



Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

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

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

Освітня програма Комп'ютерні системи та мережі  
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри \_\_\_\_\_  
(підпис)

“ \_\_\_\_\_ ” \_\_\_\_\_ 20\_\_ р.

**ЗАВДАННЯ**

**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

студенту Петченку Богдану Ігоровичу  
(прізвище, ім'я, по батькові)

1. Тема роботи Методи обробки даних в IoT

затверджена наказом по університету від “ 24 ” жовтня 2022 р. № 178 Стз

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня 2022 р.

3. Вхідні дані до роботи \_\_\_\_\_

IoT

нейронна мережа

діагностика

4. Перелік питань, що потрібно опрацювати у роботі \_\_\_\_\_

Основи побудови мереж iot

Діагностика мережі IOT

Реалізація діагностичної моделі

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 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	Термін виконання етапів роботи	Примітка
1	Отримання завдання. Аналіз літератури	25.10.2022–04.11.2022	
2	Огляд існуючих методів та алгоритмів.	05.11.2022–11.11.2022	
3	Аналіз існуючих пристроїв	12.11.2022–19.11.2022	
4	Розробка та реалізація методу	20.11.2022–29.11.2022	
5	Моделювання	30.11.2022–03.12.2022	
6	Отримання результатів	04.12.2022–06.12.2022	
7	Оформлення ПЗ	07.12.2022–12.12.2022	

Дата видачі завдання 24 жовтня 2022 р.

Студент \_\_\_\_\_  
(підпис)

Керівник роботи \_\_\_\_\_  
(підпис)

доц. Лебедєв О.Г.  
(посада, прізвище, ініціали)

## РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 58 с., 19 рис., 1 дод., 20 джерел.

ІОТ, ОБРОБКА ДАНИХ, НЕЙРОННА МЕРЕЖА, МЕТОД, LSTM.

Метою кваліфікаційної роботи є аналіз методів обробки даних у мережах інтернету речей для передиктивного обслуговування у розподіленій автоматизованій системі моніторингу.

У ході виконання кваліфікаційної роботи проведено аналіз методів обробки даних у мережах IoT для передиктивного обслуговування у розподіленій автоматизованій системі моніторингу. Проведено аналіз технології IoT, а також існуючих методів обробки даних в IoT. Розроблено метод розпізнавання неполадок у мережі IoT з використанням штучних нейронних мереж.

## ABSTRACT

Master's thesis: 58 pages, 19 figures, 1 appendices, 20 sources.

IOT, DATA PROCESSING, NEURAL NETWORK, METHOD, LSTM.

The major goal of this thesis is to develop a method of data processing in a specialized computing device based on identifiers.

In order the analysis of data processing methods in Internet of Things networks for predictive maintenance in a distributed automated monitoring system.

In the course of the qualification work

## ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ .....	7
ВСТУП .....	8
1 ОСНОВИ ПОБУДОВИ МЕРЕЖ ІОТ .....	10
1.1 Аналіз технологій побудови ІоТ.....	13
1.2 Класифікація архітектури ІоТ.....	17
1.2.1 Сенсори та сенсорні мережі .....	18
1.2.2 Шлюзи .....	19
1.2.3 Рівень керування .....	20
1.2.4 Рівень додатків .....	21
1.3 Протоколи взаємодії сенсорної мережі .....	21
1.4 Способи взаємодії в архітектурі ІоТ .....	23
2 ДІАГНОСТИКА МЕРЕЖІ ІОТ .....	29
2.1 Аналіз типових структур систем обробки діагностичної інформації у мережі інтернету речей .....	30
2.2 Аналіз діагностичних моделей для обробки технологічних часових рядів .....	33
3 РЕАЛІЗАЦІЯ ДІАГНОСТИЧНОЇ МОДЕЛІ .....	37
3.1 Розробка структури інтелектуальної системи діагностування .....	40
3.2 Інтеграція нейронної мережі.....	42
ВИСНОВКИ.....	47
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ .....	48
ДОДАТОК А Графічний матеріал кваліфікаційної роботи.....	50

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ  
І ТЕРМІНІВ

ІОТ – Інтернет речей

БЗТК – блок запам'ятовування таблиці комутації

МПК – мікропроцесорний пристрій керування

МУТМ – модуль управління трасуванням мережі

ПАС – пристрій адреси повідомлень

ПЛІС – програмована логічна інтегральна схема

## ВСТУП

В даний час все більше уваги приділяється екологічному стану навколишнього середовища. Зокрема, невід'ємною частиною та важливою умовою збереження екології є чистота гідрографічної мережі. Щоб забезпечити належний рівень захисту водних масивів від забруднень, важливо своєчасно відстежувати можливі скидання та порушення з боку промислових підприємств та антропогенних факторів у загалом.

З метою відстежування стану, наприклад, гідрографічної мережі, можливо використання пристрою, який дозволяє збирати ряд метрик в онлайн режимі, що комплексно відображають чистоту та збереження водного масиву. Очевидно, що одного пристрою мало, щоб відстежити стан навіть однієї річки, не кажучи вже про всю гідрографічну мережу нашої планети. Кількість пристроїв, необхідних для належного моніторингу, об'єднаних у загальну розподілену мережу може обчислюватися десятками, сотнями тисяч і навіть мільйонами.

Важливо врахувати ті фактори, що кожен пристрій повинен працювати в автономному режимі, в умовах низької доступності мереж, і водночас збирати цілу низку різних метрик, кожна з яких відповідає за свої показники. Для обробки масиву різнорідних даних з такої GRID-системи важливо враховувати всі нюанси та особливості при проектуванні та розгортанні обслуговуючого дата-центру таким чином, щоб розгорнута система моніторингу працювало цілодобово та безперебійно. Завдяки стрімкому розвитку інформаційних технологій, можливостей для відстеження стану системи, що забезпечує захист навколишнього середовища, стає все більше.

Комунікаційні можливості інтернету речей дозволяють в режимі реального часу збирати метричні дані з пристроїв, що працюють у умовах низької доступності для забезпечення надійну роботи всього інфокомунікаційного комплексу загалом. Важливо заздалегідь визначити

ймовірність виникнення можливих несправностей як у мережі, так і у самих вимірювальних пристроях.

Сучасні методи обробки інформації, що базуються на алгоритмах машинного навчання та штучного інтелекту, формують можливість здійснювати передиктивне обслуговування задіяних пристроїв, що є важливою складовою у надійній та відмовостійкій роботі системи моніторингу довкілля.

Предиктивне обслуговування дозволяє заздалегідь оцінити ймовірність несприятливого збігу обставин, позначаються на коректній роботі технічних засобів, базуючись на раніше накопичених даних про їхню коректну та стабільну роботу. Інтеграція таких алгоритмів та методів обробки даних у мережі, що працює на MQTT-протоколі, або йому подібних, в серверні та хмарні системи, є важливою і актуальною з наукового погляду завданням. Щоб забезпечити гідний рівень відмовостійкості та надійності розподіленої мережі вимірювальних пристроїв, важливо коректно змодельовати їхню роботу, визначити перелік периферійних пристроїв, сформулювати уявлення про архітектуру такої мережі, врахувати взаємодія всіх рівнях від перетворення аналогового сигналу в цифровий на самому вимірювальному пристрої, до кластера розподілу навантаження розподіленої системи моніторингу та модуля зберігання, обробки та класифікації отриманих даних для подальшої інтерпретації.

Мета роботи – аналіз методів обробки даних у мережах інтернету речей для передиктивного обслуговування у розподіленій автоматизованій системі моніторингу.

Завдання:

- провести аналіз технології IoT;
- провести аналіз існуючих методів обробки даних в IoT;
- розробити метод розпізнавання неполадок у мережі інтернету речей з використанням штучних нейронних мереж.

## 1 ОСНОВИ ПОБУДОВИ МЕРЕЖ ІОТ

В даний час існує безліч визначень терміну "Інтернет Речів". Термін та визначення повноцінно сформувалися лише в 1999 року, але сама ідея такої технології з'явилася набагато раніше. У 1926 році Нікола Тесла уявляв, що в майбутньому всі пристрої будуть об'єднані в єдину глобальну мережу і стануть частиною єдиного цілого, а використовувані для цього інструменти будуть легко розміщуватися в кишені. Перший пристрій, підключене до мережі Інтернету речей, що зароджується, можна віднести тостер випускника Массачусетського технологічного інституту Джона Ромки, який підключив його до мережі в 1990 році як експеримент [1].

Сьогодні до загальновизнаних і найчастіше зустрічаються визначенням поняття «Інтернет Речів» можна віднести такі: - Сукупність пристроїв, що мають інтерфейси мережевого взаємодії та самої об'єднуючої їх мережі; - Мережа фізичних об'єктів, що мають вбудовані технології. взаємодії із зовнішнім середовищем з можливістю передачі даних про своє поточному стані та прийомі даних ззовні; – концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або із зовнішнім середовищем, що розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій та операцій необхідність участі людини. У кожному визначенні простежується загальна подібна модель організації та представлення технологічних особливостей Інтернету Речів, а саме – єдина мережа об'єднаних пристроїв, які здійснюють внутрішню і зовнішню взаємодію.<sup>48</sup> Технології Інтернету Речів застосовуються з моменту виникнення по сьогоднішній день у колаборації з розвитком телекомунікаційних технологій передачі [2].

Паралельно повсюдному поширенню технології радіочастотної ідентифікації фізичних предметів (RFID), розвитку технологій міжмашинної

взаємодії (M2M), технологій бездротового зв'язку (особливо 5G), протоколу IPv6 (що дозволяє ідентифікувати до  $5 \cdot 10^{28}$  будь-яких фізичних пристроїв на кожного мешканця Землі), хмарним технологіям (SaaS, IaaS, PaaS і т.д.), розвиваються і технології Інтернету Речів [3]. Вже у 2009 році кількість підключених до мережі предметів перевищила кількість людей на планеті та стрімкими темпами набирає обертів. На рисунку 1.1 зображено тимчасову шкалу зміни кількості людей та предметів, підключених до Інтернету за розрахунками Cisco IBSG, на якій чітко простежується геометрична прогресія кількості підключених пристроїв [4].

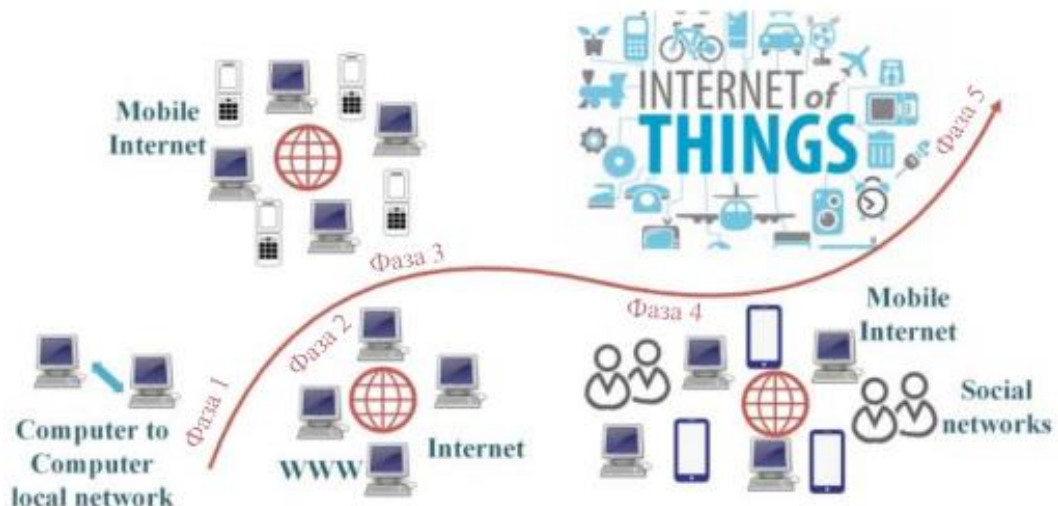


Рисунок 1.1 – IoT

Розвиваючись, IoT дозволяє включати постійно збільшується кількість фізичних предметів, що функціонують у глобальній мережі, що сприятливо позначається на виникненні нових можливостей у сфері безпеки, аналітики та управління. Така тенденція певним чином благотворно позначається на якості життя та відкриває нові можливості та перспективи в автоматизації процесів життєдіяльності, за винятком активної участі людини.

