Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи обробки та аналізу даних в IoT

(тема)

Виконав:
здобувач 2 року навчання,
групи СПм-23-3
До Нгок Куен
(власне ім'я, прізвище)

Спеціальність
123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма
Системне програмування
(повна назва освітньої програми)

Керівник: професор Олег МІХАЛЬ
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві До Нгок Куен
(прізвище, ім'я, по батькові)

1. Тема роботи Методи обробки та аналізу даних в IoT

затверджена наказом по університету від " 21 " квітня 2025 р. № 296 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 16 червня 2025 р.

3. Вхідні дані до роботи
обчислювальний вузол
обробка даних
призначення завдання
IoT

4. Перелік питань, що потрібно опрацювати у роботі
Аналіз предметної оласті та постановка завдання
Методи обробки даних в IoT
Програмна реалізація та аналіз результатів

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 15 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Отримання завдання та аналіз літератури	21.04.2025–30.04.2025	
2	Огляд існуючих рішень та алгоритмів	01.05.2025–12.05.2025	
3	Розробка методу	13.05.2025–22.05.2025	
4	Вибір програмних засобів	23.05.2025–30.05.2025	
5	Програмна реалізація	31.05.2025–02.06.2025	
6	Аналіз отриманих результатів	03.06.2025–05.06.2025	
7	Оформлення записки	06.06.2025–12.06.2025	

Дата видачі завдання " 21 " квітня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ професор Олег МІХАЛЬ
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 74 с., 16 рис., 2 дод., 7 джерел.

ІНТЕРНЕТ РЕЧЕЙ, СЕНСОРНА МЕРЕЖА, ДІАГНОСТИКА, ВИЯВЛЕННЯ НЕСПРАВНОСТЕЙ, ПРЕДИКТИВНА АНАЛІТИКА, АВТОЕНКОДЕР, МАШИННЕ НАВЧАННЯ, РЕКОНСТРУКТИВНА ПОХИБКА, АНОМАЛІЯ, МОНІТОРИНГ ДОВКІЛЛЯ, РОЗПОДІЛЕНА СИСТЕМА, MQTT-ПРОТОКОЛ, ТЕХНІЧНИЙ СТАН, КЛАСИФІКАЦІЯ, КЛАСТЕРИЗАЦІЯ, ХМАРНІ ОБЧИСЛЕННЯ, GOOGLE COLAB.

Метою кваліфікаційної роботи є розробка, реалізація та апробація методу діагностування технічного стану сенсорних пристроїв у розподіленій автоматизованій системі моніторингу, що функціонує на основі архітектури Інтернету речей. Особлива увага приділяється інтеграції методів машинного навчання для виявлення відхилень у поведінці сенсорів, що дозволяє підвищити надійність, стабільність і передбачуваність роботи екологічної інфраструктури.

У ході виконання кваліфікаційної роботи змодельовано структуру розподіленої системи моніторингу, що включає сенсорні пристрої, брокер MQTT-протоколу та хмарну обчислювальну інфраструктуру. Було створено набір синтетичних тестових даних, що імітують реальні сигнали з включенням аномальних відхилень. На основі цих даних було реалізовано повнофункціональну модель автоенкодера, навченої на нормальних даних. Метод реконструкції сигналу дозволив автоматично виявляти області, де спостерігалося суттєве відхилення, що свідчить про збої в роботі пристрою. Проведено кілька сценаріїв візуалізації з метою локалізації й оцінки аномалій, а також виконано повний аналіз ефективності моделі. Робота також

включає міждисциплінарний огляд сучасної літератури щодо захисту персональних даних, оптимізації обчислень на периферії та розвитку предиктивного обслуговування в IoT.

Запропонований метод і реалізована модель можуть бути основою для побудови інтелектуальних систем підтримки прийняття рішень у сфері моніторингу довкілля, що функціонують в умовах обмежених ресурсів і великої кількості розподілених пристроїв. Отримані результати підтверджують ефективність використання машинного навчання в задачах діагностики технічного стану сенсорних вузлів у реальних IoT-мережах.

ABSTRACT

Master’s thesis: 74 pages, 16 figures, 2 appendices, 7 sources.

INTERNET OF THINGS, SENSOR NETWORK, DIAGNOSTICS, FAULT DETECTION, PREDICTIVE ANALYTICS, AUTOENCODER, MACHINE LEARNING, RECONSTRUCTION ERROR, ANOMALY, ENVIRONMENTAL MONITORING, DISTRIBUTED SYSTEM, MQTT PROTOCOL, TECHNICAL CONDITION, CLASSIFICATION, CLUSTERING, CLOUD COMPUTING, GOOGLE COLAB.

The major goal of this thesis is to develop, implement, and validate a method for diagnosing the technical condition of sensor devices within a distributed automated monitoring system based on the Internet of Things architecture. Emphasis is placed on the integration of machine learning techniques to detect deviations in sensor behavior, which enhances the reliability, stability, and predictability of environmental infrastructure performance.

In order to the structure of a distributed monitoring system was modeled, encompassing sensor nodes, an MQTT protocol broker, and a cloud-based computing infrastructure. A synthetic dataset was generated to simulate real-world signals, including injected anomalous deviations. Based on this dataset, a fully functional autoencoder model was implemented and trained on normal operational data. The signal reconstruction method enabled automatic identification of regions exhibiting significant deviations, indicating potential device malfunctions. Several visualization scenarios were conducted to localize and assess anomalies, accompanied by a comprehensive evaluation of the model’s performance.

The work also includes an interdisciplinary review of recent literature related to personal data protection, edge computing optimization, and the development of predictive maintenance techniques in IoT environments. The proposed method and

implemented model provide a foundation for building intelligent decision support systems for environmental monitoring, operating under resource-constrained conditions and involving many distributed devices.

The obtained results confirm the effectiveness of applying machine learning techniques to diagnose the technical state of sensor nodes in real-world IoT networks.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AI – штучний інтелект

API – інтерфейс прикладного програмування

BLE – енергоефективна версія Bluetooth

CSV – формат табличних даних, розділених комами

DDoS – розподілена атака на відмову в обслуговуванні

DSL – цифрова абонентська лінія

GAN – генеративна змагальна мережа

GPRS – пакетна передача даних у мережах GSM

GSM – глобальна система мобільного зв’язку

HTTP – протокол передавання гіпертексту

IoT – Інтернет речей

IPv4 – четверта версія протоколу інтернету

IPv6 – шоста версія протоколу інтернету

LTE – мережа мобільного зв’язку четвертого покоління

ML – машинне навчання

MQTT – телеметричний протокол передачі повідомлень

NGN – мережі наступного покоління

OSI – еталонна модель взаємодії відкритих систем

PaaS – платформа як послуга

PAN – персональна мережа

QoS – якість обслуговування

RFID – радіочастотна ідентифікація

SaaS – програмне забезпечення як послуга

SSL – протокол захищених сокетів

TLS – протокол транспортного рівня безпеки

UWB – надширокосмугова технологія

Wi-Fi – бездротова локальна мережа

WSN – бездротова сенсорна мережа

WWW – всесвітня павутина

ZigBee – стандарт бездротової передачі даних з низьким енергоспоживанням

ВСТУП

На сучасному етапі розвитку технічного прогресу та цифрової трансформації питання охорони навколишнього середовища, зокрема водних ресурсів, стає надзвичайно актуальним. Стан гідрографічної мережі є критичним індикатором загальної екологічної стабільності, а її чистота – запорукою безпеки біорізноманіття, якості життя населення та функціонування господарських систем. Забруднення водних масивів унаслідок діяльності промислових підприємств, несанкціонованих скидів або неочевидних антропогенних впливів потребує оперативного виявлення, контролю та реагування.

Одним із перспективних рішень у цьому контексті є застосування розподілених сенсорних систем для постійного моніторингу екологічних показників. Інтеграція інтелектуальних вимірювальних пристроїв, здатних працювати в режимі реального часу, дозволяє з високою точністю фіксувати зміни у стані водних об’єктів, включно з хімічним, біологічним та фізичним складом середовища. Проте, для охоплення навіть однієї річкової системи необхідна велика кількість таких пристроїв, які функціонують у складі масштабної розподіленої інфраструктури. Йдеться про тисячі, а іноді й мільйони вузлів, з’єднаних у єдину сенсорну мережу, що потребує скоординованого управління, надійного зберігання та аналітики даних.

Кожен вузол такої системи має забезпечувати автономну роботу в умовах обмеженої мережевої доступності та енергоспоживання, одночасно збираючи різноманітні метричні дані. Це створює потребу в особливо ретельному проектуванні та оптимізації архітектури обслуговуючих дата-центрів, що виконують цілодобову агрегацію, обробку й інтерпретацію інформації з урахуванням складності та варіативності вхідних потоків.

Завдяки динамічному розвитку технологій Інтернету речей (IoT), з’являється можливість масштабованого впровадження подібних систем у

сферу моніторингу довкілля. Комунікаційні протоколи, зокрема MQTT, забезпечують ефективну передачу даних навіть за нестабільних умов мережевого з’єднання, а програмно-апаратні платформи дозволяють інтегрувати сенсорні модулі з хмарними та серверними системами.

Особливу роль у підвищенні надійності таких розподілених систем відіграє предиктивне обслуговування, що базується на методах машинного навчання та штучного інтелекту. Аналізуючи історичні дані про функціонування сенсорних вузлів, можна з високою точністю прогнозувати можливі відмови, зниження ефективності або нестабільну роботу окремих елементів системи. Це дозволяє реалізувати концепцію "обслуговування на основі стану", яка є значно ефективнішою за традиційні підходи, засновані на фіксованих інтервалах технічного втручання.

Інтеграція нейронних мереж у систему аналізу IoT-мереж відкриває можливості для розпізнавання аномалій, класифікації типів збоїв і динамічного призначення завдань вузлам мережі з урахуванням поточних умов. Це дозволяє підвищити загальну відмовостійкість системи, зменшити втрати даних, а також забезпечити безперервний екологічний моніторинг з високим ступенем достовірності.

Метою даної роботи є розробка науково обґрунтованого підходу до збору, обробки та інтерпретації екологічних даних у розподіленій сенсорній мережі Інтернету речей з реалізацією предиктивного обслуговування на основі штучного інтелекту. Особливу увагу приділено архітектурі системи, методам діагностики несправностей і алгоритмам класифікації даних.

Основні завдання дослідження:

- провести системний аналіз технологій Інтернету речей у контексті екологічного моніторингу;
- дослідити існуючі методи обробки даних та розподілу завдань між вузлами IoT-мереж;
- розробити метод виявлення аномалій і потенційних несправностей у сенсорній мережі на основі штучних нейронних мереж.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Поняття «Інтернет речей» сьогодні є невіддільним від цифрової трансформації суспільства, проте його становлення як науково-технічної концепції відбувалося поступово протягом кількох десятиліть. Хоча термін «Інтернет речей» було офіційно запропоновано лише у 1999 році Кевіном Ештоном, ідеї, що закладені в його основу, з'явилися значно раніше. Ще у 1926 році Нікола Тесла в інтерв'ю для журналу Collier's передбачив появу пристроїв, які дозволятимуть здійснювати миттєвий зв'язок між людьми незалежно від відстані, підкресливши, що такі засоби зв'язку будуть мати мініатюрні розміри та зможуть вільно розміщуватись у кишені. Ці прогностичні уявлення надалі стали основою для концепцій глобального зв'язку між речами.

Одним із перших практичних прикладів реалізації концепції IoT вважається експеримент, проведений у 1990 році випускником Массачусетського технологічного інституту Джоном Ромкі. Він підключив звичайний тостер до Інтернету, що дозволяло дистанційно його вмикати, тим самим продемонструвавши фундаментальну ідею взаємодії фізичного об'єкта з мережею.

Сьогодні існує декілька загальноприйнятих визначень Інтернету речей, які хоч і відрізняються за формулюваннями, але відображають спільну концептуальну основу. По-перше, IoT розглядається як сукупність фізичних пристроїв, які мають змогу обмінюватися даними через мережу без безпосередньої участі людини. По-друге, його трактують як архітектуру обчислювальної інфраструктури, де фізичні об'єкти оснащуються вбудованими сенсорами, процесорами та засобами комунікації для взаємодії з іншими об'єктами або інформаційним середовищем. Нарешті, концепція IoT передбачає трансформацію економічних і соціальних моделей за рахунок автоматизації дій, які раніше потребували участі людини.

У всіх цих визначеннях ключовим елементом залишається наявність об'єднаної мережі «розумних» пристроїв, здатних до автономної взаємодії, збору та передачі даних, а також самостійного прийняття рішень у рамках заданих алгоритмів.

Історичний розвиток IoT тісно пов’язаний із прогресом у суміжних галузях: радіочастотній ідентифікації (RFID), міжмашинній взаємодії (M2M), мобільному зв’язку п’ятого покоління (5G), масовому впровадженні IPv6, що забезпечує глобальну адресацію трильйонів пристроїв, а також хмарних обчисленнях (SaaS, PaaS, IaaS тощо). Зокрема, протокол IPv6 відкрив можливість теоретично ідентифікувати до 5×10285×1028 об’єктів на кожного мешканця Землі, що створює технічну основу для побудови глобальних IoT-екосистем.

Динаміка впровадження Інтернету речей є показовою: вже у 2009 році кількість пристроїв, підключених до Інтернету, перевищила кількість населення планети, і ця тенденція лише прискорюється. За прогнозами аналітиків Cisco IBSG, кількість підключених об’єктів зростає в геометричній прогресії, і цей процес визначає розвиток цифрової інфраструктури найближчих десятиліть.

