НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
«Інститут прикладного системного аналізу»
(повна назва інституту/факультету)

Кафедра системного проектування
(повна назва кафедри)

«На правах рукопису»
УДК _004.852

«До захисту допущено»

Завідувач кафедри
_____ _А.І. Петренко
(підпис) (ініціали, прізвище)
“___”_____20__ р.

Магістерська дисертація

зі спеціальності (спеціалізації)__122 – комп’ютерні науки та інформаційні технології (Інформаційні системи і технології проектування)_____
(код і назва спеціальності)

на тему: Шлюз в архітектурі Інтернету речей

Виконав: студент _6_ курсу, групи ДА-61м
(шифр групи)

Шеренковський Артем Олегович _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник __доцент, к.т.н., Гіоргізова-Гай В.Ш._____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант

Розроблення стартап-проекту доц., к.т.н., Гіоргізова-Гай В.Ш. _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Інститут/факультет ННК «Інститут прикладного системного аналізу»
(повна назва)

Кафедра Системного проектування
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною (освітньо-науковою) програмою

Спеціальність (спеціалізація) 122 – комп'ютерні науки та інформаційні технології (Інформаційні системи і технології проектування)
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ А.І. Петренко
(підпис) (ініціали, прізвище)
«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Шеренковському Артему Олеговичу
(прізвище, ім'я, по батькові)

1. Тема дисертації «Шлюз в архітектурі Інтернету речей»
науковий керівник дисертації Гіоргізова-Гай В.Ш., к.т.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «27» березня 2018 р. №_____

2. Строк подання студентом дисертації 10 травня 2018

3. Об'єкт дослідження Шлюз Інтернету речей

4. Предмет дослідження Можливості та місце шлюзу у сучасних IoT архітектурах

5. Перелік завдань, які потрібно розробити провести аналіз сучасного ринку Інтернету речей, провести аналіз існуючих моделей архітектур IoT та виділити місце шлюзу у них, зробити перелік основних функцій і характеристик шлюзів та провести огляд рішень відомих виробників

6. Орієнтовний перелік публікацій Аззуз І.А., Бужак Ю.Ю., Шеренковський А.О. Платформи для Інтернету речей // XIV міжнародна науково-практична конференція. – 2016. – №12. – С. 241-246.

Гіоргізова-Гай В.Ш., Шеренковський А.О. / Шлюзи в системах IoT // 20-а Міжнародна науково-технічна конференція SAIT 2018, - 2018 – С. 217-218__

7. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Реалізація стартап-проекту			

8. Дата видачі завдання __01.02.2018_

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Отримання завдання	01.02.2018	
2	Збір інформації та аналіз літератури	15.02.2018	
3	Проведення аналізу ринку Інтернету речей	28.02.2018	
4	Проведення аналізу архітектури IoT рішень	11.03.2018	
5	Проведення аналізу IoT платформ	13.04.2018	
6	Проведення огляду IoT шлюзів від відомих виробників	25.04.2018	
7	Оформлення дипломної роботи	30.04.2018	
8	Отримання допуску до захисту та подача роботи в ДЕК	09.05.2018	

Студент _____ _Шеренковський А.О.._
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _Гіоргізова-Гай В.Ш.__
(підпис) (ініціали, прізвище)

РЕФЕРАТ НА МАГІСТЕРСЬКУ ДИСЕРТАЦІЮ

виконану на тему: Шлюз в архітектурі Інтернету речей

студентом: Шеренковський Артемом Олеговичем

Робота виконана на 113 сторінках, містить 15 ілюстрацій, 24 таблиць. При підготовці використовувалась література з 32 джерел.

Актуальність теми

Ринок Інтернету речей зараз дуже швидко, проте хаотично розвивається, а його прибуток вимірюється трильйонами доларів. Неконтрольований зріст популярності технології призвів до геометричного росту кількості пристроїв, що використовують мережу, що накладає обмеження на використання хмарних сервісів у IoT. Виробники винайшли рішення у розміщенні потужного пристрою на краю Інтернету - шлюзі. Проте, не дивлячись на велику кількість публікацій на теми IoT, в них немає ні чітко виділених функції, які повинен виконувати шлюз, ні критеріїв, які б допомогли у виборі рішень від великої кількості виробників.

Тому дослідження даної технології, а також виділення основних характеристик і функції шлюзу для Інтернету речей, є актуальним напрямком досліджень саме на сьогоднішній день, у час, коли все швидко змінюється, а єдиного підходу до використання шлюзу не існує.

Мета та задачі дослідження

Метою даної роботи є аналіз архітектур IoT та місце у них шлюзу і його функціональності. Результатом проведених досліджень є виділення критеріїв класифікації та порівняння, котрі допоможуть у виборі шлюзу для IoT рішення.

Рішення поставлених завдань та досягнуті результати

У даній роботі було розглянуто сучасний IoT ринок і виділено причини, чому з’явилась потреба у проміжній ланці між хмарою та речами – шлюзі. Проведено аналіз основних моделей архітектури та виділено функціональність та місце шлюзу у кожній з них. Також у роботі було виділено основні функції, які повинна виконувати IoT-платформа.

Надалі було виділено основні функції, котрі повинні виконувати IoT шлюзи,

та критерії порівняння для обрання найбільш підходящого для певної реалізації рішення Інтернету речей. Надалі було проведено огляд шлюзів від лідерів ринку та ряду маловідомих виробників. Виділено ключові особливості кожного з них. На основі цих даних було представлено проект реалізації розумного будинку із використанням IoT шлюзу.

Об’єкт досліджень

Шлюз IoT.

Предмет досліджень

Функціональність та критерії порівняння шлюзів IoT при реалізації проектів

Методи досліджень

Для вирішення проблеми в даній роботі використовуються методи системного аналізу, порівняння, логічного узагальнення результатів.

Наукова новизна

Наукова новизна роботи полягає у створенні критеріїв класифікації та порівняння шлюзів IoT, бо наразі відсутні стандарти його використання при розробці рішень для Інтернету речей.

Практичне значення одержаних результатів

Отримані результати можуть використовуватись при виборі архітектур, визначенні необхідної функціональності шлюзу, та виборі його за критеріями, що були виділенні в ході даної роботи

Публікації

Аззуз І.А., Бужак Ю.Ю., Шеренковський А.О. Платформи для Інтернету речей // XIV міжнародна науково-практична конференція. – 2016. – №12. – С. 241-246.

Гіоргізова-Гай В.Ш., Шеренковський А.О. / Шлюзи в системах IoT // 20-а Міжнародна науково-технічна конференція SAIT 2018, - 2018 – С. 217-218

Ключові слова

Шлюз, Інтернет речей, моделі архітектури, критерії порівняння, туманні обчислення.

ABSTRACT ON MASTER'S THESIS

on topic: Gateway in the IoT architecture

student: Artem O Sherenkovskiy

Work carried out on 113 pages containing 15 figures, 24 tables. The paper was written with references to 32 different sources.

Topicality

Nowadays the IoT market grows very fast, but chaotically and its profit is measured by trillions of dollars. The uncontrolled increase of the technology popularity has led to a geometric increase in the number of devices that are using the network. As a result, it imposes restrictions on the use of cloud services in the IoT. Manufactures invented the solution in placing the powerful device on the edge of the Internet - the gateway. However, there are still no criteria by which to choose a gateway and the functions that it must perform.

Therefore, the study of this technology, as well as the allocation of the main characteristics and functions of the gateway for the Internet of Things, is an actual direction of research for today, at a time when everything is changing rapidly, and there is no single approach to the use of the gateway. However, despite the large number of publications on the IOT topics, there is no clearly-defined functions that the gateway must perform, nor criteria that would help to select devices from a large number of manufacturers.

Purpose

The purpose of this work is to analyze the architectures of the IoT and the location of the gateway and its functionality. The result of the research is the selection of criteria for classification and comparison, which will help in choosing the gateway for IoT solutions.

Solution

The modern IOT market was considered in this paper. The reasons why there was a need for an intermediate link between the cloud and things - the gateway, were highlighted. The analysis of the basic architectural models and the distinguished

functionality and location of the gateway in each of them were carried out. The work outlined the main functions that the IoT platform must perform.

The main functions that IOT gateways should perform were determined. The comparison criteria to select the most appropriate for a particular implementation of the Internet solution were highlighted. A survey of gateways from market leaders and little-known manufacturers was conducted. The key features of each of them were highlighted. A project to implement a smart home using the IoT gateway was presented based on these data.

Object of research

IoT gateway

Subject of research

Functionality and criteria for comparison of the IoT gateways in the projects implementation.

Research methods

To solve the problem in this paper were used methods of analysis and synthesis, system analysis, comparison, logical generalization of results.

Scientific novelty

The scientific novelty of the work is to create criteria for the classification and comparison of the IoT gateways because there are currently no standards for its use in developing solutions for the Internet of Things.

The practical value of the results

The obtained results can be used in selection architectures, determining the necessary functionality of the gateway, and the selection of it according to the criteria that were allocated during the given work.

Publications

Azzuz I.J., Buzhak Y.Y., Sherenkovskiy A.O. Iot Platforms // XIV International scientific-practic conference. – 2016. – №12. – P. 241-246.

Hiorhizova-Hai V.S. Sherenkovskiy A.O / Gateways in IoT systems // 20-th International Conference SAIT 2018, - 2018 – P. 217-218

Keywords

Gateway, Internet of Things, architecture models, comparative criteria, fog

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ 11

ВСТУП 12

1 АНАЛІЗ РИНКУ IOT 14

1.1 Визначення IoT 15
1.2 Сфери використання IoT. 16
1.3 Необхідність шлюзу в IoT 22
1.4 Висновки 23

2 СТАНДАРТИ СУМІСТНОСТІ IOT 25

2.1 Еталонна модель IoT від MCE-T 26
2.2 Еталонна модель від Всесвітнього форуму IoT 35
2.3 Інші еталонні моделі 42
2.3.1 Модель NIST Special Publication 800-183 43
2.3.2 Модель Industrial Internet of Things Reference Architecture 44

2.4 Висновки 48

3 IOT ПЛАТФОРМИ 51

3.1 Огляд платформи Linux Foundation 53
3.2 Огляд платформи AggreGate 56
3.3 Огляд платформи Everyware Cloud 60
3.4 Висновки 63

4 ОГЛЯД МОДЕЛЕЙ ШЛЮЗІВ ВІДОМИХ ВИРОБНИКІВ 64

4.1 Огляд шлюзів компанії Eurotech 67
4.2 Огляд шлюзів компанії Intel 68
4.3 Огляд шлюзів компанії Huawei 70
4.4 Огляд шлюзів компанії Cisco 72
4.5 Огляд шлюзів компанії NEXCOM 74
4.6 Огляд шлюзів Edge Gateway компанії Dell 74
4.7 Огляд Enterprise шлюзів компанії Hewlett Packard 77

4.8 Висновки 79
5 ПРИКЛАД ПРАКТИЧНОЇ РЕАЛІЗАЇЇ 81
6 РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ «ІОТ ШЛЮЗ» 86
6.1 Опис ідеї проекту 86
6.2 Технологічний аудит проекту 87
6.3 Аналіз ринкових можливостей 88
6.4 Розробка ринкової стратегії проекту 98
6.5 Розробка маркетингової програми 102
6.6 Висновки 106
ВИСНОВКИ 108
ПЕРЕЛІК ПОСИЛАНЬ 111

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

IoT – Internet of Things (Інтернет речей)

OT – Operational Technology (Операційні технології)

IT – Information Technology (Інформаційні технології)

VoIP – Voice over IP

МСЕ (ITU) – Міжнародний союз електрозв'язку (International Telecommunication Union)

IWF – IoT World Forum (Всесвітній форум IoT)

NIST – National Institute of Standards and Technology (Національний інститут стандартів і технології)

IIC – Industrial Internet Consortium (Консорціум індустріального Інтернету)

КПК – Кишеньковий Персональний Комп'ютер

RFID – Radio frequency identification (радіочастотна ідентифікація)

LAN – Local Area Network (Локальна комп'ютерна мережа)

WAN – Wide Area Network (Глобальна мережа)

СУБД – Система управління базами даних

ВСТУП

Інтернет речей (Internet of Things, IoT) - новітній етап тривалої революції в області обчислювальних систем і засобів зв'язку, яка ще не закінчилася. Його розмір, різноманіття і вплив на повсякденне життя, комерційну діяльність і державне управління затьмарюють попередню історію технічного прогресу. IoT - це термін, яким позначається комплекс підключених один до одного інтелектуальних пристроїв, від побутової техніки до крихітних датчиків. Домінантною темою є вбудовування мобільних приймачів малого радіусу дії в різноманітні гаджети і предмети повсякденного побуту, що відкриває нові форми комунікації між людьми і речами, а також між різними речами. Сьогодні Інтернет забезпечує з'єднання між собою мільярдів промислових і побутових предметів, як правило, за допомогою хмарних систем. Такі предмети передають інформацію датчиків, діють відповідно до свого оточенням, а іноді можуть самомодифікуватись, створюючи загальну середу управління більшої системою, як завод або навіть міст [1].

