечити належну організацію доступу до даних та їх зберігання в умовах, коли доступ до інформації обмежений лише авторизованими користувачами.

Особливу увагу слід приділити безпеці при обробці великих обсягів даних. Оскільки сенсорні мережі IoT часто працюють у реальному часі, це ставить підвищені вимоги до їхньої стійкості до різноманітних атак.

Протоколи захисту повинні передбачати здатність системи ефективно справлятися з масивними потоками даних і забезпечувати їх безперервну обробку без втрат або порушень у роботі системи.

Крім того, при проектуванні сенсорних мереж важливо враховувати питання фізичної безпеки обладнання. Сенсори, розташовані в різних точках, можуть бути піддані ризикам фізичного пошкодження або крадіжки. Для цього слід передбачити фізичний захист пристроїв, а також можливість їх дистанційного моніторингу та діагностики для виявлення та реагування на несправності.

Не менш важливим аспектом є безпека при підключенні сенсорних мереж до інших систем або Інтернету. У зв'язку з поширенням атак через Інтернет, проектувальники повинні передбачити використання сучасних технологій безпеки, таких як брандмауери, системи виявлення вторгнень (IDS), а також механізми для захисту від атак типу "відмова в обслуговуванні" (DoS) чи інших шкідливих впливів.

Ще одним аспектом є безпека енергозабезпечення мережі. Сенсорні мережі часто використовують автономні джерела енергії, такі як сонячні панелі або батареї. У разі порушення енергозабезпечення можуть виникнути збої в роботі мережі, що ставить під загрозу її надійність. Для цього необхідно передбачити наявність резервних джерел живлення та механізмів автоматичного переключення між ними, щоб забезпечити безперебійне функціонування мережі.

Необхідно також враховувати вимоги до безпеки при розробці програмного забезпечення для сенсорних мереж. Програмні рішення повинні бути розроблені з урахуванням сучасних стандартів безпеки та захисту від шкідливого програмного забезпечення. Всі програмні компоненти, які взаємодіють з даними та пристроями мережі, повинні мати вбудовані механізми захисту від атак та можливість регулярного оновлення для зменшення ризиків від виявлених уразливостей.

4.2 Потенційні небезпеки при використанні технологій BigData в IoT системах

Використання технологій BigData в системах Інтернету речей (IoT) має численні переваги, зокрема здатність обробляти великі обсяги даних, забезпечувати аналітику в реальному часі та підвищувати ефективність системи. Однак одночасно з цими перевагами з'являються і потенційні небезпеки, які потребують уваги на етапі проектування та реалізації таких систем. Одна з основних проблем полягає в безпеці даних. Оскільки IoT системи генерують величезні потоки даних, які потім обробляються і зберігаються за допомогою технологій BigData, важливо забезпечити їхню захищеність на всіх етапах. У випадку несанкціонованого доступу до цих даних вони можуть бути використані зловмисниками для проведення атак на систему або навіть для маніпулювання результатами аналізу.

Однією з серйозних небезпек є вразливості в каналах зв'язку між сенсорами та централізованими обробними платформами. Більшість сенсорних мереж IoT мають обмежену пропускну здатність і ресурси, тому використовувані для передачі даних канали можуть бути піддані атакам. Порушення цілісності даних або їх перехоплення в процесі передачі може призвести до серйозних наслідків, таких як порушення роботи мережі або отримання недостовірної інформації. Наприклад, зловмисник, отримавши доступ до сенсорних даних, може вплинути на прийняття рішень в системах моніторингу або автоматизації, що в свою чергу призведе до неправильних дій або аварійних ситуацій.

Інша небезпека полягає в обробці великих обсягів чутливих або персональних даних. IoT системи часто використовуються для збору інформації про стан навколишнього середовища, здоров'я людей або інших аспектів, що можуть містити конфіденційну інформацію. Зберігання та обробка таких даних за допомогою технологій BigData вимагає дотримання

високих стандартів безпеки, щоб уникнути витоків або неправомірного використання інформації. Без належного захисту особистих даних можуть виникнути серйозні юридичні та етичні проблеми, що пов'язані з порушенням конфіденційності та довіри користувачів.