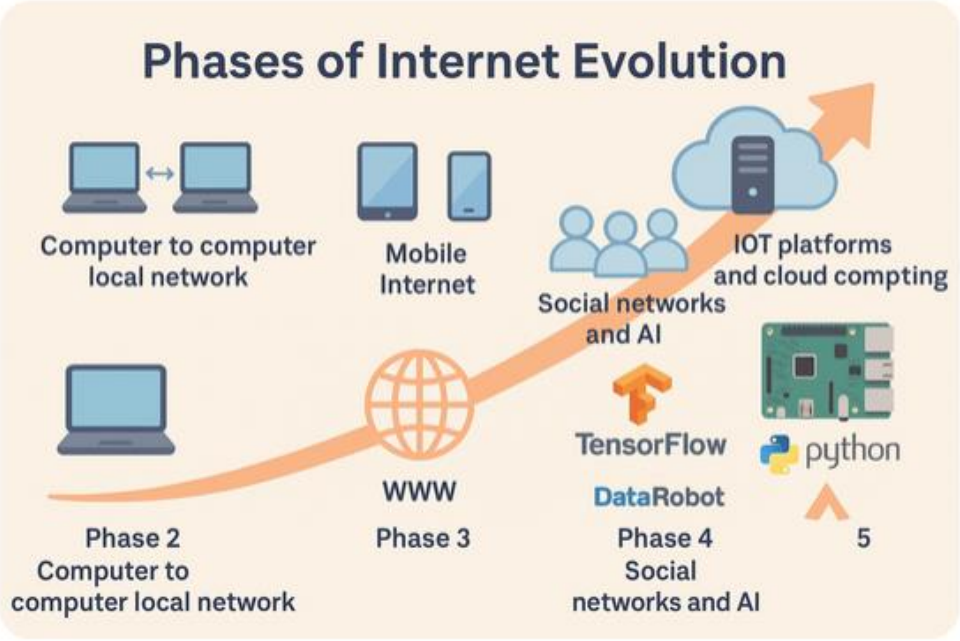

Рисунок 1.1 – Фази еволюції пристроїв

На рисунку 1.1 представлено п’ять фаз еволюції Інтернету – від локальних комп’ютерних мереж до сучасних IoT-платформ. Ілюстрація має вигляд висхідної стрілки, яка символізує поступовий розвиток мережевих технологій. Нижче наведено короткий опис кожної фази:

- фаза 1 – Локальні комп’ютерні мережі. Представлено обмін даними між двома комп’ютерами у межах однієї локальної мережі (LAN);
- фаза 2 – Всесвітня павутина (WWW). Зображено поєднання декількох комп’ютерів через Інтернет для доступу до веб-ресурсів;
- фаза 3 – Мобільний Інтернет. Додано мобільні пристрої – смартфони й планшети – як повноцінних учасників мережевої взаємодії;
- фаза 4 – Соціальні мережі та штучний інтелект. Відображено комунікацію між людьми через соціальні мережі, а також поява AI-платформ: TensorFlow, DataRobot, Python – що свідчить про інтелектуалізацію інтернет-контенту;
- фаза 5 – IoT-платформи та хмарні обчислення. Зображено хмару як символ хмарних технологій та мікроконтролер (Raspberry Pi) як приклад пристрою з вбудованим IoT-функціоналом. Цей рівень представляє сучасну еру "Інтернету речей", де не тільки люди, а й пристрої активно обмінюються даними.

Ця інфографіка наочно демонструє, як інтернет трансформувався від простого інструмента передачі даних до розумного середовища, що охоплює повністю автономні пристрої та складні системи штучного інтелекту.

Стрімкий розвиток IoT зумовив включення дедалі більшої кількості фізичних об'єктів до єдиної глобальної мережі, в якій вони можуть автономно взаємодіяти між собою, передавати дані й ініціювати події без прямої участі людини. Цей процес радикально змінює підходи до аналітики, управління та безпеки в різноманітних сферах діяльності, створюючи передумови для підвищення якості життя, автоматизації рутинних процесів і зменшення впливу людського фактора.

На сьогодні існує кілька ключових галузей, де технології IoT демонструють високу ефективність та практичну цінність:

- логістика та транспорт – інтелектуальні системи моніторингу вантажів, маршрутів, стану транспорту й оптимізації доставки;
- житлово-комунальне господарство – системи обліку ресурсів (вода, газ, електроенергія), автоматичне регулювання освітлення, опалення тощо;
- медицина – дистанційне спостереження за пацієнтами, управління медичними приладами, збирання фізіологічних показників у реальному часі;
- системи безпеки – відстеження місцеперебування людей, тварин, контроль доступу, охорона об’єктів та сповіщення про надзвичайні ситуації.;
- промислові об’єкти та екологічний моніторинг – виявлення відхилень у роботі обладнання, діагностика стану навколишнього середовища, автоматичне управління технічними процесами.

Особливої уваги заслуговує індустріальний Інтернет речей (Industrial Internet of Things, IIoT), який є окремим напрямом у межах IoT. Він охоплює комплекс пристроїв, систем комунікації, збору, обробки, візуалізації та інтерпретації інформації, що інтегруються для вирішення виробничих завдань. IIoT формує нову парадигму управління підприємствами, базуючись на синергії апаратних засобів і інтелектуальних програмних технологій.

Історично основою для IIoT стали системи релейного захисту й теплова автоматика, побудовані на основі жорсткої, непрограмованої логіки. З поширенням мікропроцесорної техніки з’явилася можливість реалізовувати гнучкі програмні алгоритми управління. Сучасний етап розвитку характеризується інтеграцією методів штучного інтелекту, таких як нейронні мережі, алгоритми нечіткої логіки та моделі машинного навчання. Вони дозволяють реалізовувати адаптивне керування, оптимізацію режимів роботи устаткування та здійснювати передиктивний аналіз на основі великих обсягів даних.

Окремо варто зазначити потенціал нейромережевих моделей у контексті математичного моделювання виробничих процесів. Нейромережеві

апроксиматори можуть вирішувати системи диференціальних рівнянь у реальному часі, що дозволяє здійснювати прогнозування технологічних параметрів з високою точністю. Це створює підґрунтя для систем підтримки прийняття рішень із розширеним просторово-часовим горизонтом планування.

Автоматизація, побудована на засадах IIoT, зменшує необхідність безпосередньої участі оператора в керуванні складними технічними системами. Це значно знижує ризики, пов’язані з людським фактором, і підвищує рівень безпеки, надійності та відмовостійкості об’єктів критичної інфраструктури. Водночас стійкість і ефективність IIoT-систем прямо залежать від якості їх проєктування, вибору архітектурних рішень та дотримання вимог до експлуатаційної надійності на всіх етапах життєвого циклу.

Таким чином, створення надійної та функціонально ефективної індустріальної IoT-системи вимагає комплексного підходу, що включає технічне проєктування, аналіз потенційних відмов, розробку захищених комунікаційних протоколів і впровадження інтелектуальних алгоритмів керування.

1.1 Технології побудови IoT

З метою уніфікації термінології та забезпечення міжнародної сумісності технологій, пов’язаних із Інтернетом речей, Міжнародний союз електрозв'язку (МСЕ) у 2012 році затвердив рекомендацію МСЕ-Т Y.2060, яка містить одне з найбільш авторитетних і визнаних визначень цього поняття. У документі зазначено, що:

«Інтернет – це глобальна інфраструктура для інформаційного суспільства, яка забезпечує розширені послуги шляхом взаємодії між фізичними та віртуальними речами на основі існуючих і розвиваних інформаційно-комунікаційних технологій».

Це визначення охоплює ключові характеристики IoT як багаторівневої, міждисциплінарної платформи, що включає елементи сенсорних технологій, телекомунікацій, хмарних обчислень, інтелектуального аналізу даних та автоматизованого управління. Змістовно воно підкреслює, що IoT не обмежується лише фізичними пристроями, а також охоплює віртуальні об’єкти, які можуть брати участь у передачі, аналізі та використанні даних.

Інфраструктура IoT, згідно з цією концепцією, будується на принципах сумісності, масштабованості та гнучкості, що дозволяє інтегрувати її в наявні телекомунікаційні системи без потреби повного оновлення обладнання. Водночас вона забезпечує основу для створення нових сервісів і додатків, які раніше були технічно неможливими або економічно недоцільними.

На рисунку 1.2 зазвичай візуалізується ця модель, що ілюструє взаємозв’язок між різними категоріями речей (фізичних та віртуальних), комунікаційною інфраструктурою, сервісними платформами та кінцевими користувачами. Така структура підкреслює орієнтованість IoT на послуги (service-oriented architecture), що є фундаментом для розвитку цифрової економіки та індустрії 4.0.

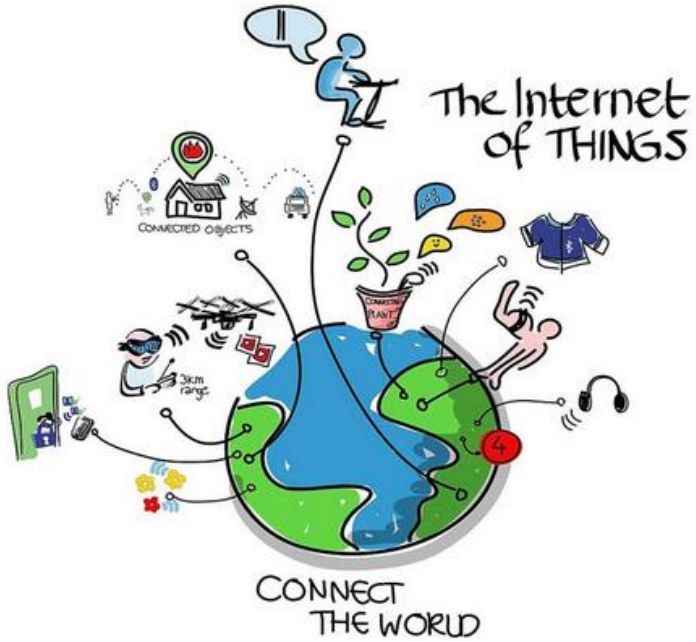

Рисунок 1.2 – Можливості IoT

Таким чином, рекомендація MCE-T Y.2060 закладає концептуальні основи для подальшої стандартизації, проєктування та впровадження рішень у сфері Інтернету речей, визначаючи його не лише як технічну систему, а як інтегральну частину інформаційного суспільства, здатну трансформувати всі аспекти життя – від побуту до глобальних виробничо-логістичних ланцюгів.

У межах концепції Інтернету речей, як зазначено в рекомендаціях MCE-T (ITU-T Y.2060), термін «річ» (англ. thing) охоплює як фізичні об'єкти, так і віртуальні сутності, які можуть бути ідентифіковані в комунікаційному середовищі. Це означає, що «річчю» може виступати не лише матеріальний пристрій (наприклад, датчик або механізм), а й програмне забезпечення, мультимедійний контент або хмарний сервіс, що має здатність до інтеграції у єдину мережу та взаємодії з іншими елементами системи.

Поряд із цим, MCE-T визначає термін «пристрій» як фізичний компонент, що обов’язково наділений комунікаційною здатністю, тобто можливістю передавати дані через мережу. За потреби, пристрій може також містити сенсорні та обчислювальні модулі, що дозволяють здійснювати збір, зберігання та попередню обробку даних. Таким чином, акцент міжнародних стандартів ITU-T робиться передусім на інфраструктурній та комунікаційній складовій, залишаючи питання прикладної функціональності (тобто програм і сервісів) другорядними.

Основною ланкою, що поєднує фізичний світ із віртуальним, виступають пристрої, здатні автономно сприймати інформацію з навколишнього середовища, здійснювати її аналіз і передавати дані далі в мережу. Передача може здійснюватися як напряму між пристроями (machine-to-machine), так і через проміжні шлюзи або хмарні платформи.

Для реалізації міжмережевої комунікації в рамках IoT застосовується широкий спектр мережевих технологій, зокрема:

- глобальні мережі (WAN) – наприклад, Інтернет, супутниковий зв'язок;
- локальні мережі (LAN) – для об'єднання пристроїв у межах будівель

або підприємств;

- бездротові самоорганізовувані мережі (WSN) – з динамічною маршрутизацією та адаптивною топологією;

- комірчасті мережі (cellular networks) – такі як 4G/5G для мобільних IoT-платформ.

Ці мережі забезпечують транспорт даних, зібраних сенсорами, до програмних компонентів, де здійснюється подальша обробка, аналіз і прийняття рішень. У зворотному напрямку можливе формування керуючих команд для виконання виконавчими пристроями.

Слід зазначити, що більшість IoT-пристроїв сьогодні оснащені власною обчислювальною логікою, тобто процесорами з вбудованим програмним забезпеченням. Вони мають операційну систему реального часу, сенсорні блоки, системи передачі даних та інтерфейси зв’язку. Це дозволяє здійснювати децентралізовану обробку інформації та зменшує навантаження на центральні вузли мережі.

У контексті комунікаційної взаємодії пристрої дотримуються загального протоколу взаємодії, згідно з яким усі вузли є рівноправними учасниками мережі, мають однаковий доступ до інформаційних ресурсів і функцій надання сервісів. Така архітектура забезпечує високу гнучкість і масштабованість IoT-систем.

З розширенням IoT-інфраструктури постала критична проблема вичерпання IP-адрес, обумовлена обмеженістю адресного простору протоколу IPv4. Вирішенням стало впровадження протоколу IPv6, який передбачає 128-бітну адресу та забезпечує теоретичну можливість унікальної ідентифікації трильйонів пристроїв. Це стало ключовим чинником для подальшого розгортання великих IoT-систем.

Еталонна модель IoT включає чотири горизонтальних рівні, що описують логічну структуру системи – від рівня фізичних пристроїв до рівня сервісів. Ця модель представлена на рисунку 1.3 і слугує основою для архітектурного проєктування сучасних систем Інтернету речей.

Рисунок 1.3 – Еталонна модель IoT

Функціональна архітектура Інтернету речей (IoT) описується багаторівневою моделлю, яка включає як горизонтальні, так і вертикальні компоненти взаємодії. Згідно з рекомендацією ITU-T Y.2060, еталонна модель складається з чотирьох послідовних рівнів: рівень пристроїв, мережевий рівень, рівень обміну даними та рівень застосунків. Рівень пристроїв передбачає використання сенсорних, виконавчих та мікропроцесорних пристроїв, які здійснюють вимірювання, збір, попередню обробку та передачу даних до вищих рівнів архітектури. Ці пристрої можуть здійснювати прямий обмін даними через мережу або працювати через шлюзи, підтримуючи як дротову, так і бездротову передачу інформації. Надзвичайно важливою функцією цього рівня є ефективне управління енергоспоживанням, зокрема активація та деактивація модулів для економії ресурсу.

Мережевий рівень відповідає за забезпечення зв’язності та транспорт даних. Тут реалізуються функції маршрутизації, керування мобільністю, авторизації та автентифікації, а також транспортні механізми для гарантованої доставки інформації від пристроїв до програмних застосунків.

Наступний рівень, що підтримує обмін даними, виконує завдання зі зберігання, агрегації, аналітики та обробки інформації, яка надходить від численних IoT-пристроїв. Він забезпечує узгодження між кількома застосунками, оптимізуючи повторне використання даних і формуючи основу для реалізації сервісів.