«Речами» в Інтернеті речей є глибоко вбудовані пристрої з такими відмітними особливостями, як вузька смуга пропускання, збір даних з низкою повторюваністю і малий обсяг використовуваних ресурсів. Ці пристрої обмінюються даними один з одним і надають дані через інтерфейси. Деякі вбудовані пристрої IoT, такі як охоронні відеокамери високої якості, відеотелефони VoIP і деякі інші, вимагають для роботи широкої полоси пропускання. Але незліченна кількість інших продуктів вимагає передачі даних всього лише час від часу. У числі напрямків, яким підуть на користь можливості збору даних, автоматизації та аналізу, що надаються IoT, - охорона здоров'я і фітнес-індустрія, моніторинг та автоматизація житлових будинків, енергозбереження та «інтелектуальна електромережа», сільське господарство, транспорт, екологічний моніторинг, інвентаризація та управління продукцією, безпека, відеоспостереження, освіта і багато інших.

Технологічний розвиток відбувається в багатьох областях. Не дивно, що

дослідження бездротових мереж проводяться і зараз, і вже досить тривалий час, правда, раніше вони називалися інакше: мобільні обчислення, всепроникаючий комп'ютинг, бездротові сенсорні мережі і кіберфізичні системи.

Розроблено безліч пропозицій і продуктів в області енергоефективних протоколів, безпеки та конфіденційності, адресації, економічних радіо, енергозберігаючих схем для продовження терміну служби батарей, надійності мереж, складених з ненадійних і безсистемно «засинаючих» вузлів. Подібний прогрес в області бездротових технологій життєво важливий для росту IoT. Крім того, мають місце такі напрямки розробки, як надання IoT-пристроїв можливості взаємодії з соціальними мережами, використання міжмашинної взаємодії, зберігання і обробка великих обсягів інформації в реальному часі, програмування додатків, що надають кінцевим користувачам інтелектуальні і корисні інтерфейси з цими пристроями і даними.

Сьогодні велика кількість виробників пропонує компоненти для IoT рішень, серед яких важливе місце займають шлюзи. При чому, функції шлюзів і їх призначення у різних IoT проектах досить сильно відрізняються.

Загалом шлюзи IoT представляють собою мережеве обладнання, яке знаходиться на кордоні між OT (Operational Technology) – апаратно–програмними комплексами для контролю і управління фізичними процесами, та IT (Information Technology) – системами і мережами для створення, обробки, зберігання, забезпечення безпеки і обміну будь-якими формами електронних даних. Але на відміну від більш звичних для OT та IT компонентів (датчики, контролери, модеми, маршрутизатори, протоколи каналів зв’язку, IoT-платформи) аналітичні огляди для шлюзів практично відсутні. Так само, відсутні і критерії їх класифікації та порівняння, що суттєво ускладнює їх вибір при проектуванні IoT-систем.

1 АНАЛІЗ РИНКУ IOT

Ринок Інтернету речей розглядається аналітиками як найбільш перспективний в найближчому десятилітті. Прогнозований загальний економічний ефект IoT вимірюється трильйонами доларів США [31]. Тож важливо правильно визначити напрямки, у яких розвивається сфера.

За оцінками Cisco, за наступне десятиліття чистий прибуток економіки IoT складе $ 14,4 трлн [2]. Відповідно до досліджень компанії, в цьому відіграють роль п'ять основних рушійних сил:

- Використання активів ($ 2,5 трлн): IoT скорочує витрати на продажу, загальні та адміністративні витрати і вартість проданих товарів, оптимізуючи виконання і ефективність бізнес-процесів.
- Продуктивність праці ($ 2,5 трлн): IoT підвищує продуктивність праці за рахунок ефективного використання людино-годин.
- Ланцюжка поставок і логістика ($ 2,7 трлн): IoT знижує кількість відходів і підвищує ефективність процесів.
- Задоволеність клієнтів ($ 3,7 трлн): IoT підвищує цінність для замовника і збільшує частку ринку, додаючи нових клієнтів.
- Інновації, включаючи зниження часу виходу на ринок ($ 3,0 трлн): IoT підвищує віддачу від вкладень в НДДКР, знижує час виходу на ринок і створює додаткові потоки доходів за рахунок нових бізнес-моделей і можливостей.

Аналогічно опублікований в 2015 році звіт McKinsey Global Institute [3] констатує, що прогнозований загальний економічний ефект IoT зараз становить $ 3,9 трлн, а до 2025 року досягне 11,1 трлн. За найвищої оцінки обсяг цього ефекту - включаючи додаткові доходи від споживачів - до 2025 року буде еквівалентний 11% світової економіки.

1.1 Визначення IoT

Відділ стандартів зв'язку МСЕ (Міжнародний союз електрозв'язку, International Telecommunication Union) опублікував Рекомендацію Y.2060, що має назву «Огляд інтернету речей» (Overview of the Internet of Things) [4]. У цьому документі містяться такі визначення, що описують охоплення IoT:

- Інтернет речей (IoT): Глобальна інфраструктура для інформаційного суспільства, яка забезпечує можливість надання більш складних послуг шляхом з'єднання один з одним (фізичних і віртуальних) речей на основі існуючих функціонально сумісних інформаційно-комунікаційних технологій і тих, що розвиваються.
- Річ: Стосовно до Інтернету речей означає предмет фізичного світу (фізичні речі) або інформаційного світу (віртуальні речі), який може бути ідентифікований та інтегрований в мережі зв'язку.
- Пристрій: Стосовно до Інтернету речей означає елемент обладнання, який володіє обов'язковими можливостями зв'язку та додатковими можливостями вимірювання, спрацьовування, а також введення, зберігання і обробки даних.

У книзі Designing the Internet of Things [5] елементи IoT зведені в просту формулу:

Фізичні об'єкти + контролери, сенсори, виконавчі механізми + Інтернет = IoT

Ця формула чітко описує саму суть Інтернету речей. Примірник IoT складається з набору фізичних об'єктів, кожен з яких:

- містить мікроконтролер, що забезпечує інтелектуальність;
- містить датчик, що вимірює будь-який фізичний параметр, і / або виконавчий механізм, що спрацьовує від будь-якого фізичного параметра;
- має можливість комунікації через Інтернет або будь-якої іншої мережі.

Елементом, що не входять в цю формулу і охопленим визначенням по Y.2060, є спосіб ідентифікації окремої речі, зазвичай званий тегом.

Хоча в літературі завжди використовується термін «Інтернет речей», точніше було б назвати його мережею речей, оскільки мова йде не про «великий» Інтернет. Наприклад, інсталяція «розумного будинку» складається з набору речей в будинку, які обмінюються інформацією по Wi-Fi або Bluetooth з центральним контролером. На заводі або фермі Інтернет речей може підтримувати корпоративні додатки, які будуть взаємодіяти з середовищем і запускати додатки, що використовують Інтернет речей. У цих прикладах віддалений доступ через Інтернет зазвичай є, але його може і не бути. Незалежно від того, чи є таке підключення до Інтернету чи ні, набір «розумних» об'єктів на майданчику, в комплекті з будь-якими іншими обчислювальними пристроями і пристроями зберігання, можна охарактеризувати як «мережу речей» або «Інтернет речей».

1.2 Сфери використання IoT.

Завдяки своїй універсальності у використанні IoT можна застосовувати майже у будь-якій сфері сучасного життя від розумного будинку до нафтових родовищ. У таблиці 1.1 наведено сектори застосування IoT:

Таблиця 1.1 - Сфери Інтернету речей

Сектори послуг	*Прикладні групи*	*Розташування*	*Приклади пристроїв*
	Публічні	Послуги, е-комерція, центри даних, мобільний зв'язок, дротовий зв'язок, ISP	Сервери, сховища, PC, маршрутизатори, комутатори, PBX
	Корпоративні	IT / центри даних, офіси, приватні мережі	
	Устаткування для стеження, контроль	Радари / супутники, військова безпека, безпілотники, зброю, транспорт, кораблі, літаки, спорядження	Танки, винищувачі, бойові комплекти зв'язку, джипи

Сектори послуг	*Прикладні групи*	*Розташування*	*Приклади пристроїв*
	Громадська інфраструктура	Люди, тварини, пошта, їжа / здоров'я, упаковка, багаж, підготовка води, екологія будівель, загальна екологія	Автомобілі, дорожні робітники, служби безпеки, пожежні, екологічний моніторинг
	Аварійні служби	Устаткування і персонал, поліція, пожежники, регулятори	Машини швидкої допомоги, машини аварійних служб
	Спеціалізовані	АЗС, ігрові клуби, боулінг, кіно, дискотеки, спецзаходи	Касові термінали, бирки, знаки, торгові автомати
	Туризм і громадське харчування	Готелі, ресторани, бари, кафе, клуби	
	Магазини	Супермаркети, торгові центри, поодинокі магазини, центри дистрибуції	
	Неавтомобільний	Повітряний, залізничний, морський	Машини, освітлення, кораблі, літаки, знаки, митниця
	Автомобільний	Легкові, вантажні, будівельна техніка, позашляховики	
	Транспортні системи	Система оплати, управління трафіком, навігація	

Сектори послуг	*Прикладні групи*	*Розташування*	*Приклади пристроїв*
Промисловість	Розподіл	Трубопроводи, конвеєри, обробка матеріалів	Насоси, клапани, чани, конвеєри, двигуни, приводи, перетворення, виробництво, складання / упаковка, ємності
	Перетворення	Метал, папір, гума, пластик, металовироби, електронні плати, тестування	
	Процеси	Нафтохімія, вуглеводні, їжа, напої	
	Автоматизація ресурсів	Гірнича справа, іригація, сільське господарство, лісове господарство	
	Охорона здоров'я	Лікарні, реанімації, мобільні станції, клініки, лабораторії, кабінети лікарів	MRI, КПК, імпланти, хірургічне обладнання, насоси, монітори, телемедицина
	Домашні системи	Імпланти, домашні системи моніторингу	
	Дослідження	Розробка ліків, діагностика, лабораторії	

Сектори послуг	*Прикладні групи*	*Розташування*	*Приклади пристроїв*
Споживчий сектор і будинок	Інфраструктура	Проводка, мережевий доступ, управління енергоспоживанням	Цифрові фотоапарати, енергосистеми, посудомийки, електронні книги, настільні комп'ютери, пральні машини, датчики, лампочки, телевізори, MP3, ігрові приставки, освітлення, сигналізація
	Безпека	Охоронні системи / сигналізації, пожежна безпека, екобезпека, для людей похилого віку, для дітей, захист енергопостачання	
	Комфорт і розваги	Кондиціонери, освітлення, приставки, розважальні системи	
	Попит / Пропозиція	Виробництво енергії, передача і розподіл, низьковольтні мережі, якість енергії, управління енергією	Турбіни, вітряки, UPS, батарейки, генератори, датчики, акумулятори
	Альтернативні джерела	Сонячна, вітрова, когенерація, електрохімічна	
	Нафта і газ	Платформи, бурові, гирлове обладнання, насоси, трубопроводи	

Сектори послуг	*Прикладні групи*	*Розташування*	*Приклади пристроїв*
Будинки	Комерційні, організацій	Офіси, освіту, торгівля, громадське харчування, охорону здоров'я, аеропорти, стадіони	ОВКВ, транспорт, пожежна безпека, освітлення, охорона, доступ
	Промислові	Виробничі, чисті, кампуси	

У таблиці 1.1 показано можливі області застосування IoT. Відтак використання IoT в гірничому виробництві необхідне для забезпечення безпеки на шахтах, що є великою проблемою для багатьох країн у зв'язку з умовами праці на підземних рудниках. З метою запобігання та зменшення кількості нещасних випадків необхідно використовувати технології IoT, які зможуть приймати аварійні сигнали з шахти [12]. За допомогою RFID, Wi-Fi і інших технологій і пристроїв бездротового зв'язку, що забезпечують ефективну взаємодію між наземним і підземним просторами, гірничодобувні компанії зможуть відстежувати місце розташування шахтарів і аналізувати критично важливі дані з безпеки, отримані від датчиків. Ще одним корисним додатком є хімічні і біологічні сенсори, що застосовуються для діагностики та раннього визначення захворювань у шахтарів, що особливо важливо, оскільки вони працюють в небезпечних умовах. Ці сенсори можна використовувати для отримання біологічної інформації про стан людського тіла і органів, для виявлення небезпечного пилу, шкідливих газів і інших чинників навколишнього середовища, які можуть стати причиною нещасних випадків. Проблема використання всіх цих технологій полягає в тому, що бездротових пристроїв потрібна енергія, яка потенційно може привести до вибуху газу в шахті. Таким чином, необхідні додаткові дослідження характеристик безпеки IoT-пристроїв, що використовуються в гірничорудній промисловості.