Основні галузі, в яких IoT найбільш застосовний в даний час, це:

- системи моніторингу та управління логістичних операцій;
- системи моніторингу та обліку в житлово-комунальному господарстві;
- системи моніторингу та управління медичними пристроями;
- системи забезпечення безпеки людей та тварин, транспортних засобів та нерухомості;
- системи моніторингу промислового обладнання та довкілля.

Перед тим, як приступати до аналізу технологій побудови мереж інтернету речей, важливо відзначити можливість застосовувати IoT у промисловості. Це напрямок формує особливий набір технологій, який прийнято визначати як індустріальний (промисловий) інтернет-речей (IIoT).

Промисловий інтернет речей - це сукупність пристроїв, засобів передачі, збору, обробки, візуалізації та інтерпретації даних, об'єднаний в єдину мережу для промислових цілей [5]. Історія виникнення даного напрямку починається з таких технологій, як теплова автоматика та релейний захист, яких схеми управління були сформовані на концепції жорсткої непрограмованої логіки [6]. З появою мікроелектроніки виникла можливість формувати алгоритми управління за допомогою програмного забезпечення. В наш час методи інтелектуального аналізу даних дозволяють інтегрувати в промислові системи нейронні мережі, алгоритми нечіткої логіки та машинне навчання, які виконують оптимізаційне завдання і є методами вирішення математичних завдань.

Моделювання процесів у реальному часі стає повсякденним, нейромережеві апроксиматори здійснюють прогнозовану підтримку у прийнятті рішень із збільшеним просторово-часовим лагом та вирішують спеціалізовані системи диференціальних рівнянь, які описують процеси технологічного порядку із підвищеною точністю [7]. Завдяки новітнім технологіям автоматизації виробничих процесів, операційна роль людини стає менш значущою, та оператори здійснюють все менше взаємодії зі складними виробничими та операційними процесами, що суттєво знижує

людський фактор гіпотетичних лих та аварій. В цілому, надійність, безпека та відмовостійкість систем промислового інтернету речей повністю залежить від різних факторів, які можуть бути відображені на будь-якому з етапів експлуатації компонентів системи та її життєвого циклу. Тому побудова надійної та відмовостійкої промислової системи максимально залежить від ступеня опрацювання її проектної та архітектурної складових.

### 1.1 Аналіз технологій побудови IoT

Офіційне визначення Інтернету Речей наводять у рекомендації МСЕ-Т У.2060 (рисунок 1.2), представлене як «IoT – глобальна інфраструктура інформаційного суспільства, що забезпечує передові послуги за рахунок організації зв'язку між речами (фізичними чи віртуальними) на основі існуючих та сумісних інформаційних та комунікаційних технологій.



Рисунок 1.2 – Можливості IoT

Речі (things) у цьому визначенні інтерпретовані як фізичний предмет, так і об'єкт віртуального світу (прикладне додаток, або контент мультимедійного порядку), який ідентифікується та об'єднується через єдину комунікаційну мережу [8]. Крім поняття речі (things), у МСЕ-Т наводиться визначення терміна пристрій (device), який інтерпретується як будь-яка частина обладнання із закладеною можливістю здійснювати комунікацію у мережі в обов'язковому порядку, та необов'язковими можливостями здійснювати сенсоринг та зондування, які передбачають збір, зберігання та обробку даних [9]. Як наслідок, можна дійти невтішного висновку, що у МСЕ-Т приділяють максимум уваги комунікаційним аспектам, а не додаткам інтернету речей.

Основну роль у зв'язку фізичного та віртуального світу беруть на себе пристрої, здатні збирати інформацію будь-якого роду та які мають можливість розповсюджувати зібрану інформацію по комунікаційній мережі будь-якими доступними способами безпосередньо між собою, а також через мережу як із допоміжними шлюзами, так і без них.

Для організації міжмережевої взаємодії передбачено безліч різних мережевих технологій, такі як:

- глобальні мережі;
- локальні мережі;
- бездротові мережі, що самоорганізуються;
- комірчасті мережі.

Перераховані вище види мереж зв'язку використовуються для транспортування даних, які були зібрані вимірювальними пристроями, які очікують отримання програм та додатків, і у зворотний бік здатні передавати команди безпосередньо до пристроїв від програмних програм.

Важливо додатково уточнити, що самі речі та пристрої найчастіше мають власними процесорами, що здійснюють управління та передобробку даних, що включають власну операційну систему, модулі вимірювальних компонентів та блоки комунікацій [10]. Пристрої та прикладні програми в

мережах інтернету речей працюють за єдиним протоколом взаємодії, основою якого закладено правило, при якому всі вузли мережі рівноправні між собою у наданні які забезпечують сервісів.

У зв'язку з багаторазовим зростанням пристроїв, виникала проблема з можливістю виділення ресурсу вільних мережевих адрес, кількість яких обмежена на протоколі IPv4, але розробка оновленої версії протоколу міжмережевої взаємодії IPv6 визначає успішне повсюдне використання Інтернету речей. Еталонна модель IoT включає чотири основні горизонтального рівня, відображеного на рисунку 1.3.



Рисунок 1.3 – Еталонна модель IoT

Рівень застосунку не піддається стандартизації і може бути використаний залежно від завдань, переслідуваних у проєктованій системі. Рівень підтримки програм та послуг використовується для виконання можливостей загального порядку, що передбачають обробку та зберігання

даних включених до системи об'єктів Інтернету речей, необхідність яких простежується як у додатків, так і у груп додатків, об'єднаних по подібною ознакою.

Мережевий рівень підтримує мережну та транспортну можливості. Мережева функція визначається необхідністю здійснювати управління мобільністю, ресурсами мережі доступу, авторизації та автентифікації. Транспортна функція призначена для можливості забезпечити пов'язаністю мережі з метою передавачі інформацію додатків. Рівень пристроїв задіяний для забезпечення можливістю пристроїв здійснювати прямий обмін даними по мережі зв'язку безпосередньо між пристроями, за допомогою шлюзів, по бездротовій динамічній мережі, та використовується для управління самими пристроями, щоб активувати та деактивувати їх із метою зберегти максимальну кількість енергоресурсу.

Шлюз у таких системах використовується для одноразової підтримки різного виду інтерфейсів підключення пристроїв (CAN, ZigBee, WiFi, Bluetooth) та для різних видів транспортних мереж (2G-5G, DSL, LTE) [11]. Додатково використовують шлюз, щоб підтримувати конверсії протоколів для тих випадків, коли протоколи у мережі та інтерфейсу пристрою різні. Усі вищеперелічені рівні охоплюються вертикальними рівнями управління та безпеки. На вертикальному рівні управління усуваються наслідки відмов, здійснюється підтримка мережевих можливостей, налаштовується конфігурація та безпека.

Пристрої, трафік, мережі та їх топології цьому рівні являють собою об'єкти управління. Функціональні особливості рівня безпеки безпосередньо залежать від рівня, до якого вони використовуються. На рівні додатків та послуг здійснюється підтримка цілісності даних та захист від вірусів. На мережевому рівні рівень безпеки гарантує коректну авторизацію та автентифікацію, підтримує політику доступу та забезпечує конфіденційність даних.

Функціональна модель архітектури IoT – А є ієрархічною, але дещо відрізняється від представленої раніше еталонної моделі згідно 55 МСЕ-Т Y.2060.

У моделі IoT – А рівні управління безпеки та управління беруть участь у всіх процесах, а горизонтальні рівні представлені послідовно та взаємодію за наступним принципом:

- пристрої взаємодіють із сервісами IoT через рівень комунікацій;
- сервіси IoT взаємодіють з рівнем програми, використовуючи допоміжний рівень організації послуг;
- рівень організації сервісів взаємодіє з рівнем віртуальних сутностей та управлінням бізнес-процесами IoT;
- рівень додатків є верхньорівневим та здійснює роботу з поставленого завдання, відповідної спеціалізації проектованої системи;
- рівні управління та безпеки беруть участь у всіх процесах та використовуються на кожному з горизонтальних рівнів.

Порівнюючи стандартну мережеву модель взаємодії відкритих систем OSI з моделлю передачі IoT-A важливо відзначити, що пропускна здатність кожної їх істотно відрізняється для певних етапів. У процесі передачі даних моделі IoT-A представлені такі поняття, як мережа з обмеженнями та мережа без обмежень. Мережа без обмежень визначається високою швидкістю передачі і має деякі подібності з Інтернет-з'єднанням. Мережі з обмеженнями характерно переважають низькою швидкістю передачі даних до 1 Мбіт/сек та високим рівнем затримок у мережі. У таких мережах застосовуються стандарт IEEE 802.15.4 та схожими з групи стандартів IEEE 802.15 [12].

## 1.2 Класифікація архітектури IoT

Інтернет речей є мережею нового покоління, тому в його архітектурі спостерігаються певні подібності з архітектурою NGN, також що містить у собі чотири шари. IoT містить у собі безліч різних інфокомунікаційних

технологій, які забезпечують можливість функціонувати всій системі загалом. На рисунку 1.6 відображено які технологічні компоненти застосовуються кожному з рівнів архітектури IoT.