Рівень застосунків є верхнім у структурі й передбачає реалізацію функціональності системи відповідно до її спеціалізованого призначення. Цей рівень не підлягає стандартизації, оскільки безпосередньо залежить від особливостей предметної області, в якій реалізується IoT-система, та охоплює широкий спектр прикладних сервісів – від медичних моніторингових систем до розумних міст і промислових об'єктів. Роль шлюзів у цій архітектурі полягає в підтримці гетерогенності інтерфейсів. Вони забезпечують взаємодію між пристроями, які використовують різні протоколи комунікації, з мережами передачі даних. Крім того, шлюзи виконують протокольну конверсію, якщо між пристроєм і мережею немає прямої сумісності, підтримуючи широкий спектр технологій, таких як CAN, ZigBee, Wi-Fi, Bluetooth, DSL, LTE, а також мобільні мережі 2G–5G.

Уся структура доповнюється двома вертикальними рівнями – управління та безпеки. Рівень управління охоплює функції діагностики, моніторингу, конфігурування компонентів, а також підтримки стабільності й продуктивності мережевої інфраструктури. Рівень безпеки, своєю чергою, інтегрується на всіх горизонтальних рівнях і виконує завдання з автентифікації, шифрування, захисту даних, забезпечення цілісності та конфіденційності. На рівні застосунків реалізується захист від шкідливого програмного забезпечення, на мережевому – контроль доступу, а на рівні пристроїв – захист фізичного доступу та цифрових ідентифікаторів.

Функціональна модель IoT-A, яка є поглибленим варіантом архітектури IoT, базується на тій самій ідеї багаторівневої побудови, але вводить додаткові взаємозв'язки. Взаємодія в цій моделі відбувається через рівень комунікацій, який поєднує фізичні пристрої з IoT-сервісами. Сервіси, у свою

чергу, взаємодіють з рівнем організації сервісів, що відповідає за агрегацію, доступність і логіку виклику функцій. Далі – рівень віртуалізації сутностей і управління бізнес-процесами IoT, який дозволяє сформувати інтелектуальну поведінку системи. Застосунки функціонують на основі цього рівня, обслуговуючи кінцеві потреби користувача. Вертикальні рівні безпеки та управління інтегруються в усі процеси та є невід'ємною частиною кожної компоненти.

У моделі IoT-A розрізняють мережі з обмеженнями та без них. Мережі без обмежень мають високу пропускну здатність і використовуються для передачі великих обсягів даних із низькою затримкою, подібно до традиційного Інтернету. Натомість мережі з обмеженнями характеризуються низькою швидкістю передачі – до 1 Мбіт/с – та високим рівнем затримок. У таких мережах використовуються енергоефективні технології на базі стандартів IEEE 802.15.4, що дозволяє пристроям працювати тривалий час у автономному режимі за рахунок низького енергоспоживання. Порівняно з класичною моделлю OSI, архітектура IoT має істотні відмінності в аспектах продуктивності та призначення окремих рівнів, оскільки вона спеціалізується на обробці та транспортуванні дрібних пакетів даних у розподілених, часто обмежених за ресурсами, середовищах.

1.2 Класифікація архітектури IoT

Інтернет речей, як концепція наступного етапу розвитку глобальних мереж, демонструє архітектурну спорідненість із мережею наступного покоління (NGN), що зумовлено їхнім спільним прагненням до гнучкої, масштабованої та сервісно-орієнтованої інфраструктури. Обидві архітектури ґрунтуються на багаторівневій моделі, у якій реалізуються ключові функції взаємодії між користувачами, пристроями, обчислювальними потужностями та прикладними сервісами. У випадку Інтернету речей ця модель охоплює набір інтегрованих технологічних рішень, які забезпечують не лише збір і

передавання даних, але й їх інтелектуальну обробку, інтерпретацію та управління відповідно до конкретних функціональних завдань.

Кожен рівень архітектури IoT, починаючи від фізичних пристроїв і завершуючи додатками кінцевого користувача, базується на різних інформаційно-комунікаційних технологіях, які забезпечують відповідні функції взаємодії, обробки та керування. Таким чином, нижчий рівень, пов’язаний із фізичними пристроями, базується на технологіях сенсорного збору даних, вбудованих системах та мережах ближнього радіусу дії, які дозволяють створювати локальні вузли збору інформації. У той час як рівні вищого порядку інтегрують хмарні обчислення, великі бази даних, алгоритми машинного навчання та штучного інтелекту, що забезпечують можливості масштабованого аналізу, автоматизованого прийняття рішень і адаптації до змін у середовищі.

Важливо підкреслити, що кожна технологічна складова, задіяна в архітектурі IoT, виконує не ізольовану, а взаємопов’язану роль, формуючи цілісну екосистему. Передача інформації від сенсорів до аналітичних модулів, далі – до логіки прийняття рішень та акторів, які реалізують реакцію системи, є безперервним і багатокроковим процесом. Завдяки цьому забезпечується не лише оперативність і надійність функціонування, а й можливість еволюційного розвитку системи через оновлення її окремих компонентів без порушення загальної структури.

Загалом, архітектура Інтернету речей є глибоко технологічно насиченою і гетерогенною, що зумовлює необхідність комплексного підходу до її проєктування. Рисунок 1.4 наочно демонструє, як різні технологічні елементи, включаючи апаратне забезпечення, програмні сервіси, засоби комунікації та аналітичні інструменти, інтегруються у відповідні шари IoT-архітектури. Такий підхід дозволяє не лише реалізувати широке коло прикладних сценаріїв, а й формувати адаптивну та стійку до збоїв систему, яка відповідає вимогам цифрової трансформації суспільства.

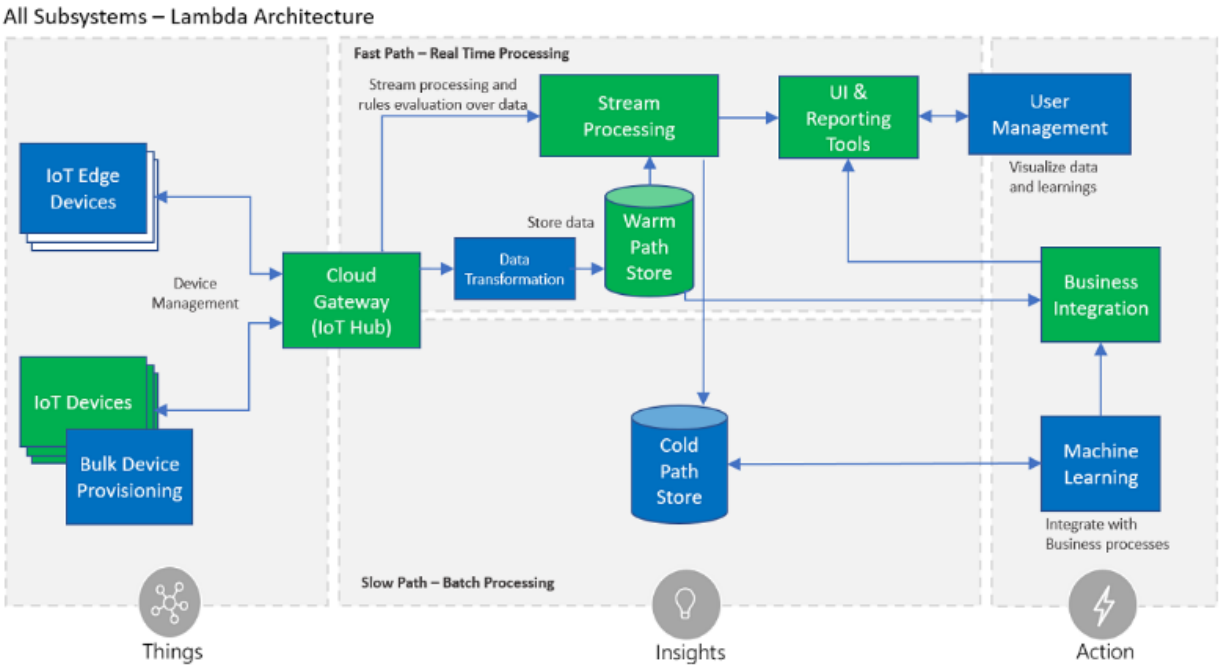

Рисунок 1.4 – Архітектура IoT

Нижній рівень архітектури Інтернету речей репрезентовано сенсорними компонентами, що забезпечують перетворення параметрів навколишнього середовища у цифрові сигнали, придатні для обробки, зберігання та передавання мережею. Саме тут формується базова основа IoT-інфраструктури – «розумні» об'єкти (smart-об'єкти), інтегровані з датчиками й сенсорами, які виступають своєрідним містком між фізичним і цифровим світами. Основною функцією сенсорів є реєстрація змін параметрів довкілля та їх оцифрування, що дозволяє створювати достовірну картину поточного стану об'єкта або середовища у режимі реального часу.

Сенсори, залежно від сфери застосування, можуть бути орієнтовані на фіксацію температурних показників, рівня кислотності (pH), атмосферного тиску, географічного розташування, швидкості переміщення, вологості, концентрації газів або інших фізико-хімічних характеристик середовища. Їх різноманіття зумовлює широку класифікацію відповідно до функціонального призначення: сенсори екологічного моніторингу, біосенсори для медичних застосунків, сенсори для побутової автоматизації або транспортної інфраструктури тощо. Кожен із цих типів пристроїв має обмежені апаратні

ресурси, зокрема обсяг енергонезалежної пам’яті, що слугує для тимчасового буферного зберігання результатів вимірювання.

Для забезпечення безперебійної передачі даних сенсори найчастіше підключаються до шлюзових пристроїв, які виконують роль локальних брокерів у комунікаційній інфраструктурі IoT. Комунікація між сенсорами та шлюзами реалізується через різні мережеві технології ближнього радіусу дії, зокрема Ethernet, Wi-Fi, Bluetooth, ZigBee, PAN або UWB. Шлюзи, в свою чергу, здійснюють маршрутизацію, агрегацію та початкову фільтрацію даних, а також виконують функцію протокольної трансляції для взаємодії з хмарними платформами.

Разом із тим, у певних випадках сенсори можуть функціонувати автономно без участі шлюзових пристроїв, здійснюючи безпосередній зв’язок із глобальними мережами передачі даних. Такий підхід можливий завдяки підтримці стандартів мобільного зв’язку, як-от GSM, GPRS, 3G/4G або LTE, що дозволяє інтегрувати сенсори у великомасштабні IoT-системи з високим ступенем мобільності та динаміки.

Особливої уваги заслуговує концепція бездротових сенсорних мереж (WSN), які орієнтовані на застосування пристроїв із мінімальним енергоспоживанням та обмеженою пропускною здатністю. Ці мережі оптимізовані для ситуацій, де відсутня необхідність у високій швидкості передавання даних, але важлива стабільність роботи пристроїв упродовж тривалого часу, навіть у складних умовах або на великих територіях. Завдяки використанню енергоощадних протоколів взаємодії WSN забезпечують ефективну та масштабовану інфраструктуру для збору польових даних у таких сферах, як агромоніторинг, управління природними ресурсами або індустріальні системи контролю.

Функціонування рівня шлюзів та мереж в архітектурі Інтернету речей відіграє ключову роль у забезпеченні ефективного передавання даних, що генеруються численними сенсорними пристроями. Зі зростанням кількості smart-об'єктів, які постійно створюють потоки інформації, питання

надійності, пропускної спроможності та стійкості транспортної інфраструктури стають визначальними у проєктуванні розподілених IoT-систем. Цей рівень виступає основним середовищем транспортування інформаційних потоків та відповідає за доставку повідомлень від сенсорного рівня до обчислювальних, аналітичних і прикладних модулів системи.

Мережева інфраструктура на цьому рівні може бути реалізована як на базі дротових технологій (Ethernet, xDSL, оптоволоконні мережі), так і з використанням бездротових засобів передачі даних (Wi-Fi, LTE, 5G, LoRaWAN, NB-IoT тощо). Вибір технології залежить від особливостей конкретного сценарію застосування, географічних умов, вимог до енергоспоживання, швидкості передачі та вартості впровадження. При цьому найважливішим завданням залишається забезпечення гарантованої якості обслуговування (QoS) при роботі з великою кількістю трафіку, що часто характеризується фрагментарністю, короткими пакетами та різнорідністю за критичністю.

Суттєвою характеристикою мережі Інтернету речей є її гетерогенність, яка означає необхідність інтеграції численних технологій і протоколів зв’язку в єдину взаємодіючу систему. Така гетерогенна конфігурація охоплює пристрої, що функціонують за різними стандартами, з різною швидкістю, частотним діапазоном, протокольним стеком і енергетичними характеристиками. Вона передбачає наявність шлюзів, які виконують функцію адаптерів між підсистемами, реалізують конверсію протоколів, здійснюють шифрування, маршрутизацію, кешування та агрегацію даних. Завдяки такій архітектурі забезпечується уніфіковане середовище, в якому можуть функціонувати пристрої будь-яких виробників і типів, не втрачаючи здатності до сумісної взаємодії.

Конвергентна модель побудови мережі передбачає об’єднання усіх типів комунікаційних каналів у єдину платформу, що дозволяє підвищити адаптивність системи до змін середовища, зменшити затримки передачі, оптимізувати витрати ресурсів і забезпечити безперебійну доставку критично

важливих даних. Шлюзи в цій моделі виступають не лише комунікаційними вузлами, а й засобами забезпечення безпеки, контролю доступу та конфіденційності переданих повідомлень. Завдяки цьому IoT-мережі здатні забезпечити масштабованість, гнучкість та незалежність хостів у використанні ресурсів мережевої інфраструктури.

Таким чином, рівень шлюзів та мереж є ключовою ланкою у структурі Інтернету речей, яка формує надійний канал взаємодії між фізичними пристроями та цифровими сервісами, забезпечуючи при цьому високий рівень продуктивності, захищеності та адаптивності до нових технологічних викликів.

Рівень керування в архітектурі Інтернету речей відіграє критично важливу роль, оскільки об’єднує комплекс інформаційних сервісів, орієнтованих на підтримку автоматизованого функціонування як технологічних, так і управлінських процесів у системі. Цей рівень виконує функцію інтелектуального ядра системи, що забезпечує узгоджену взаємодію між прикладними модулями, мережевими елементами та користувацькими інтерфейсами.