«Інтернет речей» дає нові можливості для поліпшення охорони здоров'я [13]. За повсюдної підтримки ідентифікації, зондування і комунікаційних можливостей «Інтернету речей» всі об'єкти системи охорони здоров'я (люди, техніка, препарати

і т. д.) можна постійно відслідковувати і контролювати [14]. Глобальний зв'язок «Інтернету речей» дозволяє всі медичні відомості (забезпечення, діагностика, терапія, одужання, ліки, управління, фінанси і навіть добова активність) зібрати, обробити і ефективно використовувати. Наприклад, можна вимірювати частоту серцевих скорочень пацієнта за допомогою датчиків, а потім відправляти в кабінет лікаря. При використанні персональних обчислювальних пристроїв (ноутбук, мобільний телефон, планшет і т. д.) і мобільного доступу в Інтернет (Wi-Fi, мережі 3G, LTE і т. д.) медичні служби, що базуються на IoT, стають мобільними і персональними [15]. Широке поширення сервісів мобільного Інтернету прискорює розвиток заснованих на «Інтернеті речей» послуг охорони здоров'я «на дому» [16]. Але поки цього перешкоджають проблеми, пов'язані з безпекою та конфіденційністю.

Сьогодні ланцюжки поставок харчових продуктів (Food Supply Chains, FSC) широко поширені. Вони володіють складними робочими процесами, мають значні географічні і часові масштаби, а також можуть включати велику кількість учасників. Їх складність викликала багато питань з управління якістю, оперативності та громадської безпеки харчових продуктів. Великий потенціал для вирішення проблем відстеження, прозорості та контролю відкрили технології IoT. Вони можуть захистити мережі FSC в так званих ланцюжках «від ферми до тарілки»: від високоточного сільського господарства до виробництва продуктів харчування, їх обробці, зберігання, розподілу та споживання. У майбутньому слід очікувати появи більш безпечних, ефективних і стійких FSC. Типове рішення «Інтернету речей» для FSC (т. н. харчового IoT) складається з трьох частин:

- польових пристроїв, таких як вузли бездротової сенсорної мережі (WSN), зчитувачі RFID-міток, термінали призначеного для користувача інтерфейсу і т.д.
- магістральної системи, що включає бази даних, сервера і термінали багатьох видів, підключених до розподілених комп'ютерних мереж і т.д.
- інфраструктури зв'язку, такий як бездротова локальна мережа (WLAN),

стільниковий, супутниковий зв'язок, лінії електропередач, Ethernet і т.д.

Крім цього, IoT також надає ефективні функції зондування для відстеження і контролю процесів виробництва продуктів харчування [17].

«Інтернет речей» вже використовується в галузі пожежної безпеки для виявлення займань і раннього попередження можливих стихійних лих, пов'язаних з пожежами. У Китаї RFID-мітки і / або штрих-коди зв'язуються із засобами пожежогасіння для організації загальнонаціональної протипожежної інформаційної бази даних і систем управління. Завдяки використанню RFID-міток, мобільних RFID-зчитувачів, а також інтелектуальних відеокамер, сенсорних і бездротових мереж, управління пожежогасіння та прирівняні до них організації можуть виконувати автоматичну діагностику, щоб здійснювати в режимі реального часу моніторинг навколишнього середовища для раннього попередження пожеж та проведення необхідних аварійно - рятувальних заходів. Дослідники в Китаї також використовують технології IoT, щоб вивести на новий рівень систему автоматичного протипожежного оповіщення з метою підвищення управління спалахами і іншими надзвичайними ситуаціями [18]. Нещодавно Цзи і Ци [19] продемонстрували інфраструктуру IoT-додатків, які використовуються для управління надзвичайними ситуаціями в Китаї. Інфраструктура цих IoT-додатків містить рівні зондування, передачі, підтримки, а також платформний і прикладний. IoT-інфраструктура розроблена таким чином, щоб інтегрувати локальні і специфічні галузеві системи. В даний час актуальною в цій області є проблема створення стандартів для протипожежного «Інтернету речей».

1.3 Необхідність шлюзу в IoT

Через швидке зростання кількості датчиків і речей у всьому світі і масового використання хмарної архітектури виникає проблема підключення них до хмари. Виникає необхідність у проміжній ланці котра не тільки дасть змогу підключати пристрої до звичного TCP/IP стеку, а й збереже ширину полоси завдяки обробці даних перед відправленням. IoT шлюз займає це місце, що виникло завдяки:

- Необхідність перетворювати дані, що передаються через не TCP/IP стек, а через мережі Bluetooth, ZigBee, 6LoWPAN та інші протоколи, у стандартні Інтернет пакети.
- Необхідність підтримки декількох локальних дротових або бездротових IoT мереж.
- Необхідність у надійному зв'язку з речами, навіть при відсутності Інтернет з'єднання з хмарою. Буферизація даних від неінтелектуальних датчиків, для відправки на сервер при відновленні підключення.
- Необхідність більш ефективного використання трафіку - агрегація та пакетизація великого об'єму первинного мережевого трафіку, що генерується мільярдами IoT пристроїв. Сбір різних показників у файли перед відправленням на сервер.
- Відстань до датчиків і плат із датчиками, що розташовані у просторі та вимагають низького енергоспоживання, що не завжди дозволяє безпосередній зв'язок із хмарою.
- Необхідність у забезпеченні конфіденційності та безпеки даних при спілкуванні із хмарою.
- Первина обробка даних – затримка передачі даних, проблеми зв'язку з сервером з однієї сторони та обмежена обчислювальна потужність кінцевих пристроїв з малим енергоспоживанням – з іншої.

Виходячи з цих потреб шлюзи – це високопродуктивні пристрої зі стаціонарним підключенням до джерела живлення. На базі цих пристроїв можна будувати системи реального часу, що можуть максимально оперативно реагувати на певні управляючі дії та на критичні зміни показників датчиків, а також локально та віддалено керувати компонентами IoT рішення.

1.4 Висновки

Інтернетом речей називається набір безлічі датчиків та хмарних чи туманних ресурсів. Датчики та пристрої можуть обмінюватись даними між собою та

відправляти свої дані на обробку на більш потужні пристрої для обробки.

Завдяки своїй універсальності можливе використання IoT майже у будь-якій сфері:

- IT і мережі
- Безпека та охорона
- Роздрібна торгівля
- Транспорт
- Промисловість
- Охорона здоров’я та науки про життя
- Споживчий сектор та розумний будинок
- Виробництво енергії

Для полегшення управління «речами», забезпечення кращої безпеки та підвищення ефективності використання каналів зв’язку з’являється необхідність у проміжній ланці, що буде агрегувати інформацію, перетворювати пакети у стандартні TCP/IP пакети, та реагувати на події у режимі реального часу, а не у часі транзакції, при безпосередньому підключенні до хмари. Цю ланку займає шлюз Інтернету речей.

2 СТАНДАРТИ СУМІСТНОСТІ IOT

Найближчим часом різнорідні «острівці» рішень, швидше за все, будуть випереджати в своєму розвитку розгортання IoT-рішень, заснованих на функціонально-сумісних стандартах. Так йдуть справи з будь-якою новою технологією на етапі її зародження. Наприклад, Sutaria and Govindachari [6] відзначають, що дві характеристики мережевих IoT-пристроїв, що викликають найбільші проблеми, - це наявність пристроїв з низьким енергоспоживанням (розрахованих на роботу місяцями і роками без підзарядки) і частий обмін даними по мережах з втратою пакетів. Нинішні стандартні протоколи Інтернету в цих умовах неоптимальні. У більш широкому сенсі має місце дисбаланс між величезною кількістю пристроїв, що генерують дані з шаленою швидкістю в різних місцях, і використанням мережевих технологій і хмарних систем, які зберігають величезні обсяги даних в невеликій кількості локацій при відносно низькій швидкості оновлення даних. Інтеграція цих двох класів систем для задоволення потреб користувачів вимагає певних можливостей від мережевих протоколів у всій архітектурі мережі і протоколів, від фізичного рівня до прикладного.

Над вирішенням цих питань працює кілька організацій і стандартизаційних форумів, прагнучі розширити або адаптувати протоколи Інтернету для пристроїв IoT. Основники організаціями є:

- Міжнародний союз електрозв’язку (*International Telecommunication Union, ITU):* 193 країни [20] і понад 700 членів по секторам і асоціаціям (науково-промислових підприємств, державних і приватних операторів зв'язку, радіомовних компаній, регіональних і міжнародних організацій)
- Всесвітній форум IoT (IoT World Forum, IWF): IBM, Intel, Cisco, Samsung.
- Національний інститут стандартів і технології Міністерства торгівлі США.
- Консорціум індустріального Інтернету (Industrial Internet Consortium,

IIC): SAP, IBM, Intel, Fujitsu, General Electric, Oracle

Для створення єдиної структури і класифікації необхідних функцій за їх місцем в стеку протоколів ряд цих груп також займається питанням формальної архітектури для IoT. У той час як існуючі стандарти та Інтернет зробили IoT можливим, в найближчому майбутньому навряд чи можлива поява стека нових стандартів, які доповнять або модифікують існуючі для сфери IoT. Як і багато інших досягнень, що стали можливими завдяки Інтернету, IoT буде якийсь час стихійно розвиватися і проходити через процеси природного відбору, поки поступово не виявили життєздатні технології та механізми протоколів.

Але з урахуванням складності IoT має сенс створення архітектури, яка б специфікувала основні компоненти і їх взаємозв'язок. Архітектура IoT може надати такі переваги:

- дати адміністраторам мережі або IT-менеджеру корисний контрольний список для оцінки функціональності і повноти пропозицій від різних постачальників;
- служити орієнтиром для розробників в плані того, які функції потрібні в IoT і як вони взаємодіють;
- служити основою для стандартизації, стимулюючи сумісність і скорочення витрат.

2.1 Еталонна модель IoT від МСЕ-Т

Еталонна модель IoT від Міжнародного союзу електрозв’язку (МСЕ-Т) описана в Рекомендації Y.2060 [4]. На відміну від більшості інших еталонних моделей і архітектурних моделей, описаних в літературі, модель МСЕ-Т деталізує фактичні фізичні компоненти екосистеми IoT. Це корисно, тому що це зосереджує увагу на елементах екосистеми IoT, які повинні бути з'єднані, інтегровані, керовані і надані додаткам. Детальна специфікація екосистеми описує вимоги до можливостей IoT.