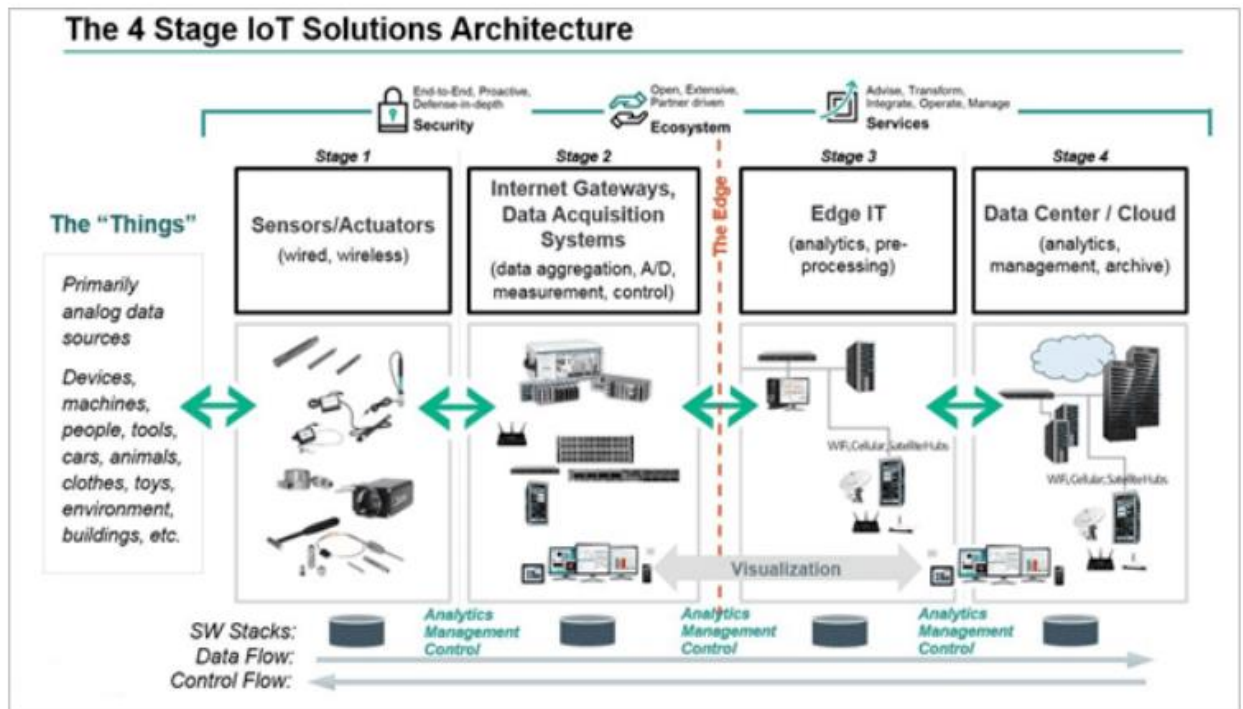


Рисунок 1.4 – Архітектура IoT

Для детального представлення функціональних завдань кожного з рівнів архітектури IoT, нижче представлено опис об'єктів та операцій, присутніх у схематичному зображенні архітектури Інтернету речей.

### 1.2.1 Сенсори та сенсорні мережі

На рівні сенсорів та сенсорних мереж, який є нижнім у представленій моделі, визначається набір smart-об'єктів, які інтегруються з датчиками та сенсорами. Сенсори збирають та обробляють інформацію з реального світу, перетворюючи її на віртуальний формат, тим самим забезпечуючи зв'язок цифрового та фізичного світів. Існує безліч типів сенсора, що функціонують

у відповідність до їх завдань і спеціалізацією. Сенсори можуть бути задіяні для збору інформації про навколишньому середовищі (наприклад температура або рН на локації водного масиву), тиску, розташування сенсора в географічному середовищі, а також здатні визначати швидкість руху та інші метричні показники.

Сенсори мають невеликий запас пам'яті для забезпечення можливості здійснювати запис зібраних результатів вимірів. Класифікація сенсорів визначається відповідно до їх призначення – для збору інформації про довкілля, для збирання інформації про тіло людини/тварини, для побутової техніки та транспортних засобів та інші. Вимірювальним пристроям на рівні сенсорів у більшості випадків необхідна агрегація зі шлюзом, що є брокером у локальній обчислювальній мережі. З'єднання з брокером здійснюється через мережі Ethernet, Wi-Fi, (PAN) Personal Area Network, ZigBee, Bluetooth, UWB (Ultra-Wide Band).

Можливий сценарій, коли сенсорам не потрібна агрегація за допомогою шлюзів, і в таких випадках з'єднання може бути організовано за допомогою підключення до глобальної бездротової мережі через GSM, GRPS, LTE та подібним.

Для підключення сенсорів з низьким рівнем енергоспоживання, де не потрібна висока швидкість передачі даних, можуть бути підключені по WSN (Wireless Sensors Network). WSN – бездротові сенсорні мережі, які дозволяють підключити практично необмежену кількість сенсорних пристроїв на великій площі, підтримуючи протоколи взаємодії, які забезпечують енергозбереження акумуляторних пристроїв.

### 1.2.2 Шлюзи

На рівні шлюзів та мереж важливо забезпечити надійну та високопродуктивну пропускну здатність у зв'язку з обсягом даних, що генерується великою кількістю сенсорних пристроїв. Рівень шлюзів і мереж є

транспортним середовищем і може бути організований як з допомогою провідної, так і бездротової інфраструктури мережі.

У IoT конфігурація мережі вимагає забезпечити можливість об'єднувати безліч мереж, організованих з урахуванням різних технологій і протоколів доступу, що визначається як гетерогенна конфігурація.

Гетерогенна конфігурація мережі «Інтернету речей» має забезпечувати достатній рівень якості передачі інформації, особлива увага приділяється безпеці, низьких затримок та достатньої пропускнуєї спроможності.

Рівень шлюзів та мережі являє собою конвергентну мережеву інфраструктуру, реалізовану через злиття різних типів мереж в єдину мережеву платформу. Завдяки конвергентній реалізації мережної інфраструктури «Інтернету речей», хости можуть задіяти доступні ресурси в мережі через відповідні шлюзи конфіденційно, безпечно та незалежно без негативного впливу на продуктивність мережі [13].

### 1.2.3 Рівень керування

Рівень керування являє собою перелік інформаційних послуг та сервісів, які виконують функцію автоматизації технологічних операцій, таких як:

- підтримка операційної діяльності;
- підтримка бізнес-завдань;
- аналітична обробка статистичної інформації;
- інтелектуальний аналіз даних;
- системи обробки тексту та мовлення;
- прогнозування на тимчасових рядах;
- зберігання даних;
- забезпечення інформаційної безпеки;
- управління бізнес-процесами та бізнес-правилами.

#### 1.2.4 Рівень додатків

Рівень додатків є набір різнотипних додатків залежно від сфери діяльності, на яку застосовується рішення на технологічну базу «Інтернету речей». Додатки є специфічними для певної галузі, що визначаються терміном "вертикальні додатки". Програми, які можуть бути використані в різних сферах діяльності, що визначаються терміном «горизонтальні».

#### 1.3 Протоколи взаємодії сенсорної мережі

Важливим критерієм вибору організації сенсорної мережі є її тип дротовий або бездротовий. Для поставленого завдання здійснювати моніторинг екологічної ситуації на глобально розподіленій території, найбільш підходящим є вибір бездротової організації сенсорної мережі. При організації бездротової сенсорної мережі найважливішим фактором є можливості мережі забезпечити низьке споживання енергії акумуляторних батарей, так як ємність акумуляторів на сенсорних пристроях має обмежений ресурс, та їх заміна та підзарядка трудомісткий та дорогий процес.

Саме тому на сенсорних пристроях повинна виконуватися тільки первинна обробка даних із мінімально необхідним набором переданої інформації та циклами прийому-передачі. На базі стандарту IEEE 802.15.4 реалізовано різноманітні протоколи передачі даних.

Протоколи ZigBee використовуються фізично та рівні доступу до середовища бездротових мереж передачі даних. Він найбільш застосуємо в локальній мережі сенсорних пристроїв, розташованих на невеликих відстанях до 75 метрів, та забезпечує роботу таких пристроїв на низькому рівні споживання з максимально високим ступенем надійності передачі даних. Завдяки застосуванню стандарту IEEE 802.15.4 за допомогою додаткового програмного забезпечення можна організувати на мережевому рівні та вище будь-які з існуючих топології мережі.

Протоколи ZigBee забезпечують можливість перебувати сенсорним пристроям у сплячому режимі більшу частину часу, активуючись лише для виконання поставлених завдань та передачі даних, що значною мірою зберігає акумуляторну ємність та продовжує термін служби батарей.

Ключовою особливістю бездротових мереж, що самоорганізуються, реалізованих на базі протоколів сімейства ZigBee, є їхня здатність самостійно знаходити один одного в мережі при включеному живленні, і у разі виходу з ладу одного з пристроїв, організація вузлів у самостійному порядку формує оновлені маршрути для подальшої передачі даних між пристроями та брокером. Для реалізації сенсорних мереж, що самоорганізуються, може бути також використано технологію бездротового з'єднання Bluetooth. У таких мережах організовано взаємодію за принципом провідних та ведених пристроїв, при цьому представлені ролі можуть бути поєднані в одному пристрої. Такі пристрої здатні передати дані і в синхронному, і в асинхронному режимах:

- синхронний режим використовується у разі передачі даних обмежені в часі і передбачає прямий зв'язок між ведучим та веденим пристроями із закріпленим каналом та тимчасовими слотами доступу;

- асинхронний режим використовується для пакетної передачі даних між провідним та кількома веденими пристроями. У бездротовій сенсорній мережі з низьким енергоспоживанням найбільше застосовна специфікація ядра технології Bluetooth v4.0, отримав назву BLE (Bluetooth Low Energy). Ця специфікація є найбільш підходящою для організації мережі вимірювальних пристроїв розподіленої системи моніторингу довкілля.

Третім можливим варіантом реалізації розподіленої сенсорної мережі є набір стандартів зв'язку IEEE 802.11. Цей стандарт забезпечує високу швидкість передачі даних (до 108 Мбіт/с), і саме тому він є найбільш застосовним у самоорганізованих сенсорних мережах, яким потрібна можливість передачі великого обсягу інформації в режимі реального часу.

## 1.4 Способи взаємодії в архітектурі IoT

Щоб організувати взаємодію різних інтерфейсів великого кількості автономних пристроїв, потрібно вдаватися до застосування протоколів передачі даних, які закладено основою організації Інтернету речей [14].

Існує безліч протоколів взаємодії в інтернет речей на мережевому та прикладному рівнях, і найбільш підходящим для поставленого завдання щодо розробки системи моніторингу навколишнього середовища є MQTT (Message Queue Telemetry Transport). Переваги протоколу MQTT складно переоцінити. Він є легким, компактним та відкритим протоколом в частині організації обміну даними та спочатку був створений для того, щоб здійснювати передачу даних на віддалено розташованих локаціях [15].

Його здатність передавати дані, що містять у собі невеликий обсяг пам'яті на мережі з обмеженою пропускнуою здатністю каналу, максимально відповідає поставленій задачі. Телеметричні дані містять у собі дані великого обсягу, а самі вимірювальні пристрої розташовуються у важкодоступних віддалених місцях з низькою пропускнуою здатністю у мережі.

MQTT протокол має важливі особливості, такі як можливість асинхронної роботи в умовах нестабільного зв'язку на лінії передачі даних та проста інтеграція в нові розгорнуті пристрої. Це дозволяє говорити про спрощену мультиплікативність та масштабованість, що є важливою умовою, оскільки розподілена автоматизована мережа моніторингу повинна покривати максимально великі території для найкращого контролю за екологічною ситуацією в гідрографічній мережі. MQTT протокол працює на прикладному рівні TCP/IP і використовує 1883 порт за замовчуванням.

Для підключення через SSL з'єднання використовується 8883 порт [16]. Структура повідомлень MQTT протоколу складається з фіксованого заголовка, який в обов'язковому порядку повинен бути присутнім у всіх повідомленнях, змінного заголовка та даних, які можуть відрізнятися та бути тільки у певних повідомленнях [17].