Основною метою керівного рівня є організація безперервного циклу обробки інформації – від збору первинних даних до ухвалення оптимальних управлінських рішень на основі аналітичної оцінки. У цьому контексті реалізуються такі функціональні блоки, як забезпечення операційної підтримки життєдіяльності системи, контроль виконання бізнес-завдань, здійснення аналітики на основі статистичних спостережень, застосування алгоритмів штучного інтелекту для розпізнавання закономірностей у великих обсягах даних, обробка природної мови та тексту, прогнозування динамічних змін параметрів на основі часових рядів, організація масштабованого зберігання даних, а також впровадження стратегій інформаційної безпеки, які охоплюють як шифрування, так і контроль доступу, ідентифікацію та протидію вторгненням.

Крім того, на рівні керування реалізуються системи управління бізнес-

процесами, що передбачає формалізацію логіки поведінки організаційних структур, моніторинг продуктивності, реагування на відхилення, а також адаптацію бізнес-правил відповідно до зміни зовнішніх або внутрішніх умов функціонування. Таким чином, рівень керування виступає ключовим компонентом IoT-систем, забезпечуючи не лише стабільну роботу технічної інфраструктури, а й стратегічне планування, інтелектуалізацію прийняття рішень та підвищення загальної ефективності автоматизованих систем.

Рівень додатків в архітектурі Інтернету речей являє собою функціональну надбудову, яка втілює прикладні рішення відповідно до конкретних завдань тієї чи іншої галузі. Він є завершальним етапом вертикальної інтеграції IoT-системи та служить безпосереднім інтерфейсом між кінцевим користувачем і цифровою інфраструктурою. На цьому рівні реалізуються прикладні сервіси, які базуються на зібраних і оброблених даних та спрямовані на підтримку прийняття рішень, автоматизацію процесів або розширення функціональних можливостей існуючих систем.

Специфіка додатків визначається тією сферою, у якій реалізується IoT-рішення. Залежно від галузевої орієнтації такі додатки класифікують як вертикальні або горизонтальні. Вертикальні додатки створюються під конкретні галузі – наприклад, для промислової автоматизації, сільського господарства, енергетики, охорони здоров’я, транспорту, розумного міста або екологічного моніторингу. Їхні функції зазвичай тісно інтегровані з особливостями певного виробничого або управлінського процесу, враховують специфіку взаємодії з фізичним середовищем та потребують вузькоспеціалізованих рішень.

У свою чергу, горизонтальні додатки є універсальнішими, оскільки розробляються для широкого спектра задач, що можуть бути реалізовані в різних галузях без необхідності значного пристосування до особливостей конкретної сфери. Це, зокрема, можуть бути системи управління пристроями, платформи обробки великих даних, інструменти для візуалізації та аналітики, сервіси аутентифікації та авторизації, або інтерфейси управління

користувацьким досвідом. Такі додатки формують функціональне ядро цифрових екосистем, яке легко адаптується до змін архітектури системи або запитів бізнес-середовища.

Таким чином, рівень додатків у системі Інтернету речей є ключовим засобом реалізації її цінності – саме через нього відбувається трансформація зібраних даних на практичні інструменти, що мають безпосереднє прикладне значення для людини, підприємства або суспільства загалом.

1.3 Підключення вузлів в сенсорній мережі

Одним із ключових параметрів, який слід враховувати при виборі архітектури сенсорної мережі, є тип її організації – дротовий або бездротовий. У контексті завдання глобального моніторингу екологічного стану територій, що мають просторову дисперсність, бездротова сенсорна мережа виявляється найбільш доцільною та ефективною альтернативою. Основною перевагою такого підходу є відсутність необхідності в прокладці фізичної інфраструктури, що суттєво знижує витрати на розгортання та розширення системи. Проте одним із головних викликів бездротових мереж є обмежений енергетичний ресурс сенсорних пристроїв, більшість з яких живляться від автономних джерел живлення з обмеженою ємністю. З огляду на складність та високу вартість заміни або підзарядки батарей, особливо у важкодоступних місцевостях, виникає нагальна потреба оптимізувати енергоспоживання.

Для досягнення цієї мети сенсорні пристрої зазвичай виконують лише базову попередню обробку даних, обмежуючи обсяги переданої інформації до мінімуму, необхідного для досягнення поставлених цілей моніторингу. В цьому контексті широкого застосування набули технології, реалізовані на базі стандарту IEEE 802.15.4, зокрема, протоколи ZigBee, що працюють на фізичному та канальному рівнях бездротової передачі даних. Завдяки низькому рівню енергоспоживання та можливості надійної передачі

інформації на відстанях до 75 метрів, ці протоколи стали основою локальних бездротових сенсорних мереж з високою ефективністю та стабільністю. Однією з важливих переваг ZigBee є здатність пристроїв більшу частину часу перебувати в енергозберігаючому (сплячому) режимі, активуючись лише для виконання вимірювання та передачі результатів. Це суттєво подовжує строк служби батарей та зменшує потребу в технічному обслуговуванні.

Крім того, характерною особливістю таких самоорганізованих бездротових мереж є їхня здатність до автоматичної реконфігурації маршрутів у випадку виходу з ладу одного або кількох вузлів. Пристрої в мережі самостійно ініціюють побудову нових маршрутів для збереження безперервності передачі даних до центрального вузла або брокера. Як альтернативу або доповнення до ZigBee в аналогічних завданнях може використовуватись технологія Bluetooth, яка забезпечує обмін інформацією між провідними й веденими пристроями як у синхронному, так і в асинхронному режимах. У синхронному режимі передбачено пряме з'єднання з виділеними тимчасовими слотами, тоді як асинхронна передача даних дозволяє спілкування між одним головним і кількома підлеглими пристроями. Особливої уваги заслуговує специфікація BLE (Bluetooth Low Energy), що є частиною ядра Bluetooth версії 4.0. Завдяки низькому енергоспоживанню та підтримці масштабованості BLE вважається ідеальним варіантом для реалізації сенсорних підсистем у розподілених екологічних мережах моніторингу.

Ще одним перспективним напрямом побудови бездротових сенсорних мереж є використання стандарту IEEE 802.11, більш відомого як Wi-Fi. Цей стандарт забезпечує високу швидкість передачі даних, що може сягати до 108 Мбіт/с, що робить його надзвичайно корисним у випадках, коли необхідно передавати великі обсяги даних у режимі реального часу. Такі мережі особливо ефективні в сценаріях, де важлива швидкодія, наприклад, у відеомоніторингу або у високоточному аналізі складних процесів, що потребують негайної реакції та динамічного аналізу.

Отже, вибір протоколу та архітектури сенсорної мережі залежить від конкретних завдань моніторингу, просторових умов розміщення пристроїв, вимог до енергоефективності, швидкості передачі даних та здатності мережі до самовідновлення і адаптації.

1.4 Способи взаємодії в архітектурі IoT

Для забезпечення ефективної та узгодженої взаємодії між численними автономними пристроями, які можуть мати різні апаратні та програмні інтерфейси, необхідно застосовувати уніфіковані протоколи передачі даних. Саме ці протоколи становлять фундаментальну основу архітектури Інтернету речей, оскільки забезпечують синхронізацію, передачу, обробку та маршрутизацію інформаційних потоків між об’єктами цифрового середовища. В умовах проектування розподіленої екологічної системи моніторингу особливої уваги заслуговує протокол MQTT (Message Queue Telemetry Transport), який нині розглядається як один із найбільш оптимальних і широко застосовуваних у галузі IoT-технологій.

Протокол MQTT вирізняється своєю надзвичайною легкістю, мінімалістичністю структури та відкритістю, що дає змогу безперешкодно інтегрувати його у будь-які типи пристроїв. Він був розроблений із початковою метою забезпечення передачі телеметричних даних у віддалених або географічно ізольованих місцях, де наявна інфраструктура зв’язку є обмеженою, а пропускна здатність каналів передачі даних – критично низькою. Завдяки цій особливості MQTT ідеально підходить для задач, де пріоритетом є компактність даних, надійність доставки і здатність функціонування в умовах нестабільного або інтервального зв’язку.

Однією з ключових переваг MQTT є можливість асинхронного режиму взаємодії, що дозволяє протоколу ефективно працювати навіть при частих розривах зв’язку або в умовах нестабільної мережі. Ця властивість особливо важлива для систем екологічного моніторингу, де сенсорні вузли можуть

бути розміщені у важкодоступних місцевостях – зокрема, у гірських регіонах, болотах, або на віддалених узбережжях – і забезпечувати надсилання телеметричних даних навіть при короткочасному з'єднанні з мережею. MQTT не потребує значного обсягу пам’яті для роботи, що дає змогу використовувати його на пристроях з обмеженими ресурсами, а також забезпечує високу енергоефективність, що критично для автономних систем з живленням від батарей.

Завдяки властивості масштабованості, MQTT також здатний забезпечити ефективну комунікацію в системах з великою кількістю пристроїв, які динамічно додаються або виводяться з експлуатації без порушення загальної логіки функціонування мережі. Це дозволяє проектувати архітектуру системи моніторингу як таку, що може безперешкодно розширюватися залежно від потреб, наприклад, охоплювати нові географічні зони або підключати нові типи сенсорів.

Протокол функціонує на прикладному рівні моделі TCP/IP і за замовчуванням використовує порт 1883 для незахищеного з’єднання. У разі потреби реалізації захищеної комунікації через SSL/TLS передбачено застосування порту 8883. Структура MQTT-повідомлень побудована на принципі фіксованого заголовка, який є обов’язковим компонентом кожного пакета. Окрім цього, структура може містити змінний заголовок та корисне навантаження, присутність яких залежить від типу переданого повідомлення.

У фіксованому заголовку в обов’язковому порядку визначається поле Message Type, яке ідентифікує тип повідомлення – наприклад, запит на підписку, публікація даних, підтвердження доставки тощо. Цей механізм дозволяє підтримувати високий рівень контролю за обміном даними, забезпечуючи надійність, цілісність та впорядкованість інформаційного трафіку у системах Інтернету речей. З огляду на зазначені властивості, MQTT є оптимальним протоколом для реалізації екологічних, телеметричних та розподілених автоматизованих систем з інтенсивним сенсорним середовищем.

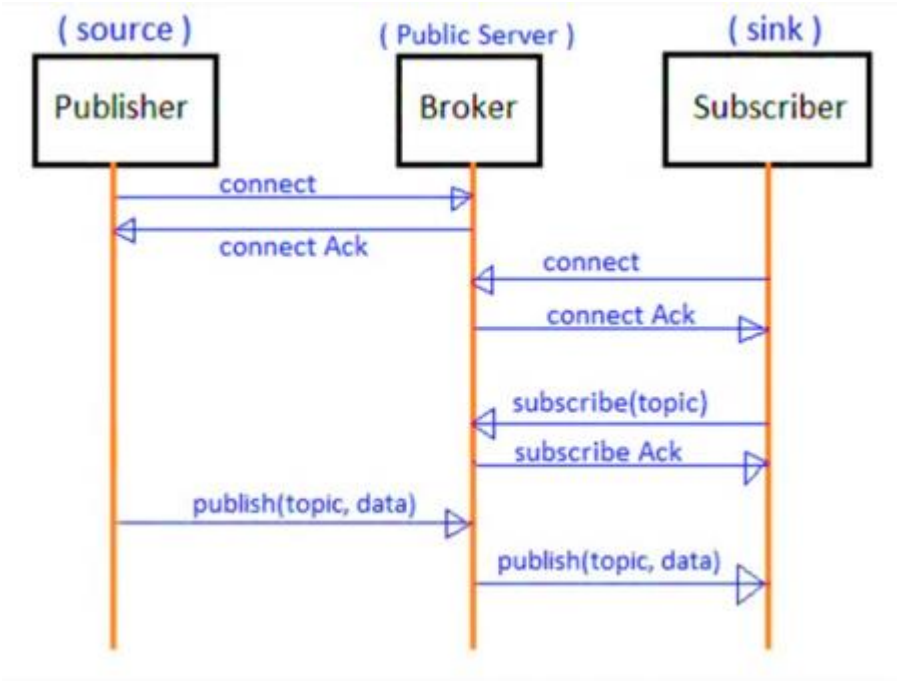

Рисунок 1.5 – Структура фіксованого заголовку MQTT-повідомлення

Протокол MQTT базується на чітко структурованій системі класифікації повідомлень, яка охоплює п’ятнадцять різних типів. Кожен із них виконує специфічну функцію в межах інформаційного обміну між пристроями-учасниками IoT-мережі. Серед ключових повідомлень, що найчастіше використовуються у практичних реалізаціях, можна виокремити повідомлення типу CONNECT, яке ініціює встановлення з’єднання між клієнтом і брокером, SUBSCRIBE – що запускає процедуру підписки на певні теми публікацій, PUBLISH – призначене для передачі даних від пристрою-відправника до брокера, та DISCONNECT – яке сигналізує про завершення сеансу зв’язку.

Кожне повідомлення MQTT має уніфіковану структуру, що починається з фіксованого заголовка. Чотири найстарші біти першого байта цього заголовка виконують функцію спеціальних керуючих прапорців, які надають повідомленням додаткові семантичні ознаки. Прапорець DUP (Duplicate delivery) активується у разі повторної доставки одного й того самого повідомлення. Така ситуація може виникати, коли сенсорне

обладнання або брокер змушені здійснити ретрансляцію даних через збій або непідтверджену доставку, що особливо важливо у випадках гарантованої доставки (QoS ≥ 1). DUP-прапорець активно застосовується у типах повідомлень PUBLISH, SUBSCRIBE, UNSUBSCRIBE та PUBREL – останнє використовується для підтвердження завершення процесу доставки з подальшим дозволом на видалення повідомлення з буфера.

Другим важливим елементом є поле QoS (Quality of Service), яке визначає рівень якості обслуговування з урахуванням бажаної надійності доставки повідомлення. MQTT підтримує три рівні QoS: 0 – доставка без підтвердження (at most once), 1 – з підтвердженням (at least once), 2 – гарантована доставка без дублювання (exactly once). Вибір QoS залежить від критичності даних та параметрів мережевого середовища.

Ще один прапорець – RETAIN – дозволяє брокеру зберігати останнє повідомлення певної тематики, щоб при підключенні нових підписників ця інформація була негайно надана без очікування нових публікацій. Така функціональність надзвичайно корисна для забезпечення синхронізації нових учасників системи з актуальним станом середовища.