Один з важливих аспектів, який загострює модель, є той факт, що IoT на ділі

не є мережею фізичних речей. Це скоріше мережа пристроїв, які з'єднано фізичними речами, разом з прикладними платформами - такими як комп'ютери, планшети і смартфони, які взаємодіють з цими пристроями. Тому огляд моделі MCE-T необхідно почати з визначення пристроїв:

- *Мережа зв'язку (Communication Network)* - інфраструктурна мережа, що з'єднує пристрої та додатки, така як мережа на основі стека протоколів IP або Інтернет.
- *Річ (Thing)* - предмет фізичного світу (фізичні речі) або інформаційного світу (віртуальні речі), який може бути ідентифікований та інтегрований в мережі зв'язку.
- *Пристрій (Device)* - елемент обладнання, який володіє обов'язковими можливостями зв'язку та додатковими можливостями вимірювання, спрацьовування, а також введення, зберігання і обробки даних.
- *Пристрій переносу даних (Data-carrying Device)* - пристрій переносу даних підключається до фізичної речі і непрямим чином з'єднує цю фізичну річ з мережами зв'язку. Прикладами можуть служити активні мітки RFID.
- *Пристрій збору даних (Data-capturing Device)* - під пристроєм збору даних розуміється пристрій, що зчитує / записуючий пристрій, що має можливість взаємодії з фізичними речами. Взаємодія може здійснюватися непрямим чином за допомогою пристроїв перенесення даних або безпосередньо за допомогою носіїв даних, підключених до фізичних речей.
- *Носій даних (Data Carrier)* - безбатарейний об'єкт перенесення даних, підключений до фізичної речі і має можливість надавати інформацію придатному для цього пристрою збору даних. Ця категорія включає штрих-коди і QR-коди, наклеєні на фізичні речі.
- *Сенсорний пристрій (Sensing Device)* - пристрій, який може виявляти або вимірювати інформацію, що відноситься до навколишнього середовища, і перетворювати її в цифрові електричні сигнали.

- *Виконавчий пристрій (Actuating Device)* - пристрій, який може перетворювати цифрові електричні сигнали, що надходять від інформаційних мереж, в дії.
- *Пристрій загального призначення (General Device)* - пристрій загального призначення володіє вбудованими можливостями обробки і зв'язку і може обмінюватися даними з мережами зв'язку з використанням дротових або бездротових технологій. Пристрої загального призначення включають обладнання та прилади, які стосуються різних галузей застосування IoT, наприклад, верстати, побутові електроприлади і смартфони.
- *Шлюз (Gateway)* - елемент IoT, що з'єднує пристрої з мережами зв'язку. Він виконує необхідну трансляцію між протоколами, що використовуються в мережах зв'язку і в пристроях.

Унікальним аспектом IoT, в порівнянні з іншими мережевими системами, очевидно є наявність безлічі фізичних речей і пристроїв, відмінних від обчислювальних пристроїв і пристроїв обробки даних. На рис. 2.1, адаптованому з Рекомендації Y.2060, зображені типи пристроїв в моделі MCE-T. Модель розглядає IoT як мережу пристроїв, тісно пов'язаних з речами. Сенсорні і виконавчі пристрої взаємодіють з фізичними речами в навколишньому середовищі. Пристрої збору даних зчитують дані з фізичних речей або записують дані на фізичні речі шляхом взаємодії з пристроями перенесення даних або носіями даних, підключеними або пов'язаними з фізичним об'єктом тим чи іншим чином.

Ця модель показує відмінність між пристроями перенесення даних і носіями даних. Пристрій переносу даних є пристроєм в сенсі Рекомендації Y.2060. Як мінімум, пристрій завжди має можливості зв'язку і може мати інші електронні можливості. Прикладом пристрою перенесення даних є RFID-мітка. У той же час носій даних - це елемент, приєднаний до фізичної речі з метою ідентифікації або інформування.

Рисунок 2.1 - Типи пристроїв та їх взаємозв'язок із фізичними речами [8]

В рекомендації Y.2060 відзначається, що технології, які використовуються для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне і гальванічне збудження. Приклади кожної з них:

- *Радіочастотні*: радіочастотні ідентифікаційні (RFID) - бірки, або радіопозначки.
- *Інфрачервоні*: інфрачервоні мітки, що можна використовувати в Збройних Силах, лікарнях та інших середовищах, де потрібно відстежувати розташування і переміщення персоналу. Це можуть нашивки на військовій формі, що відбивають світло, і такі, що працюють від батарейок та випромінюють ідентифікуючу інформацію. Останні можуть мати кнопку, при натисканні якої бейдж може використовуватись для проходу через автоматичні контрольні пункти,

або ж бейджи, що автоматично повторюють сигнал для контролю за переміщеннями персоналу. Пульти дистанційного керування, що використовуються в побуті або в інших середовищах для управління електронними пристроями, теж можна легко інтегрувати в IoT.

- *Оптичні*: штрих-коди і QR-коди можуть служити прикладами ідентифікаційних носіїв даних, які зчитуються оптично.
- *Гальванічне збудження*: прикладом можуть служити медичні імпланти, які використовують електропровідні властивості людського тіла [7]. В ході комунікації між імплантом і поверхнею гальванічна пара передає сигнали з імпланта на електроди, виведені на шкіру. Ця схема використовує дуже мало енергії, що дозволяє знизити розмір і складність імплантованого пристрою.

Останнім типом пристроїв з рисунку 1 є пристрої загального призначення. Вони володіють можливостями обробки даних і зв'язку, які можуть бути інтегровані в IoT. Хорошим прикладом є технологія «розумного будинку», яка може інтегрувати практично будь-який пристрій в будинку в мережу для централізованого або дистанційного керування.

На рис. 2.2 наведено огляд елементів, задіяних в IoT. У лівій частині малюнка наведено різні способи зв'язку з фізичними пристроями. Передбачається, що одна або кілька мереж підтримують зв'язок між пристроями.

На рис. 2.2 з'являється ще один пристрій, пов'язаний з IoT: шлюз. Як мінімум шлюз працює транслятором між протоколами. Шлюзи вирішують одну з головних проблем при проектуванні IoT, а саме проблему сумісності, як між різними пристроями, так і між пристроями та Інтернетом або корпоративною мережею. «Розумні» пристрої підтримують широкий спектр бездротових і дротових технологій передачі даних і мережевих протоколів. Крім того, можливості обробки даних у таких пристроїв, як правило, обмежені.

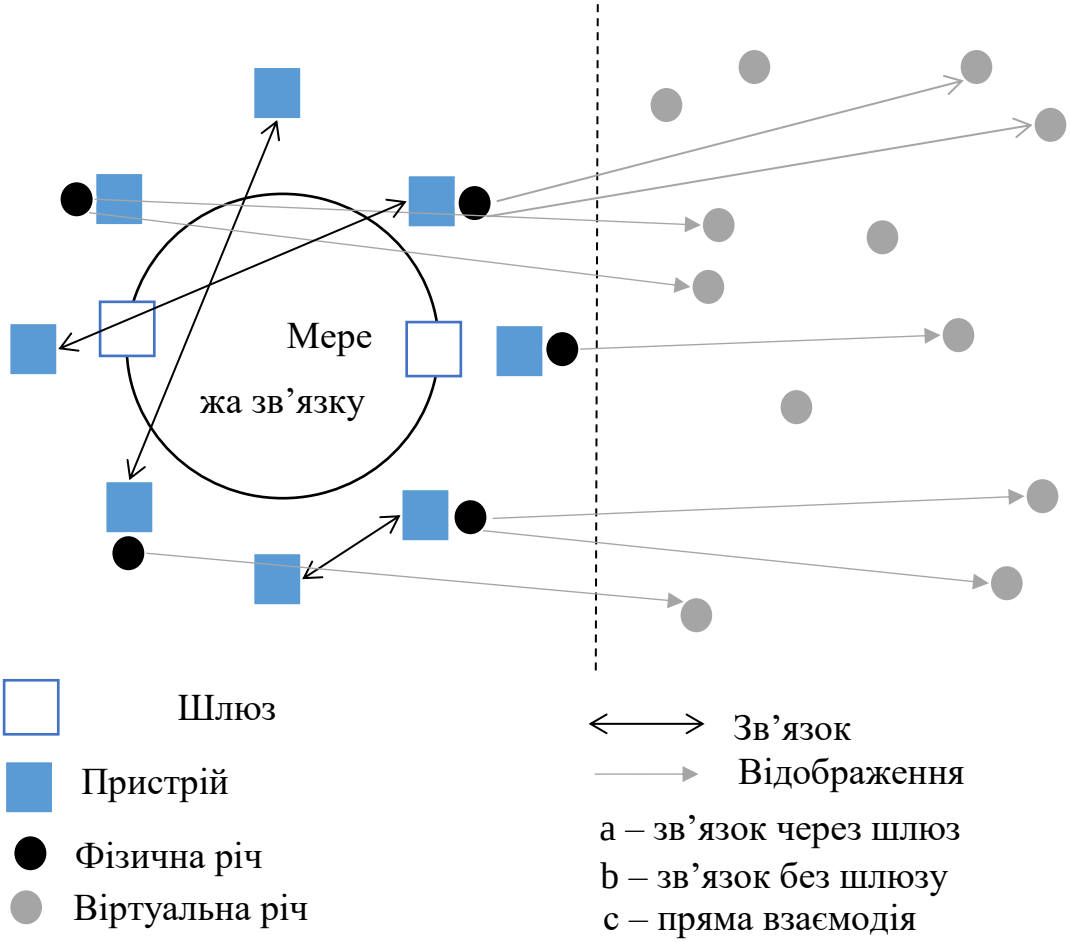

Рисунок 2.2 - Технічний огляд IoT (Рекомендація Y.2060) [8]

Рекомендація Y.2067 [8] закріплює вимоги до шлюзів IoT, які зазвичай розпадаються на три категорії:

- Шлюз підтримує різні технології доступу до пристроїв, дозволяючи пристроїв обмінюватися даними один з одним і з мережею Інтернет або корпоративною мережею, що містить додатки IoT. Такі схеми доступу можуть, наприклад, включати ZigBee, Bluetooth і Wi-Fi.
- Шлюз підтримує необхідні мережеві технології як для локальних, так і для глобальних мереж. Ці технології можуть включати в себе Ethernet і Wi-Fi на території організації, а також стільниковий зв'язок, Ethernet, DSL і кабельний доступ до Інтернету і глобальним корпоративним мережам.
- Шлюз підтримує взаємодію з додатками, управління мережею і функції

безпеки.

Дві перших вимоги включають в себе трансляцію протоколів між різними мережевими технологіями і стеками протоколів. Третя вимога зазвичай називається функцією IoT-агента. По суті, IoT-агент надає функціональність високого рівня від імені IoT-пристроїв, таку як організація або резюмування даних з декількох пристроїв для передачі в IoT-додатки, забезпечення протоколів і функцій безпеки і взаємодія з системами управління мережею.

Тут слід зазначити, що термін «мережа зв'язку» прямо не визначається в серії IoT-стандартів Y.206x. Мережа (або мережі) зв'язку підтримує зв'язок між пристроями і може безпосередньо підтримувати прикладні платформи. Вона може мати розміри невеликого IoT, такого як домашня мережа «розумних» пристроїв. У більш загальному сенсі мережу (або мережі) пристроїв з'єднується з корпоративними мережами або Інтернетом для зв'язку з системами додатків і серверами, на яких розташовані бази даних, пов'язані з IoT.

Ліва частини рис. 2.2 ілюструє можливості зв'язку пристроїв між собою. Перша можливість - зв'язок між пристроями через шлюз. Наприклад, за допомогою шлюзу сенсорне або виконавчий пристрій з підтримкою Bluetooth може здійснювати зв'язок з пристроєм збору даних або пристроєм загального призначення, що використовують Wi-Fi. Друга можливість - зв'язок по мережі зв'язку без шлюзу. Наприклад, якщо всі пристрої в мережі «розумного будинку» підтримують Bluetooth, вони можуть управлятися з комп'ютера, планшета або смартфона з підтримкою Bluetooth. Третя можливість - прямий зв'язок пристроїв між собою за окремою локальної мережі, в той час як зв'язок із зовнішньою мережею (на малюнку не показана) здійснюється через шлюз LAN. Наведемо приклад такої можливості. Уявіть собі, що на великій території, наприклад, на фермі або заводі, знаходиться велика кількість датчиків з низьким енергоспоживанням. Ці пристрої взаємодіють між собою для послідовної передачі даних на пристрій, підключений до шлюзу в мережу зв'язку.

У правій частині рис. 2.2 підкреслюється, що кожна фізична річ в Інтернеті речей може бути представлена в інформаційному світі однією або декількома

віртуальними речами, але при цьому віртуальна річ може існувати без відповідної фізичної речі. Фізичні речі зіставлені віртуальним речей, що зберігаються в БД і інших структурах даних. Додатки обробляють віртуальні речі і працюють з ними.