У фіксованому заголовку MQTT-повідомлення, відображеному на рисунку 1.5 в обов'язковому порядку присутній Message Type, що відповідає за тип переданого повідомлення.

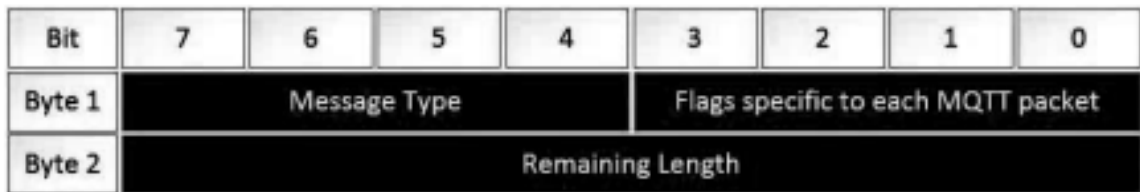


Рисунок 1.5 – Структура фіксованого заголовку MQTT-повідомлення

Всього в протоколі закладено 15 типів повідомлень та як приклад можна навести такі основні, як CONNECT (запит на підключення до серверу), SUBSCRIBE (запит на підписку), PUBLISH (публікація повідомлення), DISCONNECT (повідомлення про відключення від сервера) [18].

Чотири старші біти першого байта використовуються як спеціальні прапори:

- DUP, який пропоставляється у разі, коли вимірювальне пристрій або приймаючий брокер повторно надсилає пакет з даними. Використовується у таких типах повідомлень, як PUBLISH, SUBSCRIBE, UNSUBSCRIBE, PUBREL (дозвіл видалення повідомлення);

- QoS, що визначає якість обслуговування;

- прапор RETAIN, який враховується брокером, щоб при отримання повідомлення з типом PUBLISH негайно було надіслано повідомлення.

У змінному заголовку фігурує ідентифікуюча складова, яка дозволяє визначити джерело повідомлення та аутентифікувати в відповідність з отриманим набором даних.

Bit	7	6	5	4	3	2	1	0
Byte 8	User name	Password	Will Retain	Will QoS		Will Flag	Clean Session	Reserved

Рисунок 1.6 – Структура змінного заголовка MQTT-повідомлення

У змінному заголовку, відображеному на рисунку 1.6, фігурують ідентифікатор пакета, найменування та версія протоколу для типу повідомлення CONNECT, прапори, які вказують на поведінку вимірювального пристрою при підключенні, та інформація, що дозволяє ідентифікувати пакети та вимірювальний пристрій, що надсилає дані.

Захист передачі даних передбачен в MQTT протоколі через аутентифікацію клієнтів за пакетом CONNECT, контролю доступу клієнтів через Client ID та підключення безпосередньо до самого пробер через TLS/SSL з'єднання [19]. Корисні дані та формат їх передачі в MQTT повідомленнях містяться в додатку. Розмір даних можна визначити шляхом віднімання із Remaining Length довжини змінного заголовка [20]. Щоб вирішити поставлене завдання, недостатньо організувати взаємодію лише на рівні "Вимірювальний пристрій - Брокер".

Архітектура рішення включає з одного боку десятки тисяч вимірювальних пристроїв та брокерів з низьким рівнем споживання, оперативної реакцій на події та невеликою обчислювальною потужністю, і з іншого боку Cloud – рішення з великою обчислювальною потужністю, щоб обробляти великі масиви даних, зберігати та класифікувати їх. Крім цього, на стороні backend – сервера мають бути включені елементи машинного інтелекту для коректної реакцію ті чи інші тригери.

На рисунку 1.7 схематично відображені рівні, процеси та об'єкти взаємодії, які мають бути задіяні у топології мережі на базі IoT – технологій для вирішення поставленого завдання.

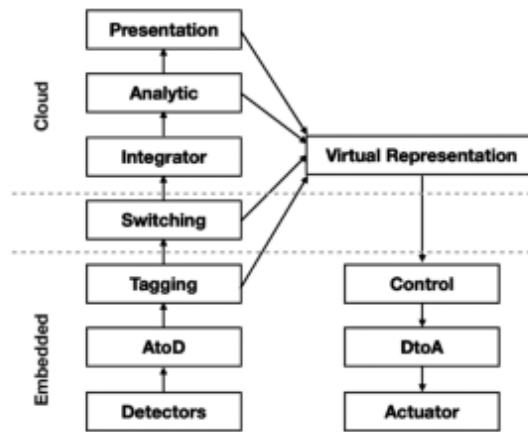


Рисунок 1.7 – Архітектура розгорнутогоIoT рішення

Процес починається на Embedded рівні з самих вимірювальних пристроїв. Вимірювальні пристрої фіксують факт зміни навколишнього середовища, формуючи аналоговий сигнал, який перетворюється на цифровий для подальшої обробки. Функцію перетворювача виконує AtoD, після чого процесор вимірювального пристрою пропоставляє до отриманої інформації Tag з позначкою timestamp-а, щоб класифікувати дані в пакеті та зафіксувати час виникнення тригера [21]. В якості рівня Switching у представленій архітектурі, що поступають з вимірювальних пристроїв пакетів виступає зв'язка «Брокер – Маршрутизуючий кластер». Тут дані класифікуються та підсумовується за виявленими однотипними Tag. У кластері містяться маршрутизатори, що обробляють Tag, відповідні профілю обробки даних кожного окремого маршрутизатора.

Розподіл маршрутизаторів на обробку типових даних, що надходять благотворно позначається на консистенції оброблюваних даних, що дозволяє покращити показники надійності та відмовостійкості кожного окремого маршрутизатора і кластера, що маршрутизує, в цілому [22]. Оброблені в кластері дані надходять на backend-систему для їх подальшої обробки та перетворення в вид, що читається у термінальне вікно користувачів системи.

Аналітичний блок backend – системи включає в себе основну логіку обробки даних, а також алгоритми AI для виявлення патернів в отриманих

даних і Machine Learning для прогнозування можливих наслідків на підставі актуальних та історично накопичених даних за відомостями навколишнього середовища. Перш, ніж визначити можливі патерни в оброблюваних даних, важливо уявити, як організовано взаємодію в маршрутизуючому кластері, що обробляє потоки даних, що надходять із брокерів. На рисунку 1.8 схематично представлена маршрутизація вузла з чотирьох аналогічних один одному маршрутизаторів (A, B, C, D), де для кожного їх передбачається наявність шести стандартних інтерфейсів.

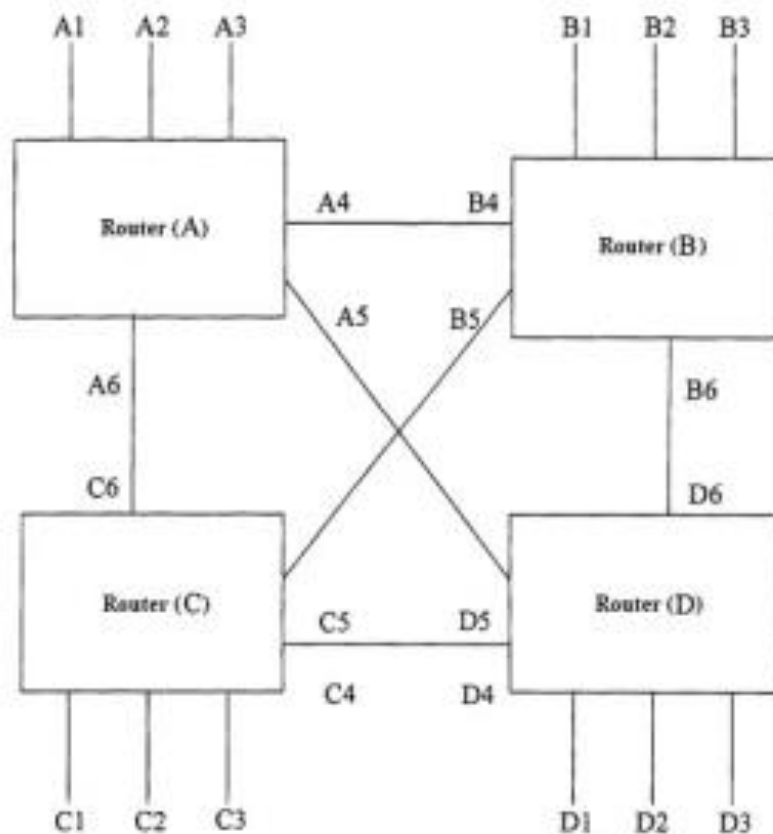


Рисунок 1.8 – Схема маршрутизації в кластері

У кожного маршрутизатора передбачається три інтерфейси, які використовуються для внутрішнього зв'язку – A4, A5, A6, інші три інтерфейси необхідні, щоб забезпечити смугу пропускання для зовнішніх джерел.

Завдяки такій організації вузла, в якому кожний пристрій забезпечений смугою пропускання  $60G$ , утворюється неблокуюча мережа зі смугою пропускання в  $120G$ , що в сукупності дозволяє збільшити смугу пропускання вузла. Щоб робота такого вузла була максимально можливого ступеня надійна та відмовостійка, потрібно враховувати дискретну послідовність станів, кожен з яких береться з дискретного простору станів, що задовольняє Марківській властивості.

## 2 ДІАГНОСТИКА МЕРЕЖІ ІОТ

Організація діагностики роботи вимірювальних пристроїв у мережі Інтернету речей є важливою складовою у проектуванні розподіленої системи моніторингу довкілля. Підтримка працездатності комплексу вимірювальних пристроїв у процесі експлуатації системи є найбільш актуальним завданням, оскільки вихід з ладу сенсорного обладнання негативно позначається на їх функціональній задачі. Для організації ремонту потрібно формувати оцінку його технічного стану на основі поточних діагностичних даних, при цьому можливість формувати прогностні значення для параметрів, що відображають технічне стан обладнання, що дозволяє своєчасно запланувати необхідні заходи та ресурси для відновлення працездатності пристроїв.

Щоб сформувати прогностні показники щодо можливого виходу з ладу вимірювального пристрою, повинні бути задіяні характеристики, які ґрунтуються на експертних знаннях, отриманих у процесі моделювання, чи експлуатації системи. Динаміка змін на часовому ряді показників стану зумовленого переліку параметрів може сигналізувати про можливий збій у роботі сенсорного пристрою.

Системні аналітики, які підтримують можливість накопичувати інформацію про стан структурної одиниці та формувати прогностні значення параметрів, що відображають їх стани з низькою помилкою ймовірності, називаються предиктивним. Неоднорідність великого обсягу даних та існуючі методи обробки діагностичних даних безпосередньо пов'язані з реалізацією систем передиктивної аналітики. Тому на етапі проектування такої системи важливо провести огляд та аналітичну роботу існуючих підходів до організації типових структур систем обробки діагностичної інформації, вибору діагностичних моделей на основі обробки технологічних рядів, та методів підтримки прийняття рішень, що формують прогнозовані подання на основі накопичених діагностичних даних.

## 2.1 Аналіз типових структур систем обробки діагностичної інформації у мережі інтернету речей

У систему предиктивної аналітики на вхід надається телеметрична інформація в неструктурованому вигляді, що надходить у режимі реального часу, що відображає поточний стан обладнання вимірювальних пристроїв, що функціонують на сенсорному рівні.