У змінному заголовку MQTT-повідомлень розміщуються ідентифікатори, що слугують для унікального визначення джерела повідомлення. Вони також можуть включати параметри аутентифікації, які дають змогу підтвердити легітимність пристрою, що ініціює передачу даних. Це критично важливо з точки зору кібербезпеки у розподілених автоматизованих системах, оскільки наявність відповідних маркерів дозволяє верифікувати кожен інформаційний пакет і запобігти спробам зовнішнього втручання або підміни даних у каналі зв’язку.

Таким чином, архітектура повідомлень у MQTT є гнучкою, розширюваною та придатною для застосування у складних і масштабних IoT-системах, забезпечуючи високий рівень контрольованості та адаптивності телеметричних обмінів.

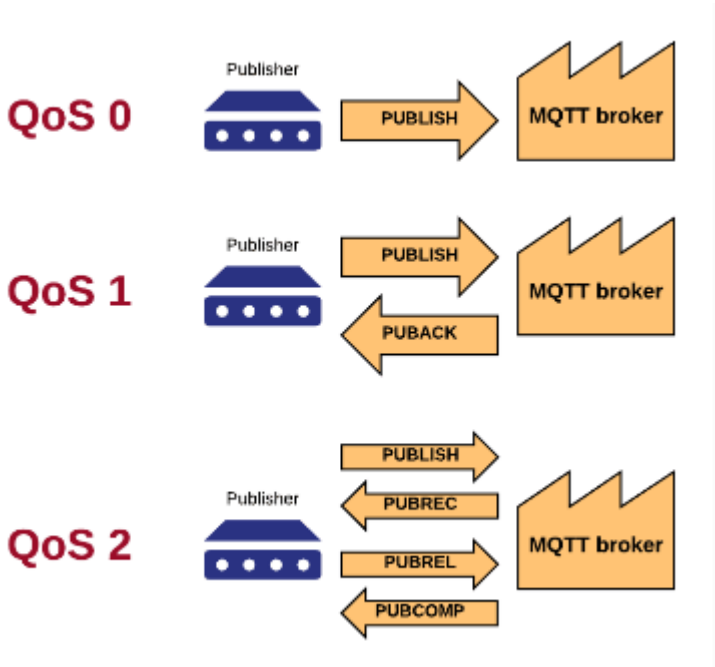

Рисунок 1.6 – Структура змінного заголовка MQTT-повідомлення

У структурі змінного заголовка MQTT-повідомлення, зокрема у випадку повідомлення типу CONNECT, містяться ключові елементи, які забезпечують ідентифікацію та налаштування сеансу зв’язку. Ці елементи включають у себе унікальний ідентифікатор пакета, що дозволяє корелювати його з відповідним клієнтським сеансом, назву протоколу MQTT та його версію, яка визначає набір допустимих функцій і параметрів, а також бітові прапорці, що задають поведінкові особливості вимірювального пристрою під час встановлення з'єднання. Крім того, у цьому заголовку присутні поля, призначені для автентифікації клієнта, такі як Client ID, а також обов’язкові механізми верифікації та безпеки, які реалізуються за допомогою TLS/SSL-з'єднання.

Безпека передачі даних у рамках MQTT-протоколу гарантується багаторівневою системою захисту. Вона охоплює процедуру автентифікації клієнта на стадії встановлення з’єднання (через повідомлення CONNECT), контроль доступу на основі унікального ідентифікатора клієнта (Client ID) та шифрування трафіку за допомогою протоколів захищеного каналу (TLS/SSL), що забезпечує конфіденційність, цілісність і автентичність

переданих даних.

Корисне навантаження, що передається у тілі MQTT-повідомлення, міститься в так званому «додатку». Розмір цього інформаційного блоку обчислюється як різниця між значенням поля Remaining Length та довжиною змінного заголовка. Такий підхід дозволяє точно визначити обсяг даних, що підлягає подальшій обробці або зберіганню.

Однак побудова ефективної системи моніторингу навколишнього середовища на основі IoT не може обмежуватись лише етапом комунікації між вимірювальними пристроями та брокером. Реалізація повноцінного рішення передбачає архітектурну побудову, у якій поєднуються обчислювально обмежені пристрої з високопродуктивними хмарними сервісами. З одного боку, система включає велику кількість автономних сенсорних пристроїв та брокерів з обмеженим енергоспоживанням, швидкою реакцією на події та невисокими обчислювальними можливостями. З іншого боку, використовується масштабоване хмарне середовище, яке надає необхідні ресурси для довготривалого зберігання, класифікації та глибинної обробки зібраних даних. Саме хмарна частина системи (Cloud Backend) не лише виконує роль сховища, а й забезпечує аналітичні функції, включаючи інструменти машинного навчання для автоматизованої інтерпретації тригерів і прийняття рішень на основі виявлених закономірностей.

На рисунку 1.7 представлено схему функціональної взаємодії усіх компонентів у межах IoT-мережі, що розробляється для екологічного моніторингу. Взаємодія починається з рівня Embedded, де розташовані вимірювальні пристрої, що сприймають фізичні параметри середовища. Виявлення змін відбувається через сенсорні компоненти, які генерують аналоговий сигнал. Цей сигнал проходить через аналого-цифровий перетворювач (AtoD), після чого дані опрацьовуються на вбудованому процесорі пристрою. У процесі попередньої обробки інформація доповнюється міткою часу (timestamp) і спеціальним тегом (Tag), що слугує для класифікації події, встановлення її контексту та формування пакету

даних для подальшої передачі.

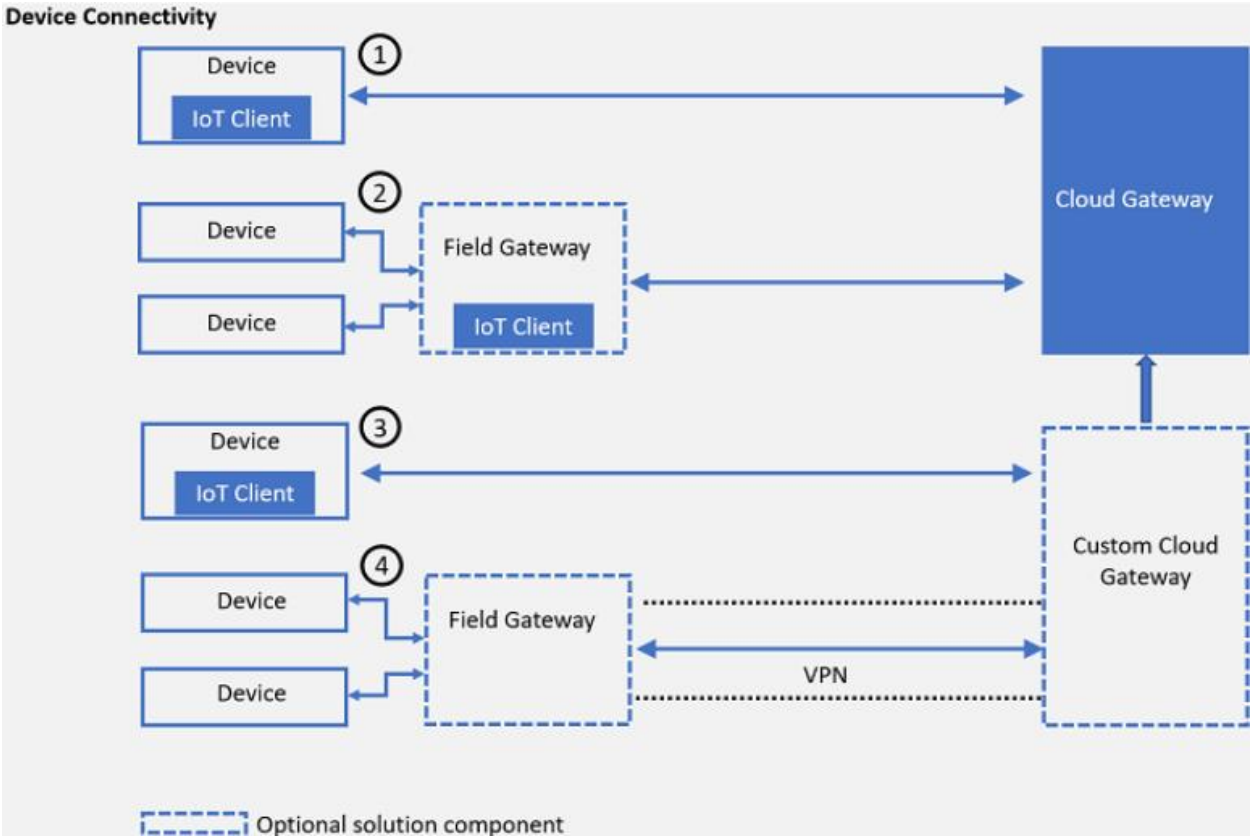

Рисунок 1.7 – Архітектура розгорнутого IoT рішення

Цей ланцюг дій, починаючи з реєстрації змін у середовищі й завершуючи передачею у хмарну інфраструктуру, ілюструє загальні принципи роботи розподіленої автоматизованої системи моніторингу довкілля, реалізованої на основі протоколу MQTT та архітектури IoT.

У структурі функціональної архітектури розподіленої системи моніторингу навколишнього середовища, побудованої на основі технологій Інтернету речей, ключову роль на рівні маршрутизації виконує логічна зв’язка між брокерами даних та маршрутизуючим кластером. Цей рівень забезпечує інтелектуальне сортування, агрегування та первинне семантичне структурування інформаційних потоків, які надходять від численних сенсорних пристроїв у вигляді MQTT-пакетів. Суть функціонування цієї ланки полягає у класифікації пакетів за попередньо визначеними тегами, які відіграють роль маркерів типових подій або вимірювань.

Маршрутизуючий кластер, як функціональна частина системи, організований у вигляді децентралізованої сукупності вузлів, кожен із яких спеціалізується на обробці даних певного типу або з певним набором атрибутів. Такий підхід дозволяє досягти високого ступеня узгодженості (консистентності) у процесі обробки, що, своєю чергою, позитивно позначається на загальній надійності та відмовостійкості як окремих маршрутизаторів, так і кластерної структури загалом. Диверсифікація потоків у межах кластера за допомогою вузькоспеціалізованих модулів дає змогу запобігти перевантаженню окремих елементів системи, забезпечити балансування навантаження та пришвидшити загальну обробку інформації у реальному часі.

Після завершення процедури маршрутизації та базової агрегації, оброблені дані передаються на рівень бекенд-системи, яка є ядром програмної частини архітектури. Саме на цьому рівні виконується вторинна обробка інформації, її трансформація у користувацький інтерфейсний формат та інтеграція у відповідні сервіси для візуалізації, зберігання або прийняття управлінських рішень. У межах backend-модуля реалізовано аналітичний блок, до складу якого входять алгоритмічні компоненти для виявлення закономірностей, трендів та відхилень у структурі надходжуваних даних. Особливу увагу приділено впровадженню засобів штучного інтелекту, включно з алгоритмами виявлення патернів та аномалій, які ґрунтуються на аналізі поточних і накопичених історичних даних.

Паралельно із цим, використовуються методи машинного навчання, які дозволяють будувати прогностичні моделі та моделі реакції системи на основі вхідних параметрів навколишнього середовища. Уся система працює з орієнтацією на масштабованість, адаптивність та високий рівень автоматизації аналізу, що забезпечує можливість розгортання подібної інфраструктури на великих територіях та в умовах обмежених комунікаційних ресурсів. Перед переходом до аналізу патернів і підготовки системи до прийняття управлінських рішень, необхідно детально осмислити

механізми функціонування маршрутизуючого кластера, який формує ключову комутаційну ланку між рівнями брокеризації та інтелектуальної обробки даних.

2 МЕТОД ОБРОБКИ ТА ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ В ІОТ

Проектування розподіленої системи моніторингу довкілля в середовищі Інтернету речей передбачає не лише забезпечення якісного збору даних, а й впровадження ефективних механізмів діагностики функціонального стану сенсорного обладнання. Надійність і тривалість експлуатації вимірювальних пристроїв є критично важливими чинниками, від яких залежить точність спостережень та своєчасність реагування на екологічні зміни. Вихід окремих сенсорів із ладу чи їх часткова деградація може суттєво спотворити картину досліджуваного середовища, тому підтримка їхньої працездатності упродовж життєвого циклу системи становить один із ключових пріоритетів.

У цьому контексті особливе значення набуває впровадження функцій поточної діагностики та оцінювання технічного стану пристроїв у реальному часі. Такий підхід передбачає збір діагностичних параметрів, їх обробку, виявлення закономірностей у поведінці технічних характеристик та формування обґрунтованих прогнозів щодо ризику відмови або зниження ефективності функціонування обладнання. Прогнозні оцінки, що базуються на аналізі динаміки змін у часових рядах технічних параметрів, дозволяють не лише оперативно виявляти тенденції до зношення чи збоїв, але й планувати профілактичні заходи, спрямовані на відновлення повної функціональності сенсорної мережі.

Для забезпечення високої точності таких прогнозів необхідно задіяти аналітичні моделі, побудовані на базі експертних знань, а також на результатах багаторічного моніторингу та моделювання процесів деградації. Інформація, накопичена під час експлуатації системи, слугує основою для ідентифікації критичних змін у поведінці пристроїв і дозволяє створювати навчальні вибірки для алгоритмів передиктивної аналітики.

Застосування предиктивного підходу в діагностиці означає

використання систем, здатних генерувати прогнозні оцінки стану обладнання з високою достовірністю, ґрунтуючись на історичних даних і актуальних спостереженнях. Ці системи мають бути здатні адаптуватися до неоднорідності вхідних даних, масштабуватися відповідно до розміру мережі та обробляти великий обсяг діагностичних повідомлень з високою швидкістю.

Таким чином, на етапі проектування системи діагностики доцільно здійснити ґрунтовний аналіз існуючих підходів до побудови інформаційно-діагностичних структур, обрати ефективні математичні моделі, що дозволяють оцінювати стан технологічного обладнання за часовими рядами параметрів, а також впровадити засоби підтримки прийняття рішень, які забезпечать точне прогнозування та своєчасне планування технічного обслуговування сенсорних пристроїв у рамках комплексної IoT-інфраструктури.

2.1 Аналіз структур систем обробки діагностичної інформації у IoT

У контексті швидкого зростання складності та масштабу систем IoT, зокрема у критично важливих галузях моніторингу довкілля, промисловості, транспорту та охорони здоров’я, надзвичайно актуальною стає задача впровадження ефективних структур обробки діагностичної інформації. Така інформація формується у процесі функціонування розподілених сенсорних систем, і її якісна обробка є необхідною умовою підтримки стабільності, безперервності та безпеки всього технологічного комплексу.