На рис. 2.3 зображена еталонна модель IoT від MCE-T, що складається з чотирьох рівнів плюс можливості управління і безпеки, що діють між рівнями. До сих пір ми говорили про рівень пристрою. У термінах функціональності зв'язку рівень пристрою включає в себе, грубо кажучи, фізичний і канальний рівні OSI. Тепер перейдемо до інших рівнів.

Рівень мережі виконує дві базові функції. Можливості мережі відносяться до взаємодії пристроїв і шлюзів. Транспортні можливості відносяться до транспорту інформації служб і додатків IoT, а також інформацією управління і контролю IoT. Грубо кажучи, ці можливості відповідають мережевому і транспортному рівням OSI.

Рівень підтримки послуг і підтримки додатків надає можливості, які використовуються додатками. Багато різноманітних додатків можуть використовувати загальні можливості підтримки. До прикладів належать спільне опрацювання даних і управління БД. Спеціалізовані можливості підтримки - це конкретні можливості, які призначені для задоволення потреб конкретного підмножини додатків IoT.

Рівень додатку складається з усіх додатків, взаємодіючих з IoT-пристроями.

Рівень можливостей управління охоплює традиційні функції управління мережею, тобто управління несправностями, управління конфігурацією, управління обліком, управління показниками роботи і управління безпекою.

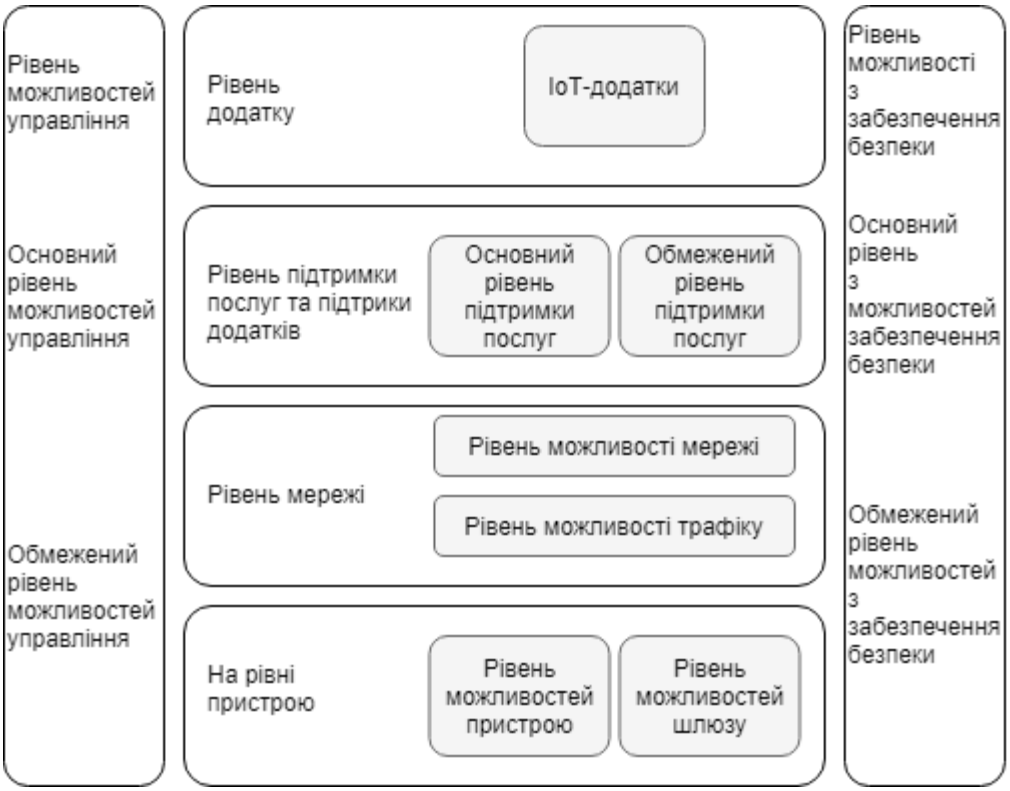

Рисунок 2.3 - Еталона модель IoT за рекомендацією Y.2060 [8]

В Рекомендації Y.2060 як приклади загальних можливостей управління перераховані:

- *управління пристроями*: приклади включають виявлення пристроїв, автентифікацію, дистанційну активацію і дезактивацію пристроїв, конфігурацію, діагностику, оновлення прошивки і / або ПЗ, управління робочим статусом пристрою;
- *управління топологією локальної мережі*: прикладом є управління конфігурацією мережі;
- *управління трафіком і перевантаженнями*: наприклад, виявлення умов перевантаженості мережі і реалізація резервування ресурсів для термінових і / або життєво важливих потоків трафіку.

Спеціалізовані можливості управління тісно пов'язані з вимогами додатків, наприклад, вимогами з контролю лінії передачі електроенергії в «розумній» електромережі.

Рівень можливостей забезпечення безпеки включає загальні можливості забезпечення безпеки, які не залежать від додатків. В Рекомендації Y.2060 приклади загальних можливостей забезпечення безпеки включають:

- *на рівні програми*: авторизацію, автентифікацію, захист конфіденційності і цілісності даних програми, захист недоторканності приватного життя, аудит безпеки і антивірусний захист;
- *на рівні мережі*: авторизацію, автентифікацію, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних сигналізації;
- *на рівні пристрою*: автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

Спеціалізовані можливості забезпечення безпеки тісно пов'язані з вимогами додатків, наприклад, вимогами безпеки мобільних платежів.

2.2 Еталонна модель від Всесвітнього форуму IoT

Всесвітній форум IoT (IoT World Forum, IWF) - щорічна подія, що спонсорується галуззю та об'єднує представників бізнесу, державних структур та вузівської науки з метою просування IoT на ринок. Комітет з архітектури Всесвітнього форуму IoT, складений з лідерів індустрії, включаючи IBM, Intel та Cisco, в жовтні 2014 опублікував еталонну модель IoT. Ця модель є загальною структурою, покликаною допомогти галузі прискорити розгортання IoT. Модель призначена для того, щоб стимулювати співпрацю та сприяти створенню повторюваних моделей впровадження.

Ця еталонна модель є корисним доповненням до моделі MCE-T. Документи MCE-T роблять упор на рівнях пристрою та шлюзу, описуючи верхні рівні лише в загальних рисах. І дійсно, в Рекомендації Y.2060 увесь опис рівня додатку вмістився в одну фразу. Найбільше уваги рекомендації серії Y.206x приділяють визначенню концепції для підтримки розробки стандартів взаємодії з пристроями

IoT.

IWF стурбований більш масштабним питанням розробки додатків, проміжного програмного забезпечення і функцій підтримки для корпоративного Інтернету речей. Запропонована семирівнева модель зображена на рис. 2.4.

Документальний опис моделі IWF, опублікований Cisco [9], вказує, що розроблена модель відрізняється наступними характеристиками:

- *спрощує*: допомагає розбити складні системи на частини так, щоб кожна з цих частин стала більш зрозумілою;
- *прояснює*: надає додаткові відомості для точної ідентифікації рівнів IoT і вироблення загальної термінології;
- *ідентифікує*: ідентифікує аспекти, в яких ті чи інші типи обробки оптимізовані в різних частинах системи;
- *стандартизує*: є першим кроком до того, щоб постачальники могли створювати продукти IoT, здатні взаємодіяти один з одним;
- *організовує*: робить IoT реальним і доступним, а не просто абстрактною концепцією.

Рисунок 2.4 - Еталона модель від Всесвітнього форуму IoT [8]

Рівень 1 утворюють фізичні пристрої та контролери, які можуть керувати кількома пристроями. Рівень 1 моделі IWF приблизно відповідає рівню пристрою в моделі MCE-T (рис. 2.3). Як і в моделі MCE-T, елементи на цьому рівні - не фізичні речі як такі, а пристрої, які взаємодіють з фізичними речами, такі як

сенсорні і виконавчі пристрої. Серед інших можливостей ці пристрої можуть вміти здійснювати аналого-цифрове і цифро-аналогове перетворення, генерацію даних, а також підтримувати дистанційний опитування і / або дистанційне керування.

Рівень 2 моделі IWF приблизно відповідає рівню мережі в моделі MCE-T. Основна відмінність в тому, що модель IWF відносить шлюзи до рівня 2, в той час як в моделі MCE-T вони відносяться до рівня 1. Оскільки шлюз є мережевим пристроєм і пристроєм зв'язку, віднесення його до рівня 2 має більше сенсу.

З логічної точки зору цей рівень реалізує зв'язок пристроїв між собою і між пристроями і низькорівневою обробкою на рівні 3. З фізичної точки зору цей рівень складається з мережевих пристроїв, таких як маршрутизатори, комутатори, шлюзи і брандмауери, що використовуються для створення локальних і глобальних мереж і підключення до Інтернету. Цей рівень дозволяє пристроям здійснювати зв'язок один з одним і за допомогою більш високих логічних рівнів обмінюватися даними з прикладними платформами, такими як комп'ютери, пристрої дистанційного управління і смартфони.

У багатьох впроваджуваних системах IoT розподілена мережа датчиків може генерувати великі обсяги даних. Наприклад, офшорні нафтові родовища і нафтопереробні заводи можуть генерувати до терабайта даних щодня. Літак може генерувати кілька терабайт даних на годину. Замість того, щоб зберігати всі ці дані постійно (або хоча б довгий час) в централізованому сховищі, доступному для додатків IoT, часто більш доцільно виконувати якомога більшу частину обробки даних якомога ближче до датчиків. Тому завданням рівня периферійних обчислень (edge computing level) є перетворення мережевих потоків даних в інформацію, придатну для зберігання і більш високорівневої обробки. Елементи обробки на цьому рівні можуть мати справу з великими обсягами даних і виконувати операції перетворення даних, в результаті яких зберігати доводиться вже набагато менший обсяг. Опублікований Cisco документ по моделі IWF [9] містить такі приклади операцій на рівні периферійних обчислень:

- *аналіз*: аналіз даних по критеріях того, чи підлягають вони обробці на більш високому рівні;

- *форматування*: переформатування даних для однакової високорівневої обробки;
- *розархівування / декодування*: обробка криптографічних даних з додатковим контекстом (таким як походження);
- *дистиляція / скорочення*: скорочення і / або резюмування даних для того, щоб мінімізувати обсяг даних, трафік в мережі і в високорівневих системах обробки;
- *оцінка*: визначення того, чи становлять дані порогове значення або аварійний сигнал; цей процес повинен включати перенаправлення даних додатковим одержувачам.

Елементи обробки на цьому рівні відповідають пристроїв загального призначення в моделі MCE-T (рис. 1). Як правило, вони розгортаються фізично на краю мережі IoT, тобто поруч з сенсорами і іншими пристроями генерації даних. Таким чином, частина базової обробки великих обсягів генеруються даних знімається з прикладних програм IoT, розташованих центрально.

Обробка на рівні периферійних обчислень іноді називається туманними обчисленнями (Fog Computing). Туманні обчислення і туманні служби, як очікується, стануть відмінною характеристикою IoT. Цей принцип проілюстрований на рис. 2.5. Туманні обчислення представляють в сучасних мережевих технологіях тренд, протилежний хмарних обчислень. У хмарні обчислення великий обсяг централізованих ресурсів зберігання і обробки даних доступний розподіленим споживачам за допомогою хмарних мережевих структур для відносно невеликого числа користувачів. В туманних обчисленнях велике число окремих інтелектуальних об'єктів здійснюють зв'язок з туманними мережевими структурами, які здійснюють обчислення і зберігають ресурси поруч з периферійними пристроями в IoT. Туманні обчислення вирішують проблеми, що виникли внаслідок діяльності тисяч або мільйонів «розумних» пристроїв, включаючи проблеми безпеки, конфіденційності, обмежених можливостей мережі і затримки. Термін «туманні обчислення» обраний тому, що туман стелиться по землі, в той час як хмари знаходяться високо в небі.