Крім того, у системах IoT, що використовують технології BigData, часто використовуються зовнішні сервіси для зберігання та обробки даних, наприклад, хмарні платформи. Ці сервіси можуть мати свої уразливості, що може поставити під загрозу безпеку даних, що зберігаються або обробляються за їх допомогою. Напад на хмарну платформу може призвести до компрометації великої кількості інформації, що має далекосяжні наслідки для усіх користувачів і зацікавлених сторін. Важливо враховувати, що в деяких випадках платформи, на яких зберігаються дані, можуть перебувати в іншій юрисдикції, що створює додаткові правові виклики щодо контролю над інформацією.

Ще однією важливою небезпекою є вразливість самих сенсорних пристроїв IoT. Оскільки сенсори зазвичай мають обмежену обчислювальну потужність і енергозабезпечення, їх захист часто залишає бажати кращого. Сенсори можуть бути фізично зламані або зламані в результаті зовнішніх атак, що дозволяє зловмисникам змінювати показання або повністю вивести пристрій з ладу. Оскільки більшість сенсорних пристроїв підключені до Інтернету або внутрішніх мереж, зловмисники можуть використовувати ці вразливості для атаки на інші частини системи, що ще більше підвищує ризик порушення безпеки.

Не менш важливим аспектом є питання управління великими даними в реальному часі. В IoT системах, де дані мають критичне значення для оперативного прийняття рішень, будь-яка затримка або помилка в обробці даних може призвести до неправильних дій. Наприклад, в системах охорони здоров'я затримка в обробці медичних даних може негативно вплинути на діагностику або лікування пацієнтів. В обробці великих обсягів даних,

зокрема в реальному часі, можуть виникати ситуації, коли система не встигає своєчасно відреагувати на події, що ставить під загрозу безпеку.

Крім того, зростаюча складність та інтеграція різних пристроїв в одну мережу призводить до того, що забезпечити безпеку на всіх етапах, від збору до обробки і зберігання даних, стає надзвичайно складно. У великих IoT системах часто використовуються різні пристрої від різних виробників, що ускладнює створення єдиного стандарту безпеки. Відсутність стандартів може призвести до ситуацій, коли окремі компоненти системи мають слабкі місця в безпеці, що підвищує ймовірність успішних атак на систему.

Таким чином, потенційні небезпеки при використанні технологій BigData в IoT системах включають ряд факторів, пов'язаних з безпекою даних, ризиками перехоплення або маніпуляцій даними, вразливістю сенсорних пристроїв та зовнішніх платформ. Врахування цих факторів під час проектування IoT систем дозволить мінімізувати ризики та підвищити надійність і безпеку таких систем у майбутньому.

4.3 Заходи безпеки при тестуванні та експлуатації сенсорних мереж

Тестування та експлуатація сенсорних мереж, що використовують технології BigData, є критично важливими етапами в процесі їхнього впровадження. Враховуючи, що ці мережі часто функціонують у реальному часі, з високою інтенсивністю передачі даних і обробки великих обсягів інформації, забезпечення безпеки на цих етапах є надзвичайно важливим. Одним із основних аспектів є тестування на стійкість до атак і порушень безпеки, що може включати як фізичні атаки на обладнання, так і програмні уразливості. Тестування повинно охоплювати перевірку надійності каналів зв’язку, стійкість до атак, а також коректність обробки даних при несприятливих умовах.

На етапі тестування необхідно перевірити, чи система здатна протистояти різноманітним атакам, таким як "відмова в обслуговуванні" (DoS) чи "перехоплення" даних. Для цього часто використовуються спеціальні методи, такі як стрес-тестування і проведення атак за допомогою моделей, що імітують реальні сценарії. Це дозволяє виявити уразливості в системі, які можуть бути використані зловмисниками для проникнення або порушення її роботи. Тестування має бути не тільки стандартним, але й включати в себе перевірку на вплив різних зовнішніх факторів, таких як зміна температури, зниження рівня сигналу або втрата з'єднання.