Типові структури систем обробки діагностичних даних у мережах IoT зазвичай включають декілька ієрархічних рівнів обробки: рівень вимірювальних пристроїв, рівень попередньої агрегації, мережевий рівень маршрутизації, рівень інтелектуального аналізу, а також рівень збереження та візуалізації результатів. Кожен із цих рівнів виконує окремі функції, але у комплексі формує цілісну архітектуру, яка забезпечує оперативне виявлення

відхилень, формування прогнозів технічного стану та генерацію рекомендацій щодо сервісного обслуговування.

На найнижчому рівні здійснюється первинна діагностика, яка базується на аналізі локальних параметрів сенсорів, таких як температура мікросхеми, рівень залишкової ємності батареї, стабільність зв’язку або частота внутрішніх збоїв. Ці дані обробляються вбудованими мікроконтролерами сенсорних вузлів і формуються у вигляді пакетів діагностичної інформації.

Далі ця інформація передається на рівень шлюзів, які виконують роль локальних брокерів, здійснюючи агрегацію діагностичних повідомлень від багатьох сенсорів. У таких системах можуть використовуватись протоколи MQTT або CoAP, які дозволяють працювати в умовах обмежених мережевих ресурсів. Крім того, на цьому етапі можуть бути реалізовані базові правила фільтрації, нормалізації та перетворення даних у уніфікований формат для подальшої обробки.

На рівні маршрутизуючого кластера здійснюється класифікація діагностичних повідомлень за типами несправностей, джерелами виникнення або пріоритетами обробки. Розподіл обробки між різними вузлами на основі типів тегів дозволяє підвищити масштабованість та забезпечити балансування навантаження в реальному часі.

Центральним елементом обробки діагностичної інформації є backend-рівень, де застосовуються методи інтелектуального аналізу даних, зокрема алгоритми машинного навчання, нейронні мережі, моделі прогнозування на часових рядах, байєсівські моделі, а також нечітка логіка. Саме тут реалізується предиктивна аналітика – здатність виявляти приховані патерни деградації на основі накопичених даних, що дозволяє своєчасно визначити потребу в сервісному втручанні.

Також важливою складовою є модуль збереження та візуалізації діагностичних даних, який забезпечує доступ до інформації для операторів та адміністраторів систем. Цей модуль має підтримувати сучасні засоби інтерактивної візуалізації, можливість автоматичного генерування звітів, а

також інтерфейси REST API для інтеграції з іншими корпоративними або виробничими інформаційними системами.

Таким чином, типові структури обробки діагностичної інформації в IoT-системах орієнтовані на багаторівневу децентралізовану архітектуру з інтелектуальними можливостями на кожному етапі обробки, що дозволяє досягти високої ефективності моніторингу, адаптивності до змінного середовища, зниження навантаження на центральні вузли та забезпечення високої надійності функціонування всієї системи. Це дає змогу своєчасно реагувати на потенційні загрози, мінімізувати простої обладнання та знижувати загальні експлуатаційні витрати.

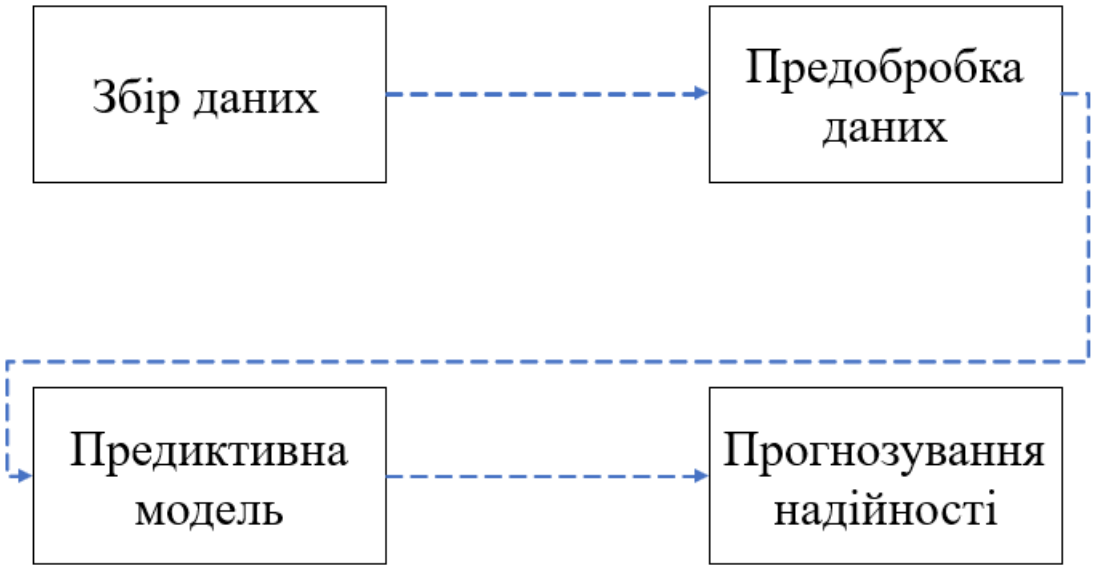

Рисунок 2.1 – Процес обробки даних в системі предиктивної аналітики

У підсумку, розроблений метод дозволяє реалізувати цілісний підхід до побудови системи моніторингу мережевого трафіку, що ґрунтується на комплексній взаємодії компонентів перехоплення, транспортного середовища, інтелектуального аналізу та інтеграції з існуючими платформами керування інформаційною безпекою. Завдяки поєднанню цих елементів, забезпечується не лише висока ефективність виявлення аномалій

та потенційних загроз, а й можливість адаптивного реагування в режимі реального часу. Запропоноване рішення відповідає актуальним викликам корпоративної кібербезпеки, забезпечуючи масштабованість, узгодженість з архітектурними стандартами та інтеграцію у структури SIEM-рішень, що дозволяє гармонійно впроваджувати його в інформаційно-телекомунікаційні інфраструктури сучасного підприємства.

У типовій системі предиктивної аналітики реалізується багатоступенева послідовність обробки діагностичної інформації, яка починається з імпорту даних про технічний стан пристроїв до відповідного аналітичного середовища. На початковому етапі здійснюється підготовка та трансформація цих даних, що включає процедури очищення, фільтрації, нормалізації та адаптації до форматів, необхідних для подальшої обробки. Після попередньої обробки відбувається кластеризація отриманої інформації з метою виявлення прихованих закономірностей, структурування множини вхідних показників за схожими патернами та забезпечення більш точного моделювання. Далі кластеризовані дані надходять до ядра прогнозної моделі, в основі якої закладені алгоритми машинного навчання та елементи інтелектуального аналізу. Модель, працюючи з історично накопиченою інформацією, здійснює побудову трендових залежностей для ключових параметрів, що відображають технічний стан сенсорних компонентів, після чого виконує розрахунок прогнозованих значень у контексті часових рядів.

Ефективність таких прогнозів безпосередньо визначається якістю архітектурної реалізації системи предиктивної аналітики, гнучкістю її алгоритмічного ядра, здатністю адаптуватися до зміни вхідного потоку та врахуванням складної динаміки технічних об'єктів. Варто зазначити, що діагностичні дані, що надходять у реальному часі з численних сенсорів, відзначаються значною неоднорідністю, різноманітністю структур, форм представлення та способів зберігання. Саме тому перед передачею до прогнозної моделі ці дані повинні бути приведені до дискретизованої форми з урахуванням часових інтервалів, що забезпечує баланс між точністю

обчислень і швидкістю реакції системи.

Надходження значного обсягу потокових даних потребує попереднього фільтрування для усунення шумів, перешкод і похибок вимірювання. Це дозволяє зберегти достовірність вхідного дата-сету, який виступає базою для формування надійних математичних моделей. Особливу увагу також приділяють рівномірному масштабуванню, стандартизації та нормалізації вхідного потоку, оскільки будь-яке порушення цих процедур може призвести до зниження ефективності прогностичних алгоритмів. У разі, якщо базових засобів підготовки виявляється недостатньо, до процесу можуть бути долучені спеціалізовані підсистеми, що здійснюють поглиблену обробку даних з використанням складніших методів адаптації та апроксимації.

Таким чином, логічна та функціональна структура системи предиктивної аналітики передбачає наявність інтегрованої архітектури, яка поєднує в собі механізми підготовки, фільтрації, кластеризації, прогнозування та відображення даних про технічний стан сенсорної інфраструктури. Це підтверджується схемами, наведеними на відповідних рисунках, де чітко позначено інформаційні та функціональні потоки, що забезпечують цілісний підхід до моніторингу, діагностики та запобігання потенційним збоям у розподіленій сенсорній мережі.

Поточні дані, отримані від датчиків, інтегрованих у вимірювальні пристрої, передаються до спеціалізованих інформаційних систем, що забезпечують функціонування в реальному часі ключових підсистем збору, обробки, візуалізації та архівування інформації, яка характеризує стан об'єкта моніторингу або керування. Ці системи формують централізований інформаційний вузол, що забезпечує оперативний доступ до актуальних даних для осіб, уповноважених приймати рішення стосовно технічного обслуговування, усунення несправностей або оптимізації параметрів функціонування елементів мережі. У режимі реального часу на вхід аналітичного контуру надходить потік інформації, який ще не пройшов повного циклу формалізації, аналізу або верифікації, й тому розглядається як

попередньо оброблені дані. Саме ця інформація, що має оперативну природу, використовується для первинного аналізу ситуацій та є основою для прогнозного моделювання.

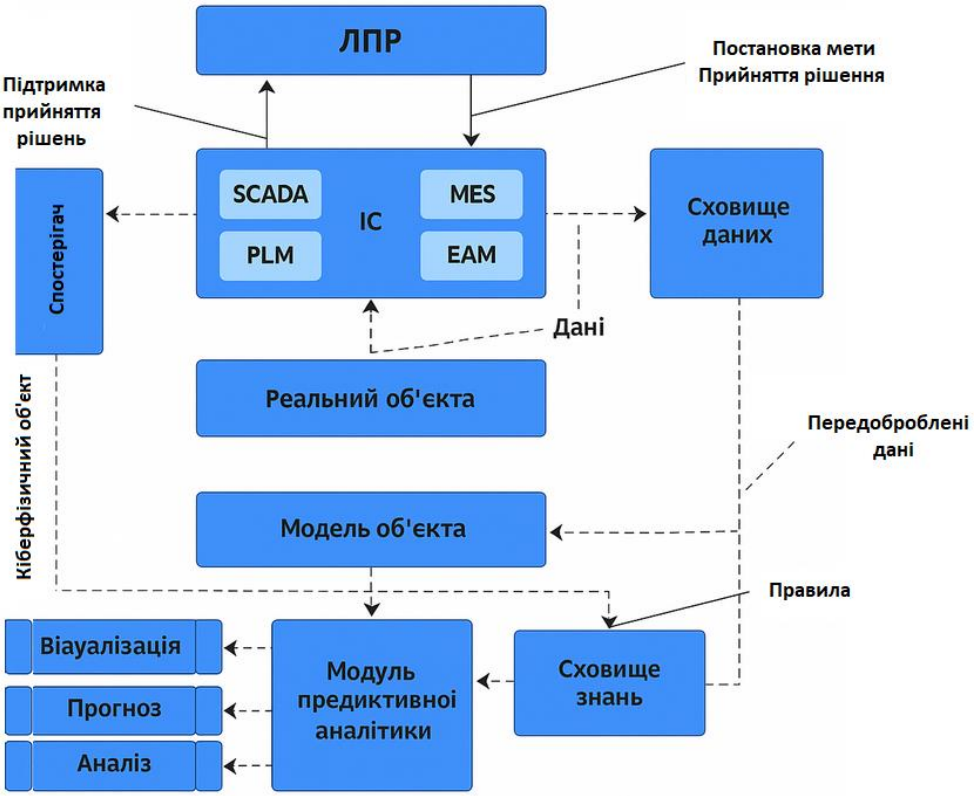

Рисунок 2.2 – Структура типової системи обробки діагностичної інформації

Натомість результати, отримані внаслідок розрахунків за допомогою верифікованої діагностичної моделі об’єкта спостереження, характеризуються вищим ступенем структурованості та аналітичної цінності. Ці дані набувають статусу обґрунтованих прогнозних параметрів і передаються до ядра системи предиктивної аналітики для глибшого аналізу, формування трендів, оцінки ризиків і побудови сценаріїв реагування на ймовірні технічні відмови. Таким чином, структура обробки передбачає багаторівневу фільтрацію, оцінку й послідовну інтерпретацію потоків даних – від сирих сенсорних вимірювань до стратегічно значущих прогнозів, що підтримують прийняття рішень у контексті надійності та довговічності функціонування системи.

2.2 Аналіз існуючих моделей та методів

Найважливішим етапом у межах системи предиктивної аналітики є виявлення аномалій, що проявляються як відхилення значень діагностичних параметрів від усталених норм, які характерні для стабільного функціонування технічної системи. Такі відхилення можуть полягати у зміні тривалості окремих фаз експлуатаційного циклу або у перевищенні гранично допустимих значень характеристик, що свідчать про нестабільну чи аварійну поведінку пристрою. Імовірнісне моделювання типових сценаріїв дозволяє визначити ситуації, в яких певні елементи вимірювального обладнання виходять із ладу або функціонують у нестандартних режимах.

Як приклад, розглядається багатовимірний часовий ряд $X = \{x_1, x_2, ..., xL\}$, де кожен елемент xt представляє собою m-вимірний вектор, що відображає стан системи в момент часу t. Частина компонентів вектора формується на основі алгоритмів керування та визначає вплив керуючих сигналів, інша частина – показники реакції системи на зовнішні впливи. Кожному часовому моменту t ставиться у відповідність значення a_t, яке характеризує рівень аномальності й дозволяє визначити нетиповість спостережуваних даних у даний момент. Слід зазначити, що навчальна вибірка, яка використовується для побудови моделей, не повинна містити аномальних значень, адже вони за своєю природою є невизначеними та не підлягають об’єднанню в однорідні кластери, що ускладнює процес класифікації.