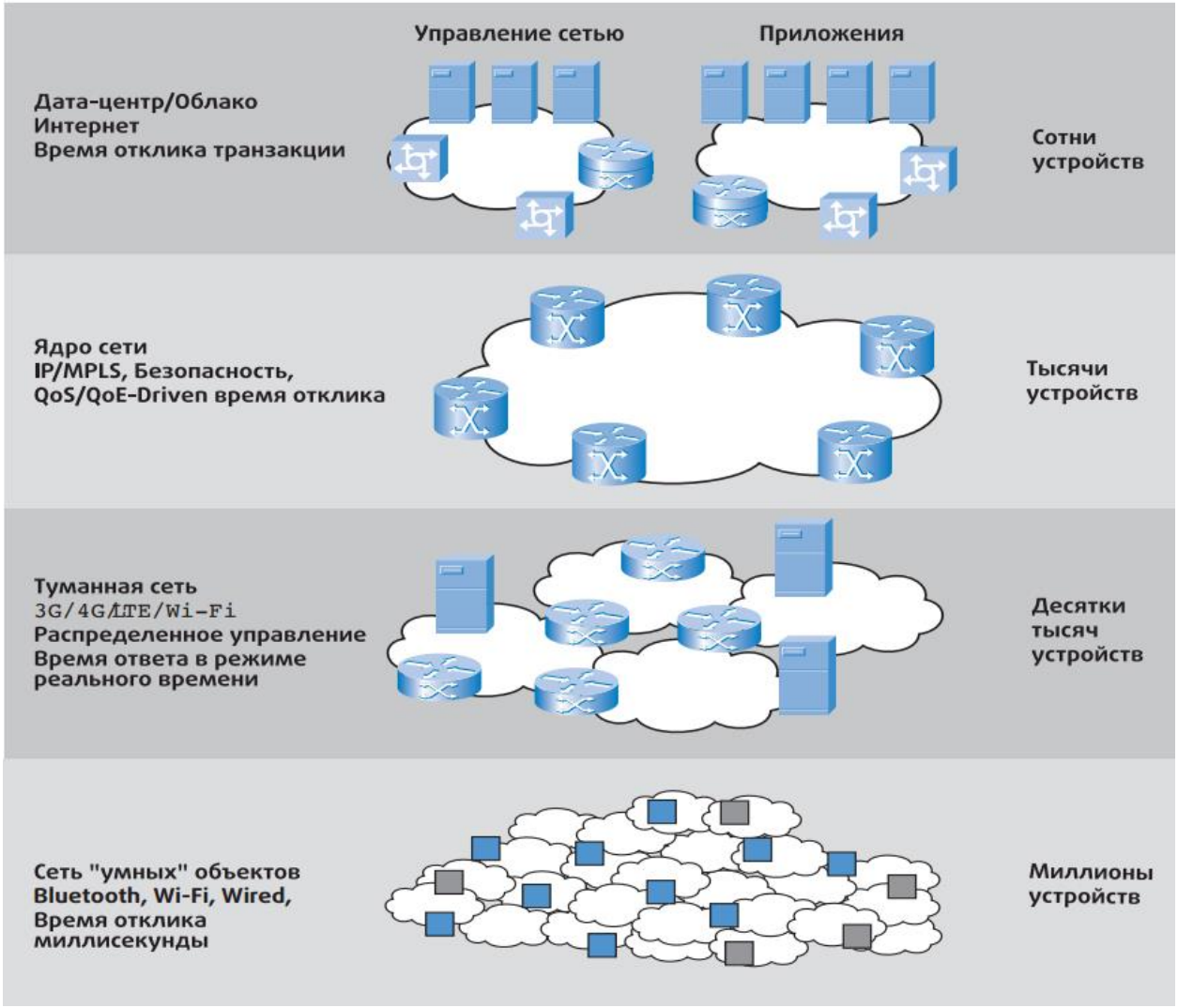

Рисунок 2.5 - Туманні обчислення [9]

Порівняння хмарних і туманних обчислень наведено в таблиці 2.1, складеної на основі даних [10].

Таблиця 2.1 - Порівняння хмарних та туманних обчислень

	Хмара	*Туман*
Розташування ресурсів зберігання / обробки	Центр	Край
Затримка	Від низької до високої	Низька
Доступ	Фіксований або бездротовий	Головним чином безпровідний
Підтримка мобільності	Не застосовується	Так
Контроль	Централізований / ієрархічний (повний контроль)	Розподілений / ієрархічний (частковий контроль)

	Хмара	*Туман*
Доступ до служб	Через ядро	На краю / з портативного пристрою (смартфон і т.д.)
Доступність	99,99%	Висока нестабільність / високий рівень резервування
Число користувачів / пристроїв	Десятки і сотні мільйонів	Десятки мільярдів
Основний генератор контенту	Люди і пристрої	Пристрої / сенсори
Генерація контенту	У центральному розташуванні	Скрізь
Споживання контенту	На кінцевих пристроях	Скрізь
Віртуальна програмна інфраструктура	Центральні корпоративні сервери	Призначені для користувача пристрої

На рівні 4, рівні накопичення даних, дані, що надійшли з різних пристроїв, профільтровані і оброблені рівнем периферійних обчислень, поміщаються в сховище, де будуть доступні для більш високих рівнів. Цей рівень разюче відрізняється і від низькорівневих (туманних), і від високорівневих (хмарних) обчислень за особливостями конструкції, вимогам і методам обробки.

Дані, що проходять крізь мережу, називаються «даними в русі». Швидкість і організація даних в русі визначається пристроями, що генерують дані. Генерація даних відбувається по подіям, або періодично, або по виникненні якої-небудь події в середовищі. Для збору даних та їх обробки необхідно реагувати на їх появу в реальному часі. Навпаки, багатьом додаткам не потрібно обробляти дані зі швидкістю мережевої передачі. На практиці ні хмарна мережу, ні прикладні платформи не змогли б встигати за обсягами даних, що генеруються величезною кількістю IoT-пристроїв. Замість цього додатки мають справу з «даними в спокої», тобто даними в тому чи іншому легкодоступному сховище. Додатки можуть звертатися до даних у міру необхідності або поза режимом реального часу. Таким чином, високі рівні функціонують за принципом транзакцій, в той час як три нижніх рівні працюють по подіях.

Нижче перераховані названі в [10] операції, що виконуються на рівні

накопичення даних:

- перетворення «даних в русі» в «дані в спокої»;
- перетворення формату з мережевих пакетів в реляційні таблиці БД;
- перехід від обчислень щодо подій до обчислень за запитом;
- значне зниження обсягу даних за рахунок фільтрації і вибіркового зберігання.

Ще один погляд на рівень накопичення даних полягає в тому, що він являє собою кордон між інформаційними технологіями (IT), під якими розуміється цілий спектр технологій обробки інформації, включаючи ПЗ, обладнання, технології зв'язку і супутні служби, і операційними технологіями (Operational Technology, OT), що представляють собою обладнання і ПЗ, які виявляють або викликають зміни шляхом прямого моніторингу та / або контролю фізичних пристроїв, процесів і подій на підприємстві.

Рівень накопичення даних вбирає велику кількість даних і поміщає їх в сховище, практично не пристосовуючи до потреб конкретних програм або груп додатків. З рівня периферійних обчислень в сховище може надходити безліч різних видів даних в різних форматах і від різнорідних оброблювачів. Рівень абстракції даних може агрегувати і форматувати такі дані способами, які роблять доступ додатків більш керованим і ефективним. У числі пов'язаних завдань можуть бути наступні:

- Комбінування даних з різних джерел, включаючи вивірку кількох форматів даних.
- Виконання необхідних перетворень для забезпечення однакової семантики даних з різних джерел.
- Приміщення відформатованих даних у відповідну базу даних, наприклад, великі обсяги повторюваних даних поміщаються в систему великих даних, таку як Hadoop. Дані подій направляються в реляційну СУБД, що відрізняється більш швидким часом реакції і адекватним інтерфейсом для таких типів даних.
- Оповіщення додатків більш високого рівня про те, що дані заповнені

або досягнутий певний рівень даних.

- Консолідація даних в одному місці (за допомогою ETL (extract, transform, load), ELT (extract, load, transform) або реплікації даних) або надання доступу до декількох джерел даних шляхом віртуалізації даних.
- Захист даних шляхом відповідної автентифікації і авторизації.
- Нормалізація / денормалізація і індексація даних для швидкого доступу додатків.

Рівень додатку містить додатки будь-якого типу, що використовують дані IoT на вході або керуючі IoT-пристроями. Як правило, додатки взаємодіють з рівнем 5 і з даними в спокої, тому їм не обов'язково функціонувати на швидкостях мережі. Слід передбачити спрощений режим роботи, який дозволить додаткам минути проміжні рівні і безпосередньо взаємодіяти з рівнем 3 або навіть рівнем 2. Модель IWF не визначає додатки по всій строгості, вважаючи цей аспект виходять за рамки дискусії про модель IWF.

Рівень взаємодії і процесу з'явився в результаті визнання того, що IoT буде корисний лише тоді, коли з ним зможуть взаємодіяти люди. Цей рівень може включати кілька додатків і обмін даними і / або керуючої інформацією по Інтернету або корпоративної мережі.

IWF вважає еталонну модель IoT прийнятої в галузі базовою структурою, спрямованої на стандартизацію концепцій і термінології, пов'язаних з IoT. Що ще більш важливо, модель IWF визначає необхідний функціонал і проблеми, які потрібно вирішити до того, як галузь зможе реалізувати цінність IoT. Ця модель корисна як для постачальників, що розробляють функціональні елементи всередині моделі, так і для замовників, допомагаючи їм виробити свої вимоги і оцінювати пропозиції постачальників.

2.3 Інші еталонні моделі

Крім моделей MCE-T і IWF можна виділити такі моделі як:

- Модель NIST Special Publication 800-183
- Модель Industrial Internet of Things Reference Architecture

2.3.1 Модель NIST Special Publication 800-183

Публікація «Networks of« Things» Національного інституту стандартів і технології Міністерства торгівлі США вийшла в розділі COMPUTER SECURITY в липні 2016 року [21]. Основними пунктами публікації є:

- Введено поняття «Network of« Things » - вид розподілених систем.
- IoT, мережі соц. медіа, мережі сенсорів, промисловий Інтернет розглядаються як види NoT.
- «Речами» може бути програмне забезпечення, «залізо», їх комбінація і людина.
- Виділено та описано характеристики п'яти ключових примітивів: сенсор, агрегатор (шлюз), канал зв'язку, зовнішня утиліта і тригер рішення.
- У модель також внесені шість елементів: середа, витрати, місце розташування, власник (оператор), Device_ID (для будь-якого прімітива), і момент часу (снепшот).

Додаткові міркування:

- Система може бути відкритою, закритою або мати проміжний стан.
- Необхідність використання шаблонів проектування для побудови великих систем.
- Рівень довіри до системи в деякий момент часу - функція від реалізації примітивів з урахуванням основних елементів.
- Низька вірогідність виявлення помилок в системі під час тестування.
- Облік механізмів і особливостей впливу на зовнішнє середовище.

У публікації зачіпаються питання безпеки і надійності.