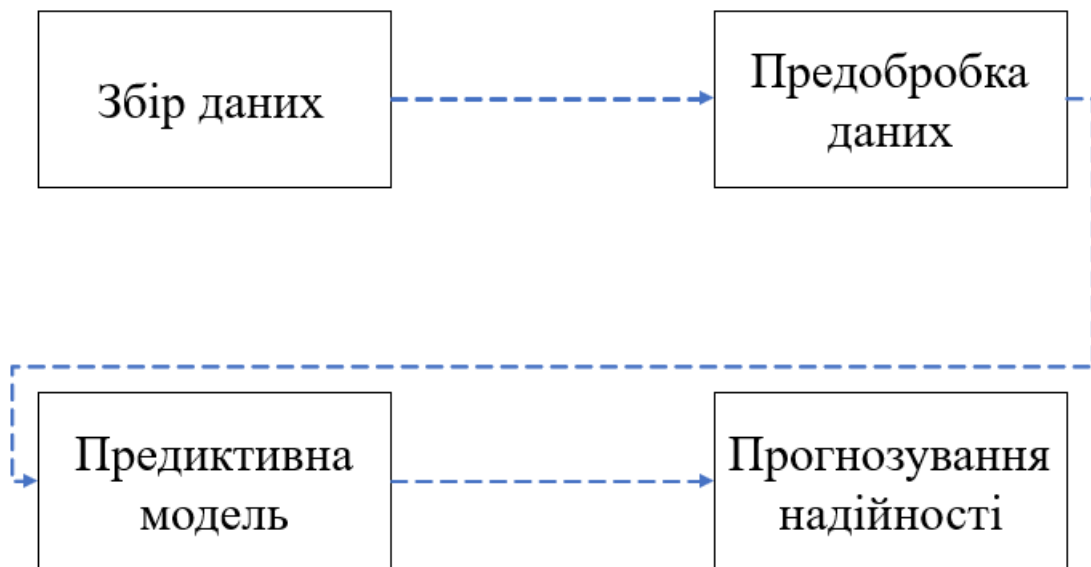


Рисунок 2.1 – Процес обробки даних в системі предиктивної аналітики

Для типової системи предиктивної аналітики є нижче представлена послідовність обробки діагностичної інформації:

- імпорт діагностичних даних у систему передиктивної аналітики;
- перетворення та підготовка діагностичних даних до неї обробці;
- кластеризація завантажених діагностичних даних для виявлення патерну їхнього розподілу;
- завантаження кластеризованих даних у прогнозу модель з закладеними у неї алгоритмами передиктивного аналізу;

- формування трендів за завантаженими даними на підставі накопиченої інформації про стан пристроїв для діагностичних параметрів, що відбивають стан компонентів;

- формування прогнозних значень для діагностичних параметрів на технологічному часовому ряду. Якість прогнозування технічного стану вимірювальних пристроїв безпосередньо залежить від архітектури та функціональних можливостей, закладених у систему передиктивного аналізу.

На рисунку 2.1 відображено основні процеси обробки даних, які закладені у систему передиктивного аналізу системи моніторингу довкілля, діагностує та прогнозує технічний стан вимірювального обладнання на сенсорному рівні.

Оброблювані дані не однорідні, і представлені різними типами, структурою передачі даних, а також способами їх зберігання та уявлення. Дані, що постійно надходять у режимі реального часу, повинні бути дискретизовані, що забезпечує достатній рівень показників якості та швидкості обробки даних у процесі передиктивного аналізу пристроїв розподіленої системи моніторингу довкілля. Дані, які надходять до системи передиктивної аналітики, повинні фільтруватися від перешкод, шумів та помилок, щоб одержувана сукупність аналізованих даних була найчистішою основою для наступного синтезу, чи корекції моделі, відповідальної за передиктивне обслуговування.

Сама сукупність аналізованих даних має бути представлена в нормалізованому та рівномірному вигляді. У разі, якщо базових алгоритмів передобробки даних недостатньо для нормалізації дата-сету, можуть бути використані допоміжні методи та моделі, що відповідають за нормалізацію вхідного потоку діагностичних даних.

На структурній схемі системи обробки діагностичної інформації відображеної на рисунку 2.2, представлені задіяні системи, підсистеми, інформаційні потоки та потоки даних, які здатні забезпечити передиктивне обслуговування проектованої сенсорної мережі.

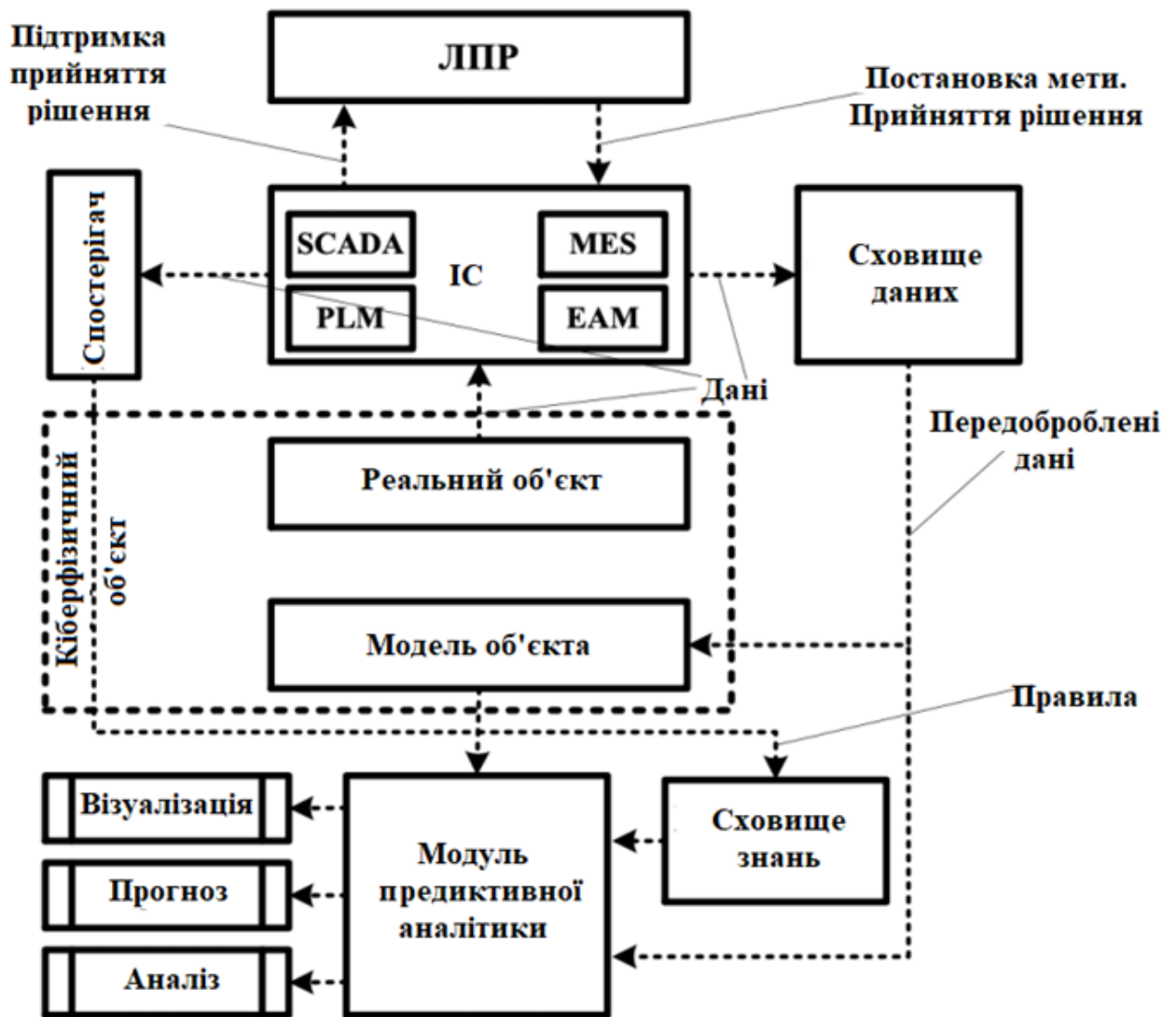


Рисунок 2.2 – Структура типової системи обробки діагностичної інформації

Дані з датчиків, вбудованих у вимірювальні пристрої, надходять у відповідний комплекс інформаційних систем, які відповідають за забезпечення роботи в реальному часі підсистем збору, обробки, відображення та архівування інформації про об'єкт моніторингу або управління. Дані доступні в повній мірі особам, тим, хто приймає рішення щодо постановки завдань на обслуговування несправних пристроїв. Та інформація, що подається на вхід у режимі реального часу на формування прогнозів, утворює статус перед оброблених даних. Ті дані, що розраховуються за діагностичною моделлю об'єкта, вже в зрештою надходять на вхід системи предиктивної аналітики.

## 2.2 Аналіз діагностичних моделей для обробки технологічних часових рядів

Найбільш значущим кроком у предиктивній аналітиці є здатність системи здійснювати детектування аномалій. Аномаліями визначаються відхилення значень у діагностичних даних від нормальних, що відбивають нормальний перебіг експлуатаційного процесу. Це можуть бути такі відхилення параметрів, як збільшення тривалості тієї чи іншої стадії експлуатаційного процесу, або зміна параметрів стану, що перевищує допустимі значення.

Завдяки моделюванню можливих ймовірнісних сценаріїв у експлуатаційному процесі, можна допускати виходячи з розрахунків, що будь-який з компонентів вимірювального пристрою вийшов з ладу, або працює в нестандартному режимі.

Нехай дано багатовимірний часовий ряд  $X = \{x_1, x_2, \dots, x_L\}$ , де кожен елемент  $x_t \in R_m$  -  $m$ -мірний вектор, який представляє свідчення стану компонентів вимірювального пристрою  $m$  на момент часу  $t$ . Частина сигналів  $x(c) \in R_c$  може надходити з датчиків управління,  $t$  а частина  $x(r) \in R_r$  -  $c$  відгуків,  $m=r+c$ .

Перші визначаються через розрахункові алгоритми базової логіки роботи пристроїв, другі формують показники фактичного порядку з навколишнього середовища. необхідно кожному моменту часу  $t$  поставити у відповідність деяке число  $a_t \in R$ , яке називається рейтингом аномальності, що показує наскільки нетипові нині значення часового ряду.

В даному випадку варто уточнити, що у навчальній вибірці не повинно бути аномальних значень, тому що аномалії можуть бути в невизначених значення і є довільними, без наявності тих чи інших загальних ознак. Саме це визначає їх як дані, які не групуються в єдиний клас за загальною ознакою та вимагають кластеризації у передобробці.

Тимчасові ряди  $X_1$  та  $X_2$  можуть бути різної довжини  $L_1 \neq L_2$ , як і кількість компонентів вимірювальних пристроїв  $m_1 = m_2 = m$ , так як наповненість функціонуючого пристрою є постійним критерієм. Якщо довжина тимчасового ряду занадто велика, тимчасовий ряд можна розбити на підряди меншої довжини, спираючись на допустимі та можливі обчислювальні ресурси та специфіку розв'язуваної задачі.