Різна довжина часових рядів або кількість сенсорних компонентів не впливає на цілісність системи, якщо функціональність пристроїв залишається незмінною. Для зменшення обчислювальної складності довгі ряди можуть бути фрагментовані на менші підпослідовності. Аномалії виявляються шляхом застосування набору математичних методів, які базуються на теоретичних принципах діагностики та класифікації. До таких методів належать підходи класифікації, кластеризації, статистичного аналізу,

використання методу найближчих сусідів, спектральні методи та гібридні рішення.

Методи класифікації базуються на припущенні, що коректна робота системи описується певними класами. Якщо об'єкт не відповідає жодному з цих класів, він розцінюється як аномалія. Класифікатори навчаються на маркованих даних, що дозволяє формувати внутрішні правила для віднесення нових спостережень до відомих класів або визначення їх як відхилень. Кластеризаційні методи (рисунок 2.3) групують подібні об’єкти без попередньої інформації про нормальні та аномальні стани. Аномалії виявляються як ті елементи, які не потрапляють до жодного з кластерів, або значно віддалені від їх центрів, або формують невеликі, ізольовані кластери.

Статистичні підходи ґрунтуються на порівнянні очікуваної поведінки системи, описаної аналітичною моделлю, з фактичними даними. Виявлена розбіжність інтерпретується як аномальна поведінка. Метод найближчих сусідів засновується на оцінюванні схожості між елементами за допомогою метрик, таких як евклідова відстань. Якщо певний елемент суттєво віддалений від своїх найближчих сусідів або перебуває у ділянці з низькою щільністю розподілу, він класифікується як аномальний.

Рисунок 2.3 – Схема запропонованого методу

Спектральні методи використовують аналіз головних компонент або подібні техніки для зменшення розмірності простору ознак, зберігаючи при цьому значущу частину варіативності даних. Вони часто виступають як інструмент попередньої обробки перед застосуванням більш складних аналітичних підходів. Гібридні методи комбінують переваги кількох підходів – наприклад, поєднують класифікацію зі статистичним аналізом або кластеризацію з методом найближчого сусіда – що дозволяє підвищити точність виявлення аномалій та адаптувати систему до специфіки даних.

У більшості випадків вибір конкретного методу залежить від природи задачі, доступних даних, вимог до точності та ресурсних обмежень. Використання як послідовного, так і паралельного застосування декількох методів дозволяє підвищити стійкість системи до помилкових спрацювань і досягти більшої узагальненості виявлення аномальних станів технічних об’єктів. Таким чином, система предиктивної аналітики формує багаторівневу модель оцінки працездатності пристроїв, яка ґрунтується на науково обґрунтованих методах аналізу тимчасових рядів та виявлення відхилень, що вказують на потенційні технічні збої.

2.3 Аналіз сучасних публікацій

Упродовж останніх років питання обробки та аналізу даних в системах Інтернету речей стало одним із ключових у галузях прикладної інформатики, штучного інтелекту та комп’ютерної безпеки. Аналіз наукових джерел свідчить про активний розвиток таких напрямів, як оптимізація обчислювальних процесів на периферії мережі, інтеграція методів машинного навчання для інтелектуального аналізу даних, а також створення механізмів забезпечення конфіденційності в середовищах IoT.

У ґрунтовному огляді, наведеному в джерелі [1], розглянуто загальні принципи побудови архітектури Інтернету речей і виокремлено основні проблеми, пов’язані з аналізом великих потоків даних. Ця публікація стала

підґрунтям для подальших досліджень у сфері обробки інформації, особливо в контексті розподілених обчислень і хмарних рішень.

Дослідження [2] акцентує увагу на практичному використанні методів аналізу даних для управління міською інфраструктурою, включаючи моніторинг сенсорних систем, аналіз трафіку та контроль стану довкілля. У цій роботі широко застосовуються методи кластеризації, нейромережеві підходи та елементи предиктивної аналітики.

Окрему категорію становлять дослідження, присвячені застосуванню штучного інтелекту в середовищах IoT, зокрема глибокого навчання. У праці [3], наприклад, проаналізовано алгоритми класифікації та виявлення аномалій у потоках даних з бездротових сенсорних мереж, що становлять основу для багатьох сучасних рішень Інтернету речей.

Значну частку публікацій також присвячено питанням захисту конфіденційності та інформаційної безпеки. У статті [4] розглянуто ризики витоку персональних даних та досліджено відповідні захисні технології, зокрема псевдонімізацію, анонімізацію та диференційовану конфіденційність. Актуальність цих питань зростає в умовах автоматизованої обробки даних із використанням алгоритмів штучного інтелекту. Автори підкреслюють, що саме аспекти конфіденційності та безпеки залишаються найбільшими викликами для IoT. Попри широке впровадження Інтернету речей у критичних сферах – таких як охорона здоров’я, енергетика, міська інфраструктура – рівень загроз залишається високим через низький ступінь захисту пристроїв, обмежені апаратні ресурси та недостатньо ефективне управління безпекою на різних рівнях архітектури. До ключових загроз відносять несвоєчасні оновлення програмного забезпечення, відсутність надійних протоколів захисту, низьку обізнаність користувачів щодо ризиків порушення приватності, а також неможливість здійснювати повноцінний моніторинг активних пристроїв у реальному часі, що створює численні точки потенційного витоку даних. Унаслідок цього середовища IoT залишаються вразливими до різноманітних кіберзагроз, таких як підміна сертифікатів,

імітація вузлів або перехоплення незашифрованого трафіку. Запропонована архітектура системи має на меті забезпечити ефективний розподіл обчислювальних завдань та захист інформації на кожному етапі її передавання через мережу.

Сучасні джерела, зокрема [5,6], демонструють зростаючий науковий інтерес до поєднання IoT-технологій з алгоритмами машинного навчання, що вимагає нових підходів до зберігання, попередньої обробки, очищення та інтерпретації даних. Автори розглядають синергію між штучним інтелектом і Інтернетом речей як трансформаційний підхід до організації обробки інформації та ухвалення рішень, що дозволяє глибше інтегрувати цифрові технології в життя людини й бізнес-процеси. Водночас, разом із численними перевагами, така інтеграція несе і нові виклики, зокрема у сфері захисту чутливих даних, прозорості прийняття рішень та етичного використання інформації. Саме тому подальші дослідження мають бути спрямовані не лише на вдосконалення алгоритмів оптимізації, а й на розробку моделей безпечного, відповідального та інтерпретованого впровадження штучного інтелекту в середовище IoT.

У цілому, аналіз наукових публікацій засвідчує чітку тенденцію до міждисциплінарного підходу, який поєднує знання з комп’ютерних наук, телекомунікацій, прикладної математики та кібербезпеки. Такий підхід дозволяє створювати не лише ефективні системи обробки даних у мережах Інтернету речей, а й системи, що гарантують захист конфіденційної інформації – одного з ключових чинників формування довіри користувачів до новітніх цифрових технологій.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ МЕТОДУ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

3.1 Програмна реалізація методу та вибір програмних засобів

Розроблений метод базується на застосуванні нейронної мережі для виявлення та прогнозування аномальних станів сенсорних пристроїв у розподіленій системі моніторингу довкілля. Метод забезпечує наступні етапи:

- збір та підготовка даних. Дані вимірювань надходять з IoT-пристроїв, формуючи багатовимірні часові ряди. Здійснюється очищення, нормалізація та дискретизація вхідних даних;

- кластеризація. Вхідні дані кластеризуються за ознаками стану пристроїв для визначення нормального поведінкового патерну.

- навчання моделі. Нейронна мережа типу автоенкодер навчається на нормальних даних. В результаті формується базова модель нормальної поведінки пристроїв;

- детектування аномалій. На етапі експлуатації модель аналізує нові дані та оцінює рівень їхньої аномальності через реконструктивну помилку автоенкодера; Якщо помилка реконструкції перевищує заданий поріг, стан пристрою визначається як аномальний.

- прогнозування технічного стану. Довгостроковий прогноз технічного стану формується через аналіз трендів реконструктивних помилок, отриманих на послідовних часових інтервалах.

В додатку Б представлено код для розробленого методу.

Бібліотеки numpy, pandas, matplotlib, sklearn і tensorflow використовуються для обробки даних, побудови моделі нейронної мережі (автоенкодера), нормалізації та візуалізації результатів.

Генерується періодичний синусоїдальний сигнал з невеликим випадковим шумом. У нього штучно вводяться аномалії (додаткові збурення)

на певних ділянках: від 120 до 130 та від 320 до 340, шляхом додавання або віднімання значень.

```python
# Встановлення необхідних бібліотек
!pip install numpy pandas sklearn tensorflow matplotlib

# Імпорт бібліотек
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
from sklearn.preprocessing import MinMaxScaler
from sklearn.model_selection import train_test_split
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import Dense

# Створення синтетичних даних з аномаліями
np.random.seed(42)
time_steps = 500
normal_data = np.sin(np.linspace(0, 50, time_steps)) + np.random.normal(0, 0.05, time_steps)
anomalous_data = normal_data.copy()
anomalous_data[100:120] += 2
anomalous_data[300:320] -= 2
df = pd.DataFrame({'value': anomalous_data})

# Масштабування даних
scaler = MinMaxScaler()
df['scaled'] = scaler.fit_transform(df[['value']])

# Вибір нормальних даних для тренування
normal_indices = list(range(0,100)) + list(range(120,300)) + list(range(320,500))
X_normal = df.loc[normal_indices, 'scaled'].values.reshape(-1, 1)
X_train, X_test = train_test_split(X_normal, test_size=0.2, shuffle=False)

# Створення та навчання автоенкодера
model = Sequential([
    Dense(16, activation='relu', input_shape=(1,)),
    Dense(8, activation='relu'),
    Dense(16, activation='relu'),
    Dense(1)
])
model.compile(optimizer='adam', loss='mse')
history = model.fit(X_train, X_train, epochs=50, batch_size=16, validation_data=(X_test, X_test))

# Прогнозування та виявлення аномалій
df['reconstruction'] = model.predict(df['scaled'].values.reshape(-1,1))
df['loss'] = np.abs(df['scaled'] - df['reconstruction'])
threshold = df.loc[normal_indices, 'loss'].mean() + 3 * df.loc[normal_indices, 'loss'].std()
df['anomaly'] = df['loss'] > threshold

# Візуалізація результатів
plt.figure(figsize=(15,5))
plt.plot(df['value'], label='Original data')
plt.plot(df[df['anomaly']].index, df[df['anomaly']]['value'], 'ro', label='Anomalies')
plt.legend()
plt.title('Detection of Anomalies in Sensor Data')
plt.xlabel('Time')
plt.ylabel('Sensor Reading')
```

Рисунок 3.1 – Фрагмент реалізації методу

Використовується MinMaxScaler для нормалізації значень сигналу в діапазон [0, 1], що покращує стабільність і якість навчання нейронної мережі.

Обираються нормальні ділянки даних (до та після аномалій), які використовуються для навчання автоенкодера, тобто моделі, яка повинна відтворювати лише "здорову" поведінку системи.

Нейронна мережа типу автоенкодер складається з кількох шарів. Модель навчається відновлювати (реконструювати) вхідні нормалізовані дані, мінімізуючи різницю між вхідними та вихідними значеннями.

Після навчання модель застосовується до всіх даних. Різниця між фактичним значенням і реконструйованим обчислюється як "reconstruction loss". Якщо ця похибка перевищує порогове значення (середнє плюс 3 стандартні відхилення), точка вважається аномальною.

Будується графік, на якому синім кольором зображений початковий сигнал, а червоними точками позначені виявлені аномалії. Це дозволяє візуально оцінити ефективність моделі.

Код на рисунку 3.1 реалізує базову архітектуру автоматизованого виявлення несправностей у даних з сенсорів шляхом використання автоенкодера. Такий підхід може бути масштабований і застосований у реальних системах моніторингу в мережах Інтернету речей

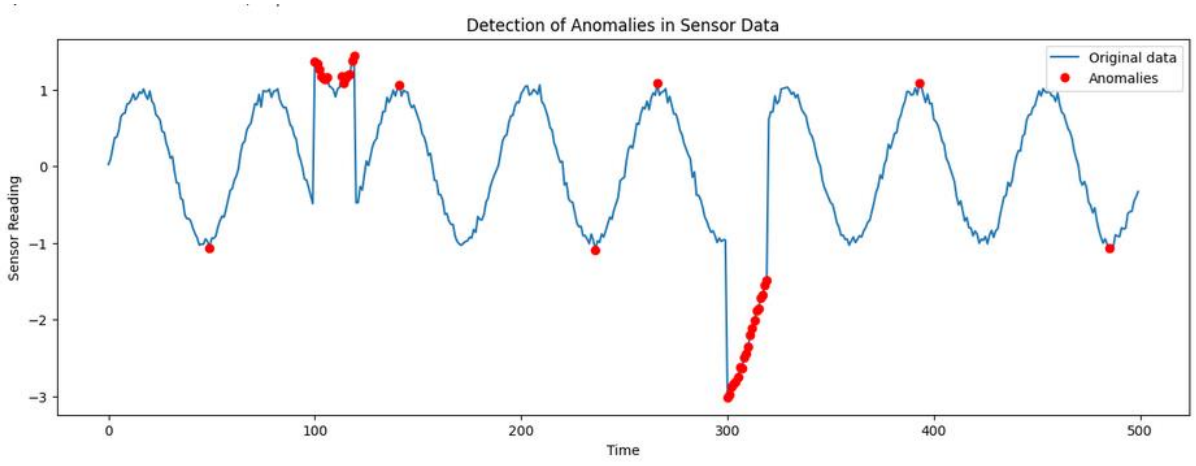

Рисунок 3.2 – Визначення аномалій в даних з датчиків

Рисунок 3.1 ілюструє результат функціонування системи виявлення аномалій у даних, що надходять із сенсорних пристроїв розподіленої мережі Інтернету речей. Синя крива на графіку відображає зміну вимірюваного параметра в часі, який має характер періодичного сигналу з невеликими флуктуаціями, зумовленими випадковим шумом. Цей сигнал є результатом

імітації нормальної поведінки пристрою, що функціонує в стабільному режимі. Упродовж більшості періодів спостерігається рівномірна синусоїдальна амплітуда, яка не виходить за межі допустимих коливань, що притаманні типовому режиму роботи сенсора.