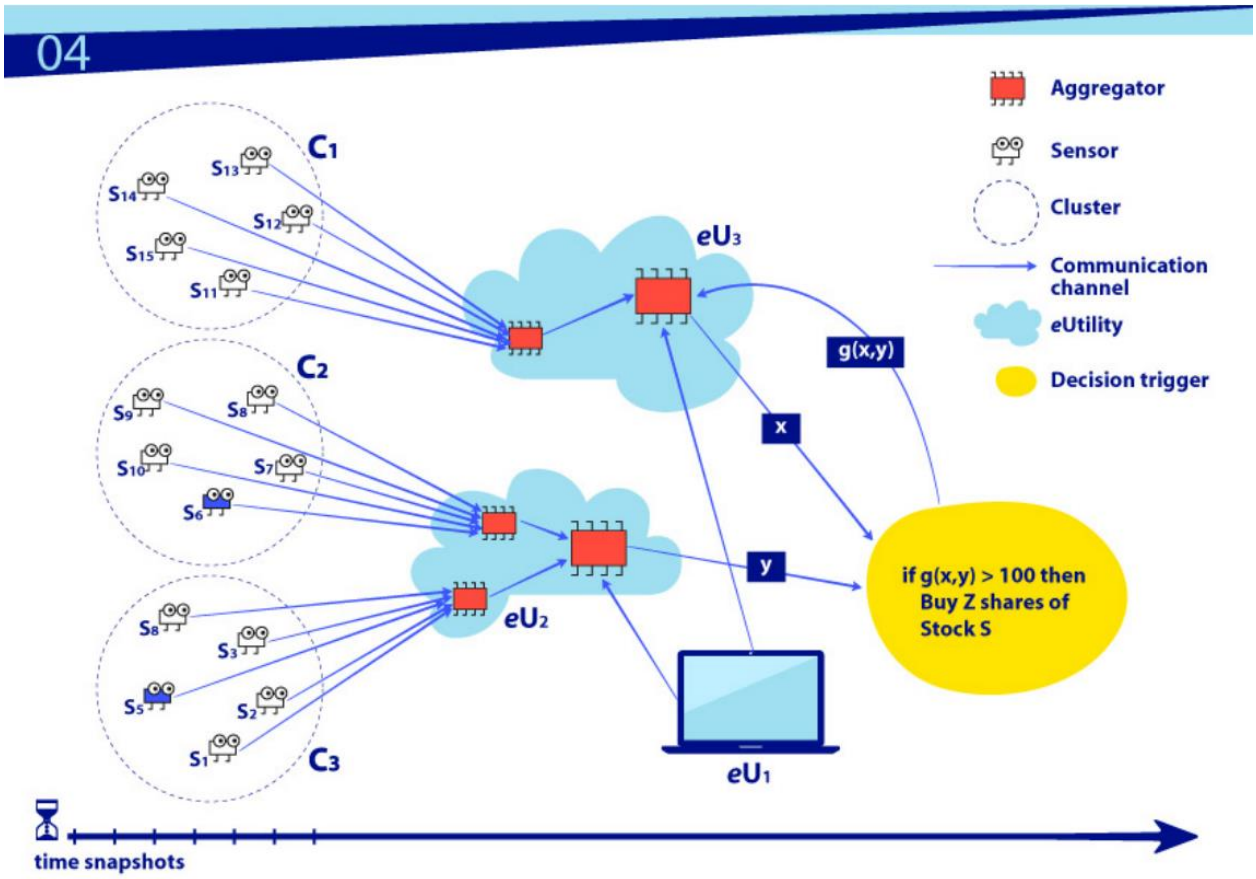

Рисунок 2.6 - Архітектура моделі за публікацією NIST Special Publication 800-183 [21]

Як можна побачити з рисунку 6 для шлюзів (агрегаторів) тут виділяється більша роль аніж у архітектурах міжнародного IoT форуму та Міжнародного союзу електрозв'язку. Агрегатор не просто виконує функцію «перепакування» з одного стеку протоколів у інший, а ще й агрегує, аналізує та зберігає дані.

2.3.2 Модель Industrial Internet of Things Reference Architecture

Консорціум промислового інтернету об'єднує понад 100 компаній. У січні 2017 року побачила версія 1.8 документа The Industrial Internet of Things. Volume G1: Reference Architecture. Також були опубліковані INDUSTRIAL INTERNET SECURITY FRAMEWORK, і INDUSTRIAL INTERNET CONECTIVITY FRAMEWORK. Серед авторів архітектури представники SAP, IBM, Intel, Fujitsu, General Electric, Oracle.

В референсній архітектурі представлено три шаблони реалізації IIoT-системи [22]:

- Трирівневий шаблон
  - Рівень краю збирає дані з кінцевих вузлів, використовуючи локальну мережу. Архітектурна характеристика цього рівня, включаючи широту розподілу, розташування, обсяг управління та характер локальних мереж, залежить від конкретних випадків використання.
  - Рівень платформи отримує, обробляє та пересилає команди управління з рівня підприємства на рівень краю. Він об'єднує процеси та аналізує потоки даних з краю та інших рівнів. Він забезпечує функції керування пристроями та активністю. Він також пропонує спеціальні послуги, не пов'язані з доменом, такі як запити даних та аналітика.
  - Рівень підприємства впроваджує доменні додатки, системи прийняття рішень та забезпечує інтерфейси для кінцевих користувачів, включаючи операторів. Рівень підприємства отримує потоки даних з краю та рівня платформи. Він також передає команди керування рівнями краю та рівнями платформи.

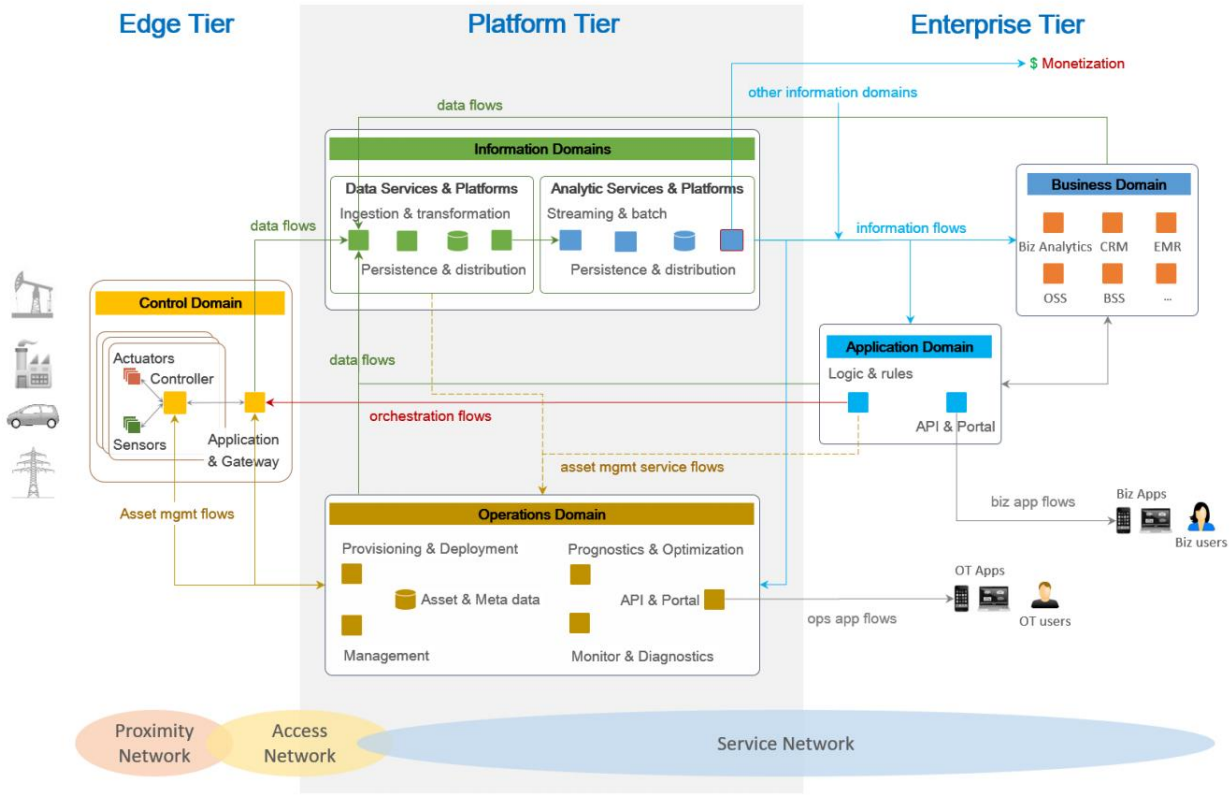

Рисунок 2.7 - Трирівневий шаблон [22]

- З'єднання та управління за допомогою шлюзів: шлюзовий зв'язок та схема архітектури керування складаються з локального рішення для підключення до краю системи IIoT з шлюзом, який переходить до широкосмугової мережі, як показано на рисунку 8. Шлюз виступає як кінцева точка для широкосмугової мережі при ізоляції локальної мережі краєвих вузлів. Ця схема архітектури дозволяє локалізувати операції та керування (край аналітики та обчислення). Його основна перевага полягає у зниженні складності систем IIoT, з тим щоб вони могли збільшуватись як у кількості керованих активів, так і в мережах. Однак він може не підходити для систем, де активи рухаються таким чином, що не дозволяє розташовувати стабільні кластери в межах локальної мережі.
    - У топології hub-and-spoke граничний шлюз діє як концентратор для підключення кластера вузлів краю один до одного та до широкосмугової мережі. Він має прямий зв'язок з кожним

об'єктом в кластері краю, що дозволяє приймати дані з кінцевих вузлів, а також керувати вузлами.

- У мережевій сітці (або однорангової) топології краєвий шлюз також виступає як концентратор для підключення кластера вузлів краю до широкосмугової мережі. Проте в цій топології деякі верхні вузли мають можливість маршрутизації. Як результат, шляхи маршрутизації від вузла краю до іншого та до шлюзу змінюються і можуть змінюватися динамічно. Ця топологія використовується для забезпечення широкого покриття для програм з низькою потужністю та низькою швидкістю передачі даних на пристроях з обмеженим ресурсом, які географічно розподілені.

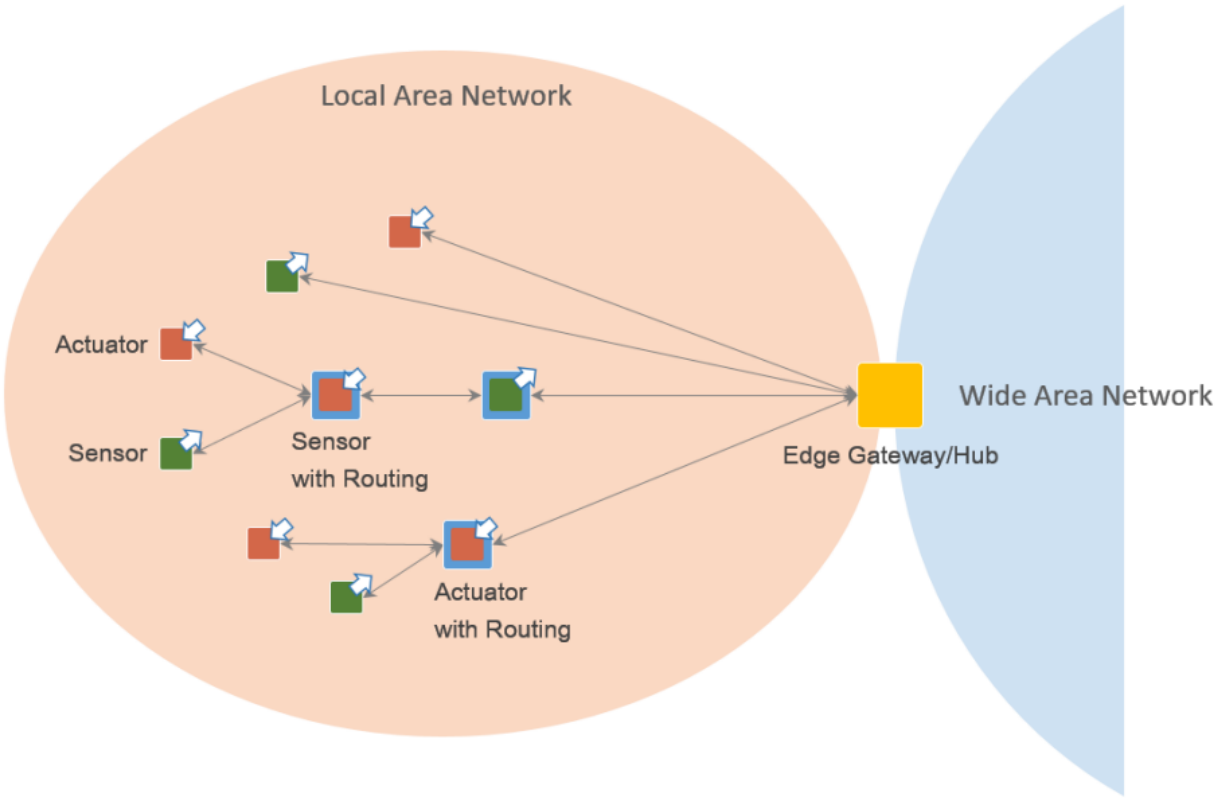

Рисунок 2.8 - З'єднання та управління за допомогою шлюзів [22]

- Багатошарова шина даних: багатошарова шина даних є загальною архітектурою в системах IIoT у кількох галузях промисловості (рис. 2.9). Ця архітектура забезпечує низьку латентність, захищену

однорангову передачу даних через логічні шари системи. Це найбільш корисно для систем, які повинні управляти прямими взаємодіями між додатками в областях, таких як контроль, локальний моніторинг та аналітика краю.