Для виявлення аномалій даних є велика кількість різних моделей, сформованих у відповідність до спеціалізації вирішуваного завдання, але в їх основу закладені базові діагностичні методи, що базуються на математичні принципи. Методи для теоретичного аналізу різних станів вимагають результатів безлічі станів  $N$ , сформованих у період експлуатації системи або на основі змодельованих даних.

Діагностичні методи в обробці технологічних рядів часу визначено набором стандартних підходів, наведених нижче:

- класифікація;
- кластеризація;
- статистичний аналіз;
- метод найближчого сусіда;
- спектральні методи;
- гібридні методи.

На підставі методу класифікації закладено припущення, що коректну роботу системи можна визначити одним або відразу декількома класами. Саме тому екземпляр, який не належить до таких класів, буде відхиленням. Пошук аномалій організований у дві послідовні ітерації – навчання та розпізнавання. Набір маркованих даних подається на навчання класифікатора, завдяки чому формується уявлення про належність аналізованих даних до раніше навченого класу.

У випадку, якщо аналізовані дані не відповідатимуть раніше навченому класу, такі дані будуть позначені як аномальні. Методи на основі кластеризації формують згруповані дані щодо ознакою схожості екземплярів

у кластери без необхідності мати уявлення про властивості можливих відхилень.

Виявлення аномалій відбувається на підставі одного з можливих припущень

- примірники даних, визначені як нормальні, співвідносять з кластером, проте ті викиди, які неможливо співвіднести з кластером, визначаються як аномалії. Особливість цього підходу не гарантує коректну інтерпретацію результуючої вибірки, оскільки проблема визначення меж кластерів може стати критичною для певного виду вибірок;

- у зв'язку зі складністю визначення кластерних кордонів, сформовано уявлення про нормальність даних у кластері виходячи з них віддаленості від центру: чим дані в кластері ближче до центру, тим більше нормальними вони визначені, водночас у разі сильної віддаленості від центру, дані будуть позначені як аномальні;

- у разі, якщо розподіл даних утворює відразу кілька кластерів, то ознака нормальності визначається найбільших кластерів, а кластери з меншою наповненістю видаються як аномальні. Сценарій застосування статистичного аналізу визначається підходом, при якому проводиться дослідження технологічного процесу, формується модель і зв'язок у ньому, а потім реальна робота системи порівнюється з її реальною поведінкою.

У разі, якщо спостерігається різниця змодельованої та реальної роботи системи, визначається функція аномальності, і формується висновок про те, що в системі можуть бути збої та відхилення у роботі.

Алгоритм найближчого сусіда базується на основі уявлення про міру схожості між об'єктами, що досліджуються. Як приклад можна привести Евклідову відстань.

Підходи в алгоритмах найближчого сусіда засновані на нижче поданих припущеннях:

- відстань до найближчого об'єкта досліджуваних даних визначено всім екземплярів класу, закладених для тестування. Той екземпляр, що

найбільш віддалений від найближчого об'єкта, визначається як викид, що ознакою аномальності;

- застосування такого поняття, як відносна щільність, формується з оцінки щільності на околицях кожного з досліджуваних екземплярів даних. Той екземпляр, що розташований на околицях з низькою щільністю, визначається як аномальний. Примірник, розташованої в області з високою щільністю, визначається як нормальний.

Спектральні методи знаходять апроксимацію даних, використовуючи комбінацію атрибутів, які передають більшу частину варіативності в даних. Дані методи найбільш застосовні в операціях, що відповідають за передобробку даних, та найбільш ефективні в комбінації з іншими алгоритмами, відповідальними за передобробку даних. Гібридні методи включають комбінації відразу декількох методів розпізнавання аномалій, поєднуючи у своїй переваги кожної їх. Додатково варто зазначити, що техніка застосування методик може бути як послідовна, так і паралельна. Це дозволяє досягати усереднення у результатах аналізу.

### 3 РЕАЛІЗАЦІЯ ДІАГНОСТИЧНОЇ МОДЕЛІ

Для реалізації діагностичної моделі розпізнавання збоїв та неполадок, що виникають на ділянці мережі інтернету речей, що відповідає за надійну роботу вимірювальних пристроїв у розподіленій автоматизованій системі моніторингу навколишнього середовища, потрібно:

- визначити та змодельовати конфігурацію вимірювальних пристроїв, а також організацію їх внутрішньої та зовнішньої взаємодії;
- розробити структуру інтелектуальної системи технічного діагностування та обробки інформації;
- розробити функціональну та логічну модель системи технічного діагностування та обробки інформації;
- обрати алгоритм розпізнавання неполадок;
- інтегрувати розроблену діагностичну модель розпізнавання неполадок, що виникають на ділянці мережі.

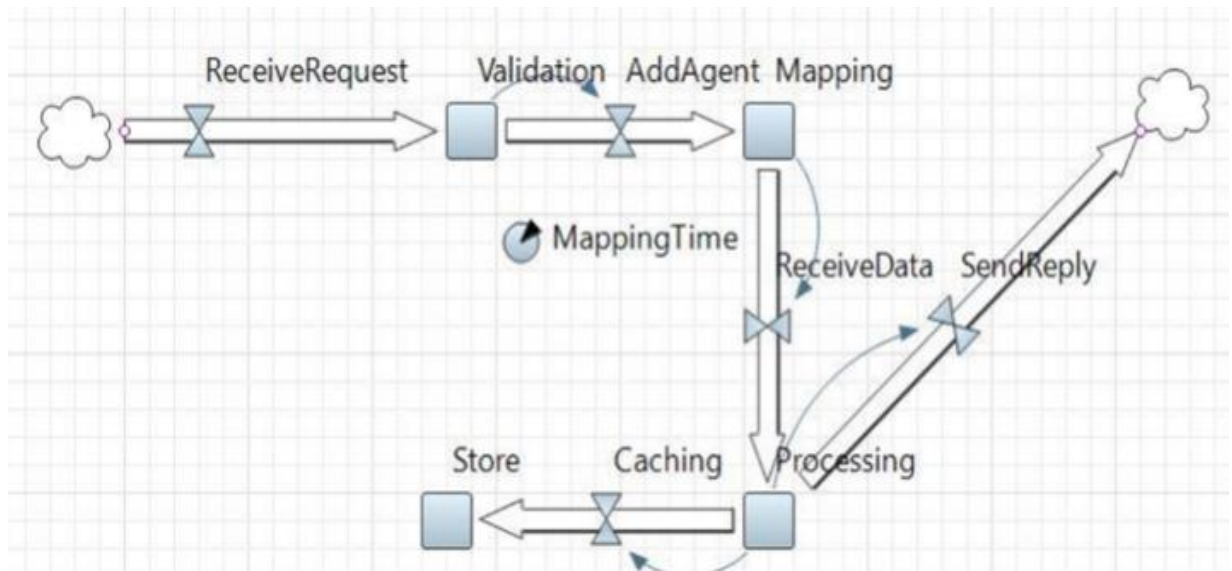


Рисунок 3.1 – Реалізація імітаційного моделювання. Процес функціонування периферійного обладнання у вимірювальному пристрої

Мультиагентне моделювання інформаційної взаємодії, засноване на Agent-based model дозволяє виконати дослідження, що визначає поведінку децентралізованих агентів та поведінку всієї системи в цілому на даній ділянці інженерної мережі, що є найбільш релевантним для розподіленої системи пристроїв, які забезпечують моніторинг екологічної ситуації у навколишньому середовищі. Для реалізації імітаційного моделювання вирішено використати програмний засіб AnyLogic. Змодельована структура та процес функціонування периферійного обладнання вимірювального пристрою представлено на рисунку 3.1.

Наведена на рисунку 3.1 модель функціонує таким чином, що вхідні запити від периферійних пристроїв надходять хаотично. У разі, коли валідація та сертифікація прийомопередавальної інформації здійснена успішно при першому виявленні пристрою в мережі, ідентифікаційні дані пристрою додаються до карти мережі та надалі ідентифікується як надійне привілейоване джерело.

Після того, як отримана інформація оброблена та збережена, здійснюється відправка відповідної команди на сервер, після чого на рівні нотифікацій здійснюється відмітка про отримання. На рисунку 3.2 зображено вікно конфігурації програмного засобу AnyLogic, в якому відображено роботу змодельованого процесу імітаційної взаємодії.

В результаті здійсненого моделювання були розраховані та виявлені ключові проблеми з урахуванням особливості обраної топології IoT – мережі, що використовується при реалізації системи моніторингу навколишнього середовища, вони наведені нижче:

- внаслідок виникнення колізій джерел даних, запити агента на здійснення передачі даних періодично можуть бути відхилені, що враховується в архітектурній складовій системи, що розробляється;

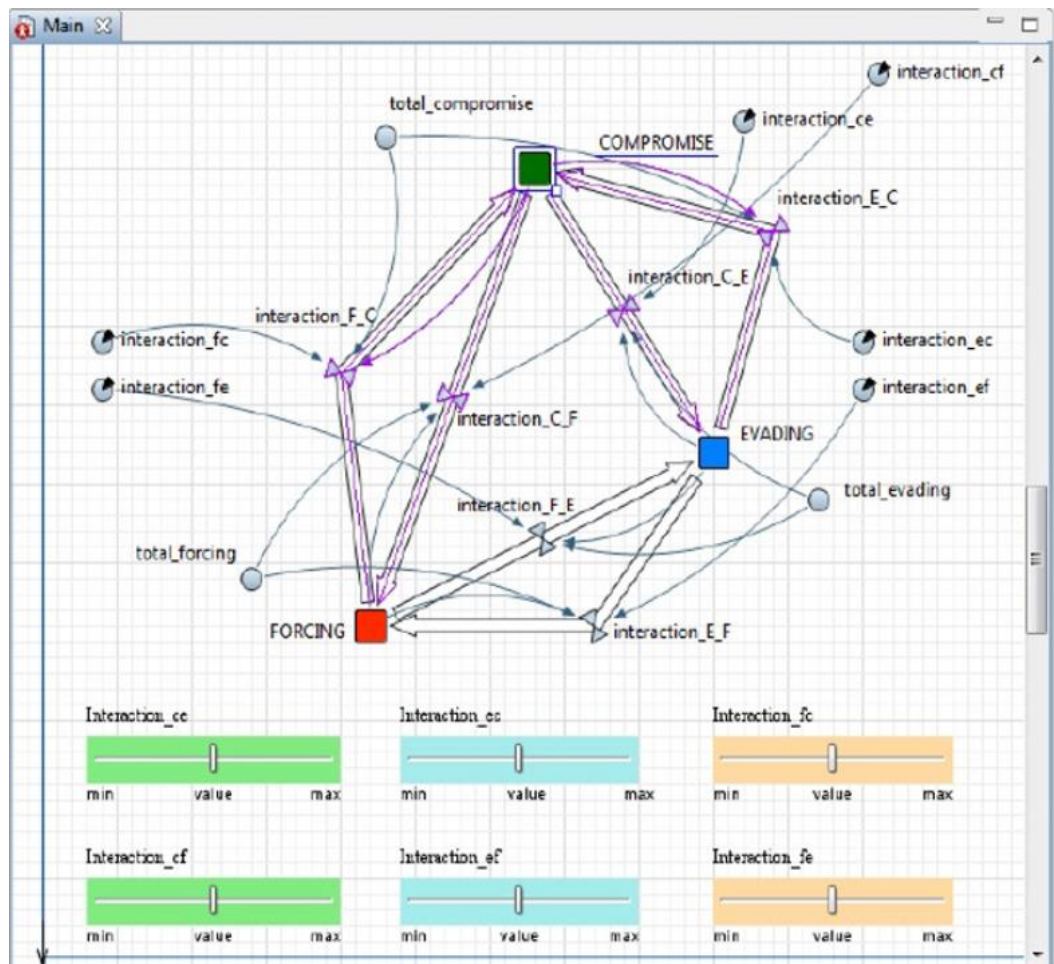


Рисунок 3.2 – Процес функціонування периферійного обладнання у вимірювальному пристрої

- можливе дублювання одного і того ж периферійного пристрою в топологічній карті мережі, що вирішується шляхом автоматичного видалення пристрою, якщо від нього за вказаний проміжок часу не надійшла відповідь;
- у випадку, якщо пристрій не може надіслати дані, що може виражатися в полемці вимірювального периферійного обладнання, у відсутності даних, система повторно пропонуватиме здійснити цю дію до тих пір, поки команда не буде виконана, або якщо у логіці пристрою зумовлено максимальну кількість спроб, які необхідно здійснити;
- коли запит успішно подолав збудований маршрут, інформаційна взаємодія вважається здійсненою. Змодельовавши та активуючи такі режими, як режим опитування, переривань, і, що особливо важливо, множинного

доступу, проведений аналіз дає уявлення про те, до яких параметрів слід приділити максимальну увагу при подальшій розробці алгоритмів взаємодії на всіх задіяних рівнях топології IoT – мережі для розгортання комплексу підсистем розподіленої системи моніторингу довкілля.