Особливо важливою є перевірка системи на предмет її стійкості до кібератак, таких як інжекція шкідливих даних або спроби маніпулювання сенсорними даними. У випадку використання BigData, де обробляються величезні обсяги даних, критично важливо забезпечити їх захист на всіх етапах, включаючи передачу, зберігання та обробку. Наявність захисту в реальному часі дозволяє виявляти та зупиняти атаки ще на ранніх етапах, що забезпечує більш високий рівень безпеки при експлуатації мережі. Важливою частиною цього є використання криптографії для шифрування даних, що передаються між пристроями в мережі. Технології шифрування мають бути реалізовані таким чином, щоб навіть у разі перехоплення даних, вони не могли бути використані без відповідного ключа доступу.

Експлуатація сенсорних мереж також вимагає регулярного моніторингу їх стану і своєчасного реагування на можливі проблеми, такі як втрата з'єднання між сенсорами або збої в їхній роботі. Постійний моніторинг дозволяє своєчасно виявити неполадки та запобігти можливим аваріям, таким як втрата даних або неполадки в самому обладнанні. Для цього розробляються спеціальні системи управління, які автоматично перевіряють стан кожного сенсора та всіх компонентів мережі. Ці системи повинні мати можливість оперативно повідомляти оператора про виявлені збої та автоматично відновлювати роботу мережі в разі помилки.

Ще одним важливим етапом є забезпечення безпеки фізичної інфраструктури сенсорних мереж. Оскільки сенсори можуть бути встановлені в різних місцях, їх фізичний доступ повинен бути обмежений. Необхідно реалізувати засоби захисту від несанкціонованого доступу до пристроїв, таких як вбудовані замки, датчики руху або відеоспостереження. Також має бути забезпечено резервне живлення для запобігання відмовам мережі при збої основного джерела енергії. Зазвичай, для забезпечення безперебійної роботи використовуються джерела живлення з акумуляторами або сонячними панелями, що дозволяє уникнути проблем, пов'язаних із відключенням енергопостачання.

Враховуючи потенційні загрози, важливою складовою експлуатації є регулярні оновлення програмного забезпечення, яке відповідає за обробку даних і взаємодію між пристроями. Оновлення повинні включати виправлення уразливостей у безпеці, що були виявлені після запуску мережі, а також забезпечення відповідності стандартам безпеки, що постійно змінюються. Для цього часто використовуються автоматизовані системи для оновлення програмного забезпечення без необхідності зупиняти роботу мережі.

Особливу увагу слід приділити питанням безпеки на етапі інтеграції сенсорних мереж з іншими інформаційними системами, зокрема, хмарними платформами, де зберігаються великі обсяги даних. Під час інтеграції може виникнути необхідність в обміні даними між різними мережами або зовнішніми сервісами, тому важливо встановити чіткі протоколи безпеки, щоб уникнути витоків або несанкціонованого доступу. Без належної організації обміну даними безпека мережі може бути знижена через вразливості в обробці та передачі даних між різними сервісами.

ВИСНОВКИ

У кваліфікаційній роботі проведено комплексне дослідження проблематики проєктування високопродуктивних сенсорних мереж IoT з використанням технологій Big Data. На основі аналізу сучасних архітектур, методів зв'язку та інтелектуальних алгоритмів розроблено модель IoT-системи, що забезпечує енергоефективну роботу в умовах великого потоку телеметричних даних.

Обґрунтовано базові принципи функціонування бездротових сенсорних мереж, наведено багаторівневу архітектуру IoT-систем із розподілом обов'язків між периферійними пристроями, шлюзами та хмарними платформами. Особливу увагу приділено енергоефективності при побудові сенсорних вузлів.

Проаналізовано ключові технології передавання даних (LoRa, NB-IoT, SIGFOX, Weightless-P), їх порівняльні характеристики, а також можливості інтеграції з інструментами Big Data. Розглянуто впровадження штучного інтелекту в системах IoT для прогнозної аналітики та виявлення аномалій.