На фоні цієї регулярної картини виділено низку червоних точок, які позначають аномальні спостереження, тобто ті значення, які суттєво відрізняються від очікуваної поведінки системи. Аномалії локалізовані в кількох часових ділянках, що відповідає штучно введеним збуренням у дані. У перших двох випадках, близько до відміток 100 і 300 на осі часу, можна побачити помітні відхилення, що проявляються у вигляді стрибків амплітуди – спочатку вгору, а потім вниз. Саме ці відхилення були ідентифіковані навченою моделлю як нетипові, що ілюструє здатність автоенкодера ефективно виявляти збої шляхом аналізу реконструктивної похибки.

Така реакція моделі свідчить про її чутливість до змін у структурі даних і здатність ідентифікувати як грубі порушення, так і менш помітні відхилення, що не належать до класу нормальних спостережень. Отже, наданий графік підтверджує успішну реалізацію алгоритму виявлення аномалій, що є важливим компонентом для побудови предиктивної аналітики в автоматизованій системі моніторингу технічного стану сенсорних пристроїв.

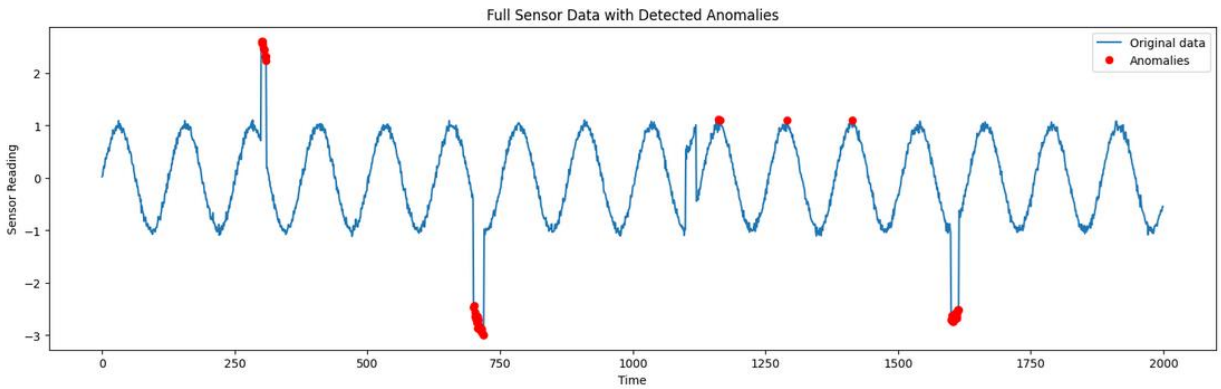

Рисунок 3.3 – Визначення аномалій в даних з датчиків (більше даних)

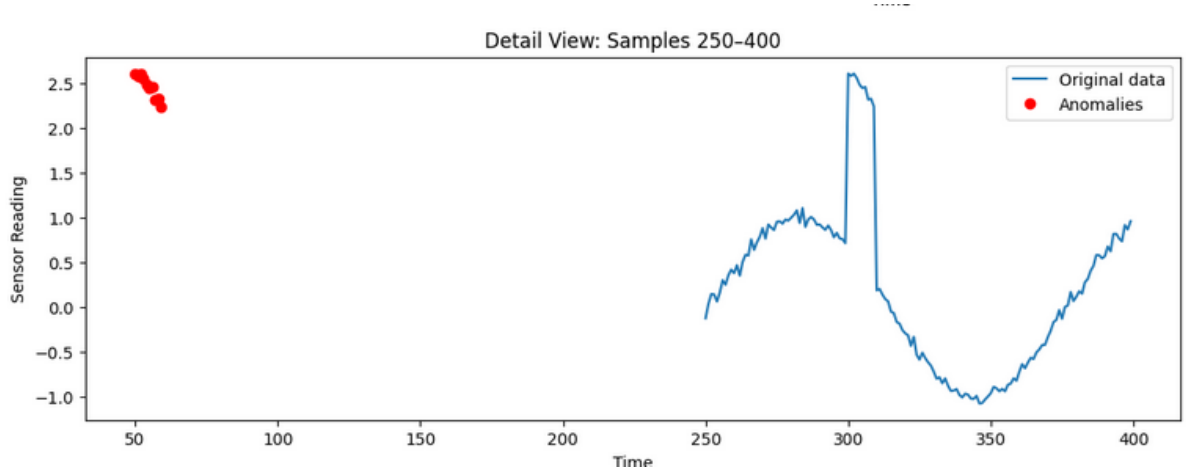

Рисунок 3.4 – Визначення аномалій в даних з датчиків (більше даних)

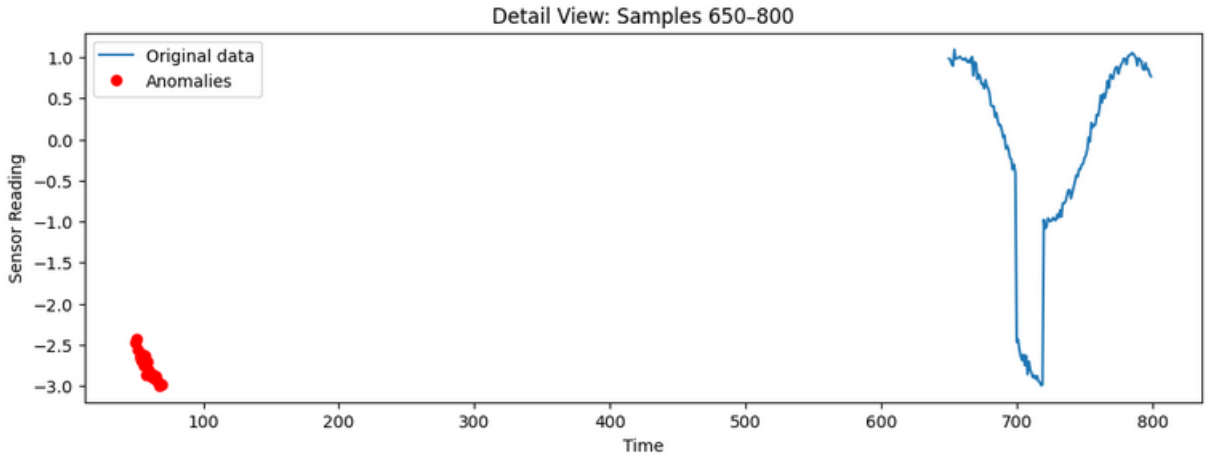

Рисунок 3.5 – Визначення аномалій в даних з датчиків (більше даних)

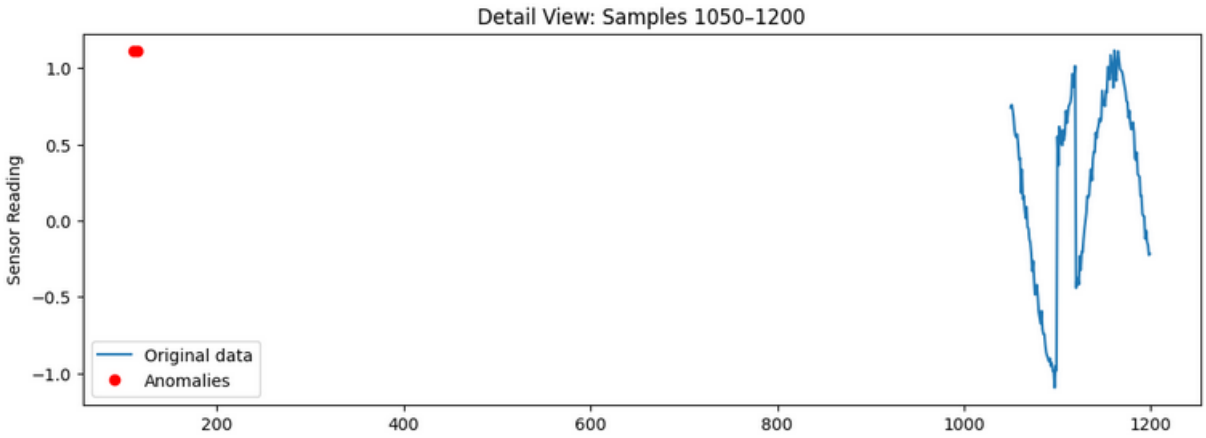

Рисунок 3.6 – Визначення аномалій в даних з датчиків (більше даних)

На рисунку 3.3 зображено повну картину зміни сенсорного сигналу протягом усього часового проміжку моделювання. Сигнал має переважно періодичний характер, що відображає типову роботу пристрою в умовах стабільного середовища. На фоні цього періодичного коливання чітко виділяються кілька зон з аномаліями, позначеними червоними точками. Вони відображають нетипові відхилення від синусоїдального патерну, зумовлені введеними збуреннями, що імітують технічні збої в роботі пристрою. Аномалії зафіксовані в декількох часових ділянках, що відповідає сценаріям штучного зміщення або спотворення сигналу.

На рисунку 3.4 графіку подано деталізовану візуалізацію одного з сегментів сигналу у часовому діапазоні між 250 та 400 вибірками. У цьому фрагменті спостерігається помітний стрибок амплітуди у позитивному напрямі, що є наслідком навмисно згенерованої аномалії. Система успішно виявила відхилення, що підтверджується щільним скупченням червоних маркерів у моменті зміни сигналу. Ця ділянка ілюструє здатність моделі автоенкодера оперативно реагувати на короткочасні, але значні спотворення амплітуди.

Рисунок 3.5 демонструє ще одну ділянку часового ряду, обмежену інтервалом від 650 до 800. У цьому сегменті сигнал зазнає різкого зниження, що супроводжується глибоким падінням амплітуди нижче за нормальний рівень. Це є імітацією критичного збою сенсорного пристрою. Аномалії чітко позначені й згруповані в зоні мінімального значення сигналу. Така поведінка сигналу свідчить про високий рівень контрасту між нормальним та аномальним станом, що дозволяє моделі точно виявити аномальні точки.

На рисунку 3.6 подано локальну ділянку між 1050 та 1200 вибірками. Сигнал у цій області демонструє дещо складніший шаблон із декількома імпульсами та пульсаціями, що свідчить про наявність нестабільності у функціонуванні пристрою. Аномалії виявлені не лише в центральному максимумі або мінімумі, а й у точках із незначними відхиленнями, що підтверджує чутливість моделі до дрібних змін у поведінці системи.

Результати демонструють, що навіть у межах неоднорідного шаблону сигналу система здатна виокремити критичні значення, які не відповідають навчальній вибірці нормального стану.

Усі графіки разом ілюструють узгоджену роботу системи виявлення аномалій, що базується на нейромережевій реконструкції, із здатністю адаптуватися до різних типів збоїв – як короткочасних імпульсів, так і тривалих зсувів сигналу.

ВИСНОВКИ

У результаті проведеного дослідження було розроблено, обґрунтовано та програмно реалізовано метод діагностування несправностей у розподіленій системі моніторингу довкілля на основі технологій Інтернету речей з використанням інструментів машинного навчання. Запропонована архітектура передбачає організацію потокової обробки даних з великої кількості сенсорних пристроїв, що працюють у режимі реального часу, з подальшою реконструкцією нормальної поведінки системи за допомогою нейронної мережі типу автоенкодер. Це дозволяє виявляти відхилення, які потенційно сигналізують про вихід з ладу обладнання або порушення в роботі компонентів системи.

У дослідженні було реалізовано повноцінний цикл аналізу: від генерації імітованих даних із вбудованими аномаліями до навчання моделі на нормальних вибірках та ідентифікації відхилень на основі реконструктивної похибки. Побудовані графіки підтвердили високу ефективність запропонованого підходу – всі ключові аномалії були точно виявлені навіть на складних ділянках сигналу. Метод продемонстрував здатність адаптуватися до різних типів порушень, таких як імпульсні збурення, плавні зміщення або комбінації відхилень.

Особливу увагу приділено структурній моделі обробки діагностичної інформації, у межах якої були розглянуті способи виявлення аномалій на основі класифікаційних, кластеризаційних, статистичних та гібридних методів. У якості найбільш придатного підходу для цільового завдання було обґрунтовано застосування автоенкодера з можливістю реконструкції часових рядів і виявлення нетипових сегментів.

Важливим елементом роботи стало також формування прогнозних моделей для предиктивного обслуговування, що базуються на накопичених даних та історії змін у поведінці сенсорів. Це дозволяє не лише фіксувати

факт наявності несправностей, а й формувати інтервали ймовірного відмовлення з метою завчасного втручання. Такий підхід значно підвищує надійність, безперервність і адаптивність функціонування розподіленої IoT-системи моніторингу.

Окремо було проаналізовано актуальні наукові публікації, що підтвердили міждисциплінарний характер тематики та потребу в об’єднанні знань з інформатики, штучного інтелекту, телекомунікацій та інформаційної безпеки. Зроблено висновок, що перспективи розвитку таких систем мають прямий зв’язок із вдосконаленням механізмів захисту даних, підвищенням прозорості прийняття рішень у нейромережах та етичним впровадженням аналітики в чутливих середовищах.

Загалом, результати роботи засвідчили доцільність використання інтелектуальних методів для моніторингу стану сенсорних пристроїв у великих розподілених IoT-мережах. Запропоноване рішення може стати основою для побудови систем раннього попередження про несправності, систем екологічного контролю, а також платформ для цифрового управління розумними середовищами.

За результатами роботи опубліковано статтю в фаховому виданні [7].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. J.Gubbi, R. Buyya, S. Marusic, M. Palaniswami. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. Vol.29, iss.7, Elsevier, 2013. P. 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

2. Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014) Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1, 2014. P. 22-32. https://doi.org/10.1109/JIOT.2014.2306328

3. M. Alsheikh; S. Lin; D. Niyato; H. Tan. Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications. IEEE Communications Surveys & Tutorials, Vol. 16, 2014. P. 1996 – 2018. https://doi.org/10.1109/COMST.2014.2320099

4. L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider. IoT Privacy and Security: Challenges and Solutions. Applied Sciences, Vol. 10(12), 2020. 17 p. https://doi.org/10.3390/app10124102

5. J.P. Singhal. A Survey on AI enabled IoT Applications. International Journal of New Media Studies, vol. 9, 2022. P. 42-46.

6. O. Aouedi, T. Vu, A. Sacco, D. Nguyen, K. Piamrat, G. Marchetto, Q. Pham. A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions. IEEE Communications Surveys & Tutorials, 2024. 56 p. https://doi.org/10.1109/COMST.2024.3430368

7. Do K., Klymova I., Naumova E., Herevych M., Yankovskyi O. Data processing and analysis methods in IOT using machine learning. Системи управління, навігації та зв’язку, вип.2. Полтава, 2025. С. 119-124.