У числі певних параметрів, найбільш очевидними стали такі, як кількість сенсорних пристроїв, формат передачі та пакета даних, середній час передачі даних при ймовірнісній оцінці в умовах потенційного виникнення колізій на кожній з активних ділянок мережі у процесі передачі.

### 3.1 Розробка структури інтелектуальної системи діагностування

Для своєчасного обслуговування комплексу вимірювальних пристроїв важливо приділити особливу увагу структурі інтелектуальної системи, відповідальної за діагностування та обробку інформації. Показники, які характеризують надійність роботи пристрою та його периферійного обладнання, є одночасно і показниками системи технічної діагностики, і водночас самим об'єктом діагностування. Це твердження працює і у зворотний бік – діагностика об'єкта виконується на боці системи технічної діагностики, що формує складність у розділення ознак системи від безпосередньо самого об'єкта діагностування. Запит на діагностування формується виходячи із стратегії, яка визначає процес експлуатації системи та її обслуговування. Під обслуговуванням розуміється управління станом усіх задіяних компонентів у системі.

Система технічного діагностування визначає нижче представлений набір складових:

- об'єкт діагностування, робота якого вимагає контролю, а елементи, з яких він складається, мають бути ідентифіковані;
- діагностичні засоби, що являють собою набір контрольно-вимірювальної периферії, органів управління, комутаційних засобів та можливостей сполучатися з об'єктом діагностування;

- програмне забезпечення, що відповідає за обробку, трансляцію та збереження результатів діагностики, щоб надалі використовувати їх для побудови прогнозів у поведінці, а також стан об'єкта діагностики.

Програмне забезпечення є найбільш пріоритетною складовою у системі технічної діагностики, оскільки саме вона відповідає за належне якість її роботи. Програмне забезпечення технічної діагностики включає в себе:

- модуль, що відповідає за діагностику, який співвідносить поточний стан периферійного обладнання до одного з можливих, закладених у його потенційних діагнозів;

- діагностичні засоби, що являють собою набір контрольно-вимірювальної периферії, органів управління, комутаційних засобів та можливостей сполучатися з об'єктом діагностування;

- база даних, в якій акумульовані всі можливі відомості щодо діагностичних ознак, а також наперед визначені максимально допустимі значення станів, що відображають перед відмовним статусом об'єкта діагностування. У базі даних обов'язково відображається всі безлічі станів обладнання;

- підсистема, що відповідає за збирання інформації про можливі нові діагностичних ознаках, та наповненням бази даних оновленим сформованим переліком таких;

- математичні моделі діагностування, за допомогою яких здійснюється реалізація безпосередньо самого діагностування, з застосуванням відповідних методів та можливістю надалі порівнювати результати діагностики;

- алгоритми навчання використовуваних математичних моделей діагностування, в основу яких закладаються технології машинного навчання;

- для відображення зведеної інформації про стан системи та об'єктів діагностування, використовується модуль відображення результатів діагностики.

На рисунку 3.3 відображено структуру інтелектуальної системи технічного діагностування та обробки інформації, реалізованої в розподіленій автоматизованій системі моніторингу довкілля, здійснює діагностику стану вимірювальних пристроїв та їх периферійне обладнання.

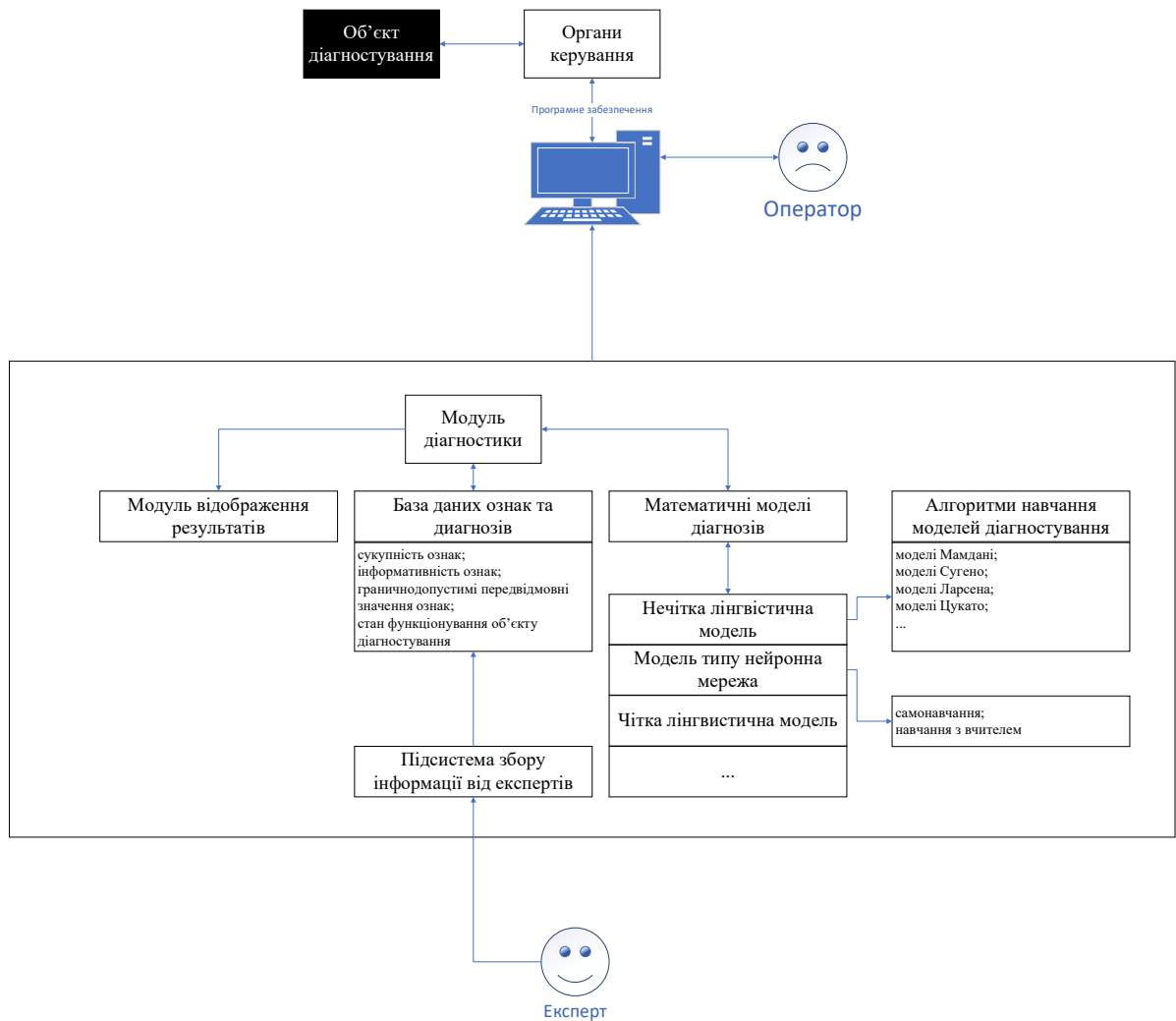


Рисунок 3.3 – Структура системи технічного діагностування та обробки інформації

### 3.2 Інтеграція нейронної мережі

Нейронна мережа, яка інтегрується в систему обробки інформації, здійснює аналіз даних у режимі реального часу з наступною обробкою результуючих вибірок для передиктивного обслуговування вимірювальних

пристроїв, реалізована з урахуванням LSTM – моделі. Для того, щоб вирішити зазначене завдання, було зібрано обчислювальний комплекс, що працює за протоколом MQTT. Вироблено збирання та налаштування IoT-модему, що працює за MQTT протоколом та передає дані через нього на брокер.

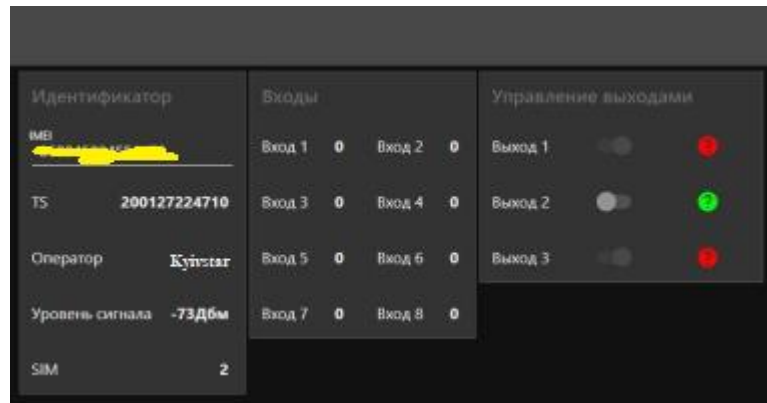


Рисунок 3.4 – Налаштований IoT-модем

LSTM мережі – це модифікація рекурентних нейронних мереж, в основу проектування яких закладено можливість уникати проблеми, пов'язані із довгостроковими залежностями. Методом зворотного розповсюдження помилки вдалося виключити проблему, що викликає зникнення, або критичні перевищення градієнтів у процесі навчання.