Виконано математичне моделювання енергоефективності IoT-систем з урахуванням затримок при підключенні пристроїв та можливих колізій при передаванні даних. Побудовано модель споживання енергії та розраховано тривалість автономної роботи пристроїв у режимах IDLE і PSM. Додатково розроблено комп'ютерну модель на основі нейронної мережі типу NARX, яка дозволила здійснити точне прогнозування енергоспоживання з похибкою не більше 5 % порівняно з аналітичними методами.

У результаті виконаної роботи сформовано архітектуру сенсорної мережі з підтримкою Big Data, визначено оптимальні параметри для забезпечення автономності пристроїв, обґрунтовано доцільність використання нейронних мереж для задач прогнозування в IoT, проведено симуляції, які підтверджують ефективність запропонованої моделі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія. Київ: Видавничий дім «АртЕк», 2018. 344 с.

2. Бергенті Ф., Каїре Дж., Готта Д. Large-scale network and service management with WANTS. Industrial Agents: Emerging Applications of Software Agents in Industry. Elsevier, 2015. 366 p.

3. Вермесан О., Фрієс П., Гійомен П. та ін. Internet of Things Strategic Research and Innovation Agenda. In River Publishers Series in Communications. Aalborg: River Publishers, 2013. 158 p.

4. Вайлсбек С., Грімм В. Agent-based and Individual-based Modeling: A Practical Introduction. Princeton: Princeton University Press, 2011.

5. Ільченко М. Ю., Кравчук С. О. Телекомунікаційні системи. Київ: Наукова думка, 2017. 730 с.

6. Ковбаса А. О., Лисенко О. І. Огляд концепції потокової обробки даних. Перспективи телекомунікацій: матеріали XIV міжнар. наук.-техн. конф. (Київ, 2020). Київ: КПІ ім. Ігоря Сікорського, 2020. С. 298–300.

7. Ковбаса А. О., Лисенко О. І. Парадигма MapReduce як метод розподіленої обробки великих об'ємів даних. Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій: матеріали 2-ї міжнар. наук.-практ. конф. (Київ, 19 груд. 2019 р.). Київ: НУХТ, 2019. С. 175–177.

8. Кірічек Р., Кулик В. Long-Range Data Transmission on Flying Ubiquitous Sensor Networks (FUSN) by Using LPWAN Protocols. Communications in Computer and Information Science. 2016. Vol. 678. С. 442–453. DOI: 10.1007/978-3-319-51917-3_39.

9. Майк Райлі. Programming Your Home: Automate with Arduino, Android, and Your Computer. Dallas, Texas; Raleigh, North Carolina: The Pragmatic Bookshelf, 2012.

10. Муртаґ Н., Гатерслебен Б., Уззел Д. 20;60;20 – Differences in Energy Behaviour and Conservation between and within Households with Electricity Monitors, 2014.

11. Оуссус А., Бенжеллун Ф., Лахцен А., Белфкіха С. Big Data Technologies: A Survey. Journal of King Saud University – Computer and Information Sciences. 2018. Vol. 30. P. 431–448.

12. Розроблення стартап-проекту: Методичні рекомендації до виконання розділу магістерських дисертацій для студентів інженерних спеціальностей. Київ: НТУУ «КПІ», 2016. 28 с.

13. Ру Ф. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations. Boca Raton: CRC Press, 2016. 137 p.

14. Фантона Дж. І., Оае С. А. Evolution of Smart Building. Proceedings of the 2013 International Conference on Environment, Energy, Ecosystems and Development, 2013.

15. Фарукві А., Сергісі С., Шаріф А. The impact of informational feedback on energy consumption: a survey of the experimental evidence. Energy. 2020. Vol. 35. P. 1598–1608.

16. Шмарцо Б. Big Data: Understanding How Data Powers Big Business. Мілан: Wiley, 2013. 240 с.