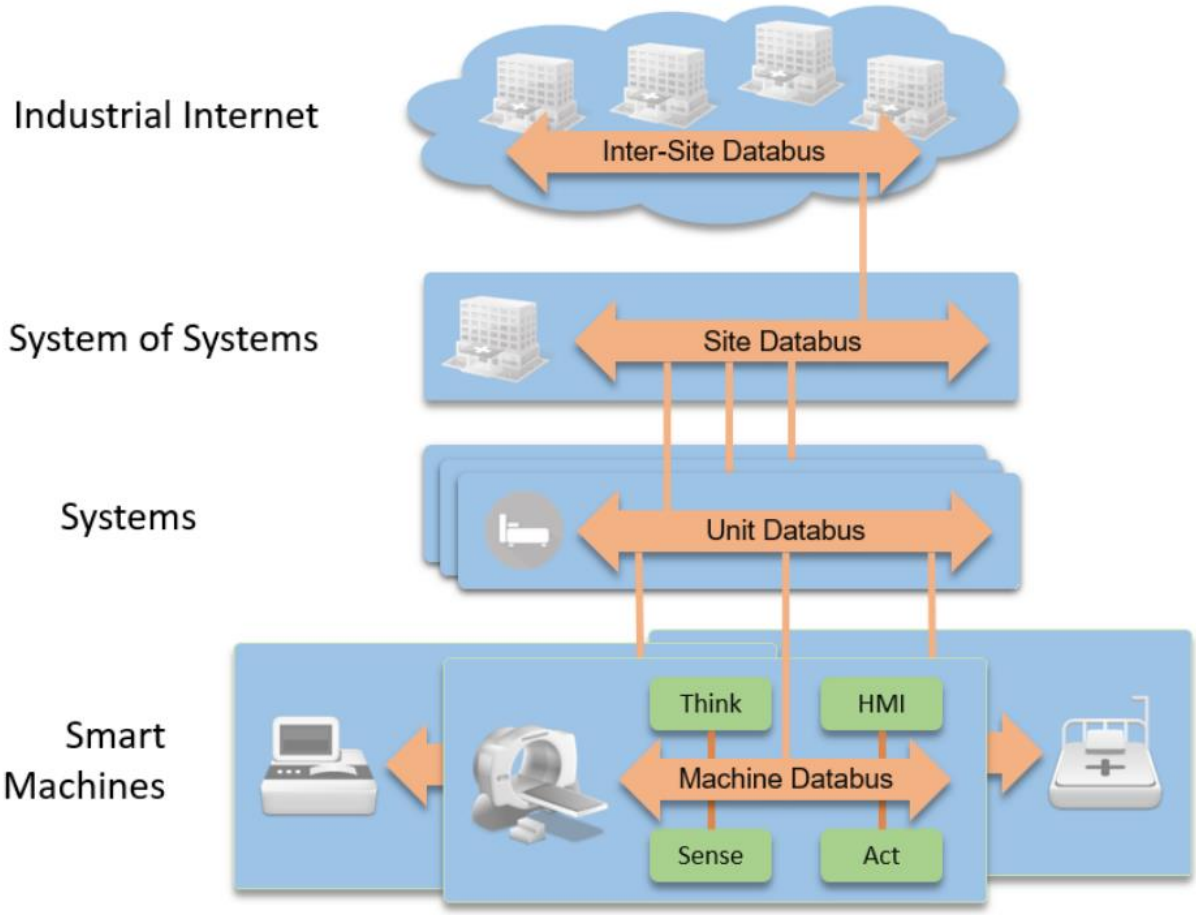

Рисунок 2.9 - Шаблон з використанням багатошарової шини даних [21]

В даній архітектурі шлюз являється осередком зв'язку між речами та зовнішнім світом, він виступає в якості маршрутизатора та не має функцій зберігання даних, агрегації та аналітики.

2.4 Висновки

Основними задачами стандартизації і моделей архітектури є прийняття спільного рішення щодо побудови платформ Інтернету речей та надання наступних переваг:

- дати адміністраторам мережі або IT-менеджеру корисний контрольний список для оцінки функціональності і повноти пропозицій від різних постачальників;
- служити орієнтиром для розробників в плані того, які функції потрібні в IoT і як вони взаємодіють;
- служити основою для стандартизації, стимулюючи сумісність і скорочення витрат.

Основними організаціями та колективами, що займаються питаннями стандартизації є:

- Міжнародний союз електрозв’язку (International Telecommunication Union, ITU): 193 країни [20] і понад 700 членів по секторам і асоціаціям (науково-промислових підприємств, державних і приватних операторів зв'язку, радіомовних компаній, регіональних і міжнародних організацій)
- Всесвітній форум IoT (IoT World Forum, IWF): IBM, Intel, Cisco, Samsung.
- Національний інститут стандартів і технології Міністерства торгівлі США.
- Консорціум індустріального Інтернету (Industrial Internet Consortium, IIC): SAP, IBM, Intel, Fujitsu, General Electric, Oracle

Всі з перечислених організацій віддають шлюзу функцію створення локальних мереж для підключення неінтелектуальних "речей" і узгодження протоколів при взаємодії між OT та IT. Мережа може мати як стандартний TCP/IP стек протоколів, так і бути не IP мережею для підключення датчиків за допомогою таких технологій як Bluetooth, ZigBee або 6LoWPAN та ін. Також всі вони визначають функції безпеки і керування, проте вони можуть відрізнятися, відтак у моделі ITU ці функції обмежені лише на рівні пристрою, а у інших моделях вони ще забезпечуються на рівні мережі. Всі організації окрім ITU до OT відносять ще й функції аналітики даних від речей. У моделі IWF шлюз класифікують, як мережевий пристрій, проте в архітектурі на суміжному рівні виділяються функції

перефирійних/туманних обчислень. Cisco, котрий бере активну участь у IWF, явно позиціонує свої шлюзи, як пристрої, що проводять аналітику даних та реагують на події. ІІС для шлюзів виділяє функції аналітики краю, що по факту є додаванням до можливостей шлюзу рівню туманних обчислень з моделі IWF. В моделі національного інституту стандартів шлюз одразу називається агрегатором і являється частиною апаратного забезпечення, що займається дослідженням даних від датчиків. Він являється певним сервером, що знаходиться у безпосередній близькості до речей. Відтак шлюз перестає бути лише конвертором з одних протоколів у інші, він набуває здібностей аналізувати дані, оброблювати їх і зберігати/надсилати у більш стислій формі. Можливе реагування на показники певних датчиків або певні події у режимі реального часу, а не у часі транзакції, як при безпосередньому підключені речей до хмари.

3 IOT ПЛАТФОРМИ

IoT-платформи об'єднують власне "речі" і "Інтернет". По суті - це ключовий інструмент розробки IoT-додатків і сервісів, що поєднує фізичні об'єкти і Мережу.

При цьому багато постачальників, які намагаються "тримати ніс за вітром", пропонують "IoT-платформи", які в корені відрізняються між собою. І в ряді випадків не є "платформою" в широкому сенсі слова, але абсолютно очевидно мають підстави себе такою вважати - є "річ", є якийсь ресурс в Інтернеті, який приймає / передає дані від / до "речі". І щось робить (намагається робити) з цими даними. Отже, претендувати на високе звання платформи цілком може. Притому, що чіткого і конкретного визначення IoT-платформи просто не існує.

На думку авторів "IoT Analytics", повноцінною IoT-платформою слід вважати таку платформу, яка дозволяє розробляти відповідні додатки / рішення (IoT Application Enablement Platform).

А ось чотири типи платформ, які називають "IoT-платформами", проте вони не цілком підходять під класифікацію IoT Analytics:

- Connectivity / M2M platforms. Платформи в своїй роботі фокусуються на зв'язку розумних об'єктів через телекомунікаційні мережі, але рідко на обробці сигналів від датчиків (приклад такої платформи: Sierra Wireless з продуктом AirVantage).
- IaaS backends. Інфраструктура-як-сервіс-сервери, що надають хостинг-простір і обчислювальні потужності для додатків і сервісів, раніше оптимізували для десктопів і мобільних додатків, але зараз в фокус потрапив і IoT (приклад - IBM Bluemix, але не IBM IoT Foundation).
- Hardware-specific software platforms. Деякі компанії, що продають розумні гаджети, створюють власний програмний бекенд і міркують про нього, як про IoT-платформі. Але, так як ця платформа носить закритий для всіх інших характер, правомірність такого найменування сумнівна (наприклад - Google Nest).
- Consumer / Enterprise software extensions. Існуючі пакети

корпоративного програмного забезпечення і операційні системи типу MS Windows 10 стають все більш відкритими для інтеграції IoT-пристроїв. В даний час ця область ще недостатньо розвинена, щоб називатися IoT-платформою, але майбутнє у неї дуже перспективне.

Загалом все заплутано і ясності в термінології немає. Це ще посилюється "модністю" теми і бажанням розробників IoT-платформ комбінувати фантазії маркетологів, як, наприклад, це робить IBM (IoT Foundation application enablement platform + Bluemix IaaS backend).

IoT Analytics виділили вісім компонентів повноцінної IoT-платформи:

- *Зв'язок і нормалізація (Connectivity & normalization):* зведення різних протоколів і форматів даних в один "програмний" інтерфейс, гарантуючи точну передачу даних і взаємодію з усіма пристроями.
- *Управління пристроями (Device management):* забезпечення належного функціонування підключених "Інтернет-речей", їх конфігурацію, безперебійну роботу, встановлення патчів і оновлень. Причому, не тільки ПО власне "речей", але і додатків, що працюють на пристрої або прикордонних шлюзах.
- *База даних (Database):* тут все досить зрозуміло і прозоро - сховище даних від "речей", що масштабується. Вимоги до цих даних, спроба навести порядок в обробці і перенесення даних з, наприклад, різних "платформ" або зовсім до інформаційних систем "третіх осіб".
- *Обробка та управління діями (Processing & action management):* дані, отримані від "речей" в кінцевому підсумку впливають на події в реальності. Отже "платформа" повинна вміти будувати процеси, "тригери подій" та інші "розумні дії" на основі конкретних даних датчиків.
- *Аналітика (Analytics):* дані від "речей" є цінними самі по собі. Тому існування комплексу засобів їх аналізу є обов'язковою вимогою до "платформи". Якщо сюди включити ще й кошти кластеризації даних і глибокого машинного навчання аж до прогнозуючої аналітики, то

цінність "платформи" очевидно зростає.

- *Візуалізація (Visualization):* всю перераховану вище аналітику було б непогано показати таким чином, щоб людям було зрозуміло, приємно і красиво. Будувати графіки, моделі, просто візуалізувати те, що відбувається з "речами". Ну, і просто зручний інтерфейс.
- *Додаткові інструменти (Additional tools):* набір інструментів, який дозволяє розробникам IoT створювати прототипи, тестувати і пробувати різні системи. Бажано, щоб не дуже заглиблюватися в код і програмування.
- *Зовнішні інтерфейси (External interfaces):* інтеграція за допомогою платформи - одна з головних можливостей. Світ інтернет-розробки сьогодні не терпить замкнутих рішень. Завжди може знадобитися передача і обмін зі сторонніми системами. Тому справжня IoT-платформа повинна мати інтерфейси прикладного програмування (API), комплекти розробки програмного забезпечення (SDK) і шлюзи.

3.1 Огляд платформи Linux Foundation

Організація Linux Foundation представила новий спільний проект EdgeX Foundry, націлений на розвиток відкритої платформи для спрощення створення рішень на базі IoT-пристроїв. Метою EdgeX Foundry є надання універсальної модульної платформи для забезпечення взаємодії між IoT-пристроями, додатками і сервісами, а також створення екосистеми з компаній-виробників, що випускають сумісні і взаємозамінні компоненти для Інтернету речей. Платформа не прив'язана до обладнання конкретних постачальників і операційним системам, і розвивається незалежної робочою групою, під егідою Linux Foundation [32].

Платформа дозволяє створювати шлюзи, які б поєднували наявні IoT-пристрої і збирають дані від різних датчиків. Крім організації взаємодії з пристроями, в цій платформі шлюз виконує завдання по первинній обробці, агрегування та аналізу інформації, виступаючи проміжною ланкою між мережею з

IoT-пристроїв і локальних керуючим центром або хмарної інфраструктурою управління. На шлюзах також можуть виконуватися обробники, оформлені у вигляді мікросервісів. Взаємодія з IoT пристроями може бути організовано по дротову або бездротову мережу з використанням TCP / IP-мереж і специфічних (НЕ-IP) протоколів.