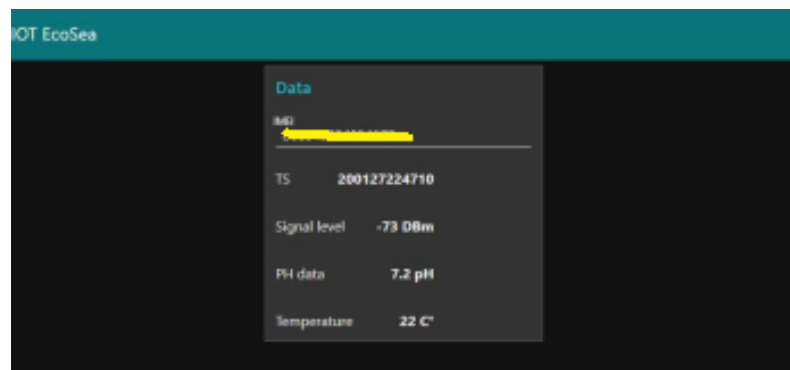


Рисунок 3.5 – Відображення клієнтської частини

Підключено вимірювальний пристрій, що відстежує кислотність рідини та її температуру, а також брокера, що обробляє вступну напругу з вимірювального пристрою (рисунок 3.6).

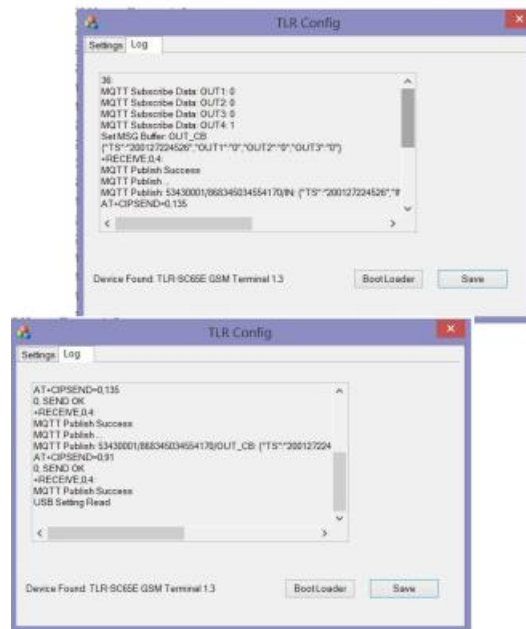


Рисунок 3.6 – Налаштований брокер

Схема будь-якої рекурентної нейронної мережі виглядає як ланцюжок модулів, що повторюються.

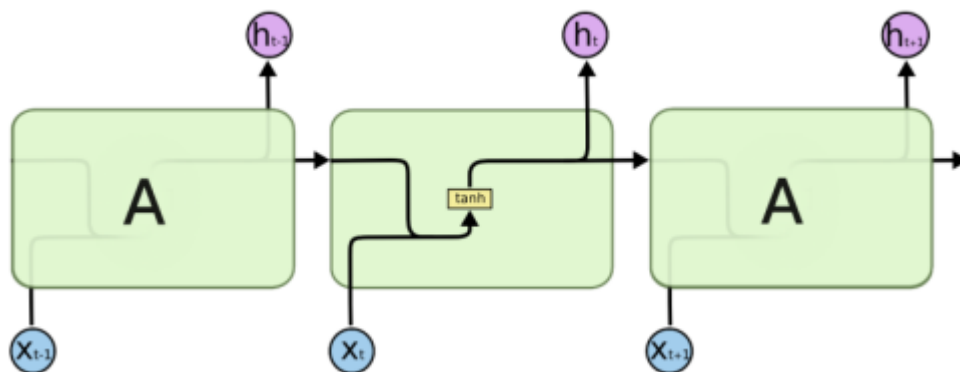


Рисунок 3.7 – Структура стандартної рекурентної нейронної мережі

Структура стандартних рекурентних нейронів мереж представлена досить просто, тому що в ній присутній лише один шар гіперболічного тангенсу. Типову структуру стандартної рекурентної нейронної мережі зображено на рисунку.

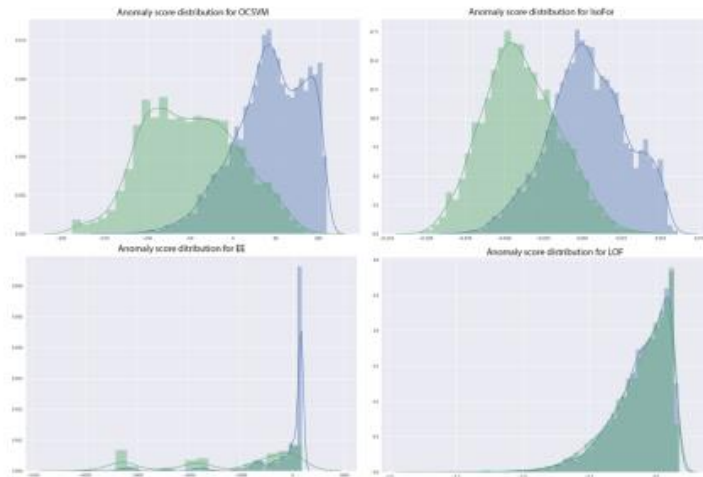


Рисунок 3.8 – Результати роботи

Для кожної окремої ситуації потрібно протестувати відразу кілька алгоритмів пошуку аномалій, щоб вибрати найбільш підходящий для поставленого діагностичного завдання.

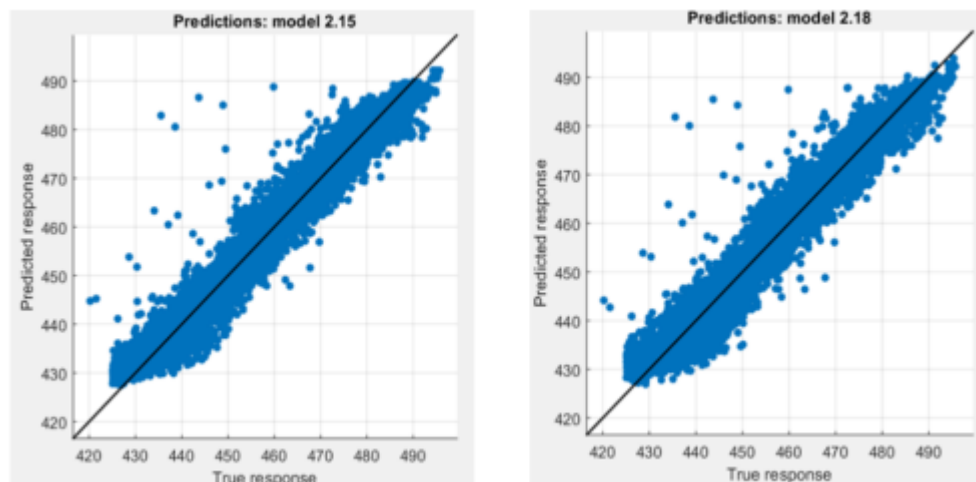


Рисунок 3.9 – Результати роботи

В основу для проведення експерименту відібрано методи One Class SVM (OCSVM), IsolationForest (IF), EllipticEnvelope (EE) і LocalOutlierFactor (LOF), на вхід яким забезпечені дані, сформовані на підставі проведеного імітаційного моделювання з варіативними сценаріями поломки та виходів з ладу компонент вимірювального пристрою(рисунку 3.8, 3.9). Для підвищення точності прогнозування обраної нейромережевої моделі, потрібно було провести додаткове дослідження, застосувавши на тестовий вибір методів бегінга дерев і за SVM.

## ВИСНОВКИ

В ході підготовки кваліфікаційної роботи проведено аналіз методів обробки даних у мережах IoT для передиктивного обслуговування у розподіленій автоматизованій системі моніторингу. Проведено аналіз технології IoT, а також існуючих методів обробки даних в IoT. Розроблено метод розпізнавання неполадок у мережі IoT з використанням штучних нейронних мереж.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Храмцов, П. Всеосяжний Інтернет: прогнози та реальність [текст]/П. Храмцов// Відкриті системи. СУБД. - 2013. - №4. - С. 19-22.
2. Чеклецов, В.В. Почуття планети (Інтернет Речів та наступна технологічна революція) [текст]/В.В. Чеклецов. - М.: Російський дослідницький центр з Інтернету Речів, 2013. - 132 с.
3. Черняк, Л. Інтернет речей: нові виклики та нові технології [текст]/Л. Черняк// Відкриті системи. СУБД. - 2013. - №4. - С. 14-18.
4. Черняк, Л. Від перших радіометок до Інтернету речей [текст] / Л. Черняк // Відкриті системи. СУБД. - 2005. - №07-08. - С. 92-94.
5. Черняк, Л. Платформа Інтернету речей [текст] / Л. Черняк // Відкриті системи. СУБД. - 2012. - №7. - С. 44-45. ETSI TS 102690 «Machine-to-Machine комунікації (M2M); Functional architecture» [електронний ресурс], V1.1.1. - 2011. - 280 р.
6. ETSI TS 102921 «Machine-to-machine communications (M2M); m1a, d1a and m1d interfaces» V1.1.1 [електронний ресурс]. - 2012. - 538 р.
7. Internet of Things Russia [електронний ресурс]. - Режим доступу: <http://internetofthings.ru>
8. ISO/IEC 18092:2004. Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1) [електронний ресурс].
9. ITU-T Rec. Y.2060 (06/2012): Overview of the Internet of things [електронний ресурс]. Вишневський, В. Mesh-мережі стандарту IEEE 802.11s – технологи та реалізація [текст]/В. Вишневський, Д. Лаконцев, А. Сафонов, С. Шпілев// Перша миля. - 2008. - №2-3. - С. 26-31.136
10. Восков, Л.С. Web речей – новий етап розвитку інтернету речей [Текст]/Л.С. Восков, Н.А. Пилипенко // Якість. Інновації. Утворення. - 2013. - № 2. - С. 44-49.

11. Гайкович, Г.Ф. Стандартизація в галузі промислових мереж. Розвиток бездротових стандартів для АСУ ТП [Текст]/Г.Ф. Гайкович // Електронні компоненти. - 2009. - №1. - С. 48-53. Barry Naughian, “De-sign, Launch, and Scale IoT Services” // Apress – 2018, pp. 194-220
12. Perry Lea, “Internet of Things for Architects” // Packt Publishing – 2018, pp. 410-422 12. Dominique D. Guinard, Vlad M. Trifa, “За допомогою Web до Build the IoT” // Manning - 2016, pp. 144-161
13. Anand Tamboli, “Build Your Own IoT Platform” // Apress – 2019, pp. 65-84
14. Gaston C. Hillar, “Hands-On MQTT Programming with Python” // Packt Publishing - 2018, pp. 92-113
15. Jeff Mesnil. Mobile and Web Messaging. O’Reilly Media, Inc., 2014 ISBN 978-1-4919-4480-6 - II. MQTT, pp 43-47
16. Bryan Boyd та ін. Building Real-time Mobile Solutions with MQTT and IBM MessageSight. IBM Redbooks, 2014, p.38
17. Gerard Blokdyk, “MQTT: A Concise and Practical Tutorial” // Paperback – November 5, 2017, pp. 25-32
18. Ousmane Sadio, Ibrahima Ngom, Claude Lishou “Lightweight Security Scheme for MQTT/MQTT-SN Protocol” //
19. Sadio, O., Ngom, I. and Lishou, C., 2019. Lightweight Security Scheme For MQTT/MQTT-SN Protocol - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: <<https://ieeexplore.ieee.org/document/8939177>> [Accessed 29 березня 2021]
20. Дяченко В.О., Лебедев О.Г., Петченко Б.І. Обробка даних в IoT// Проблеми інформатизації : десята міжнародна науково-технічна конференція. Черкаси – Баку – Бельсько-Бяла – Харків, 2022, т.2, с.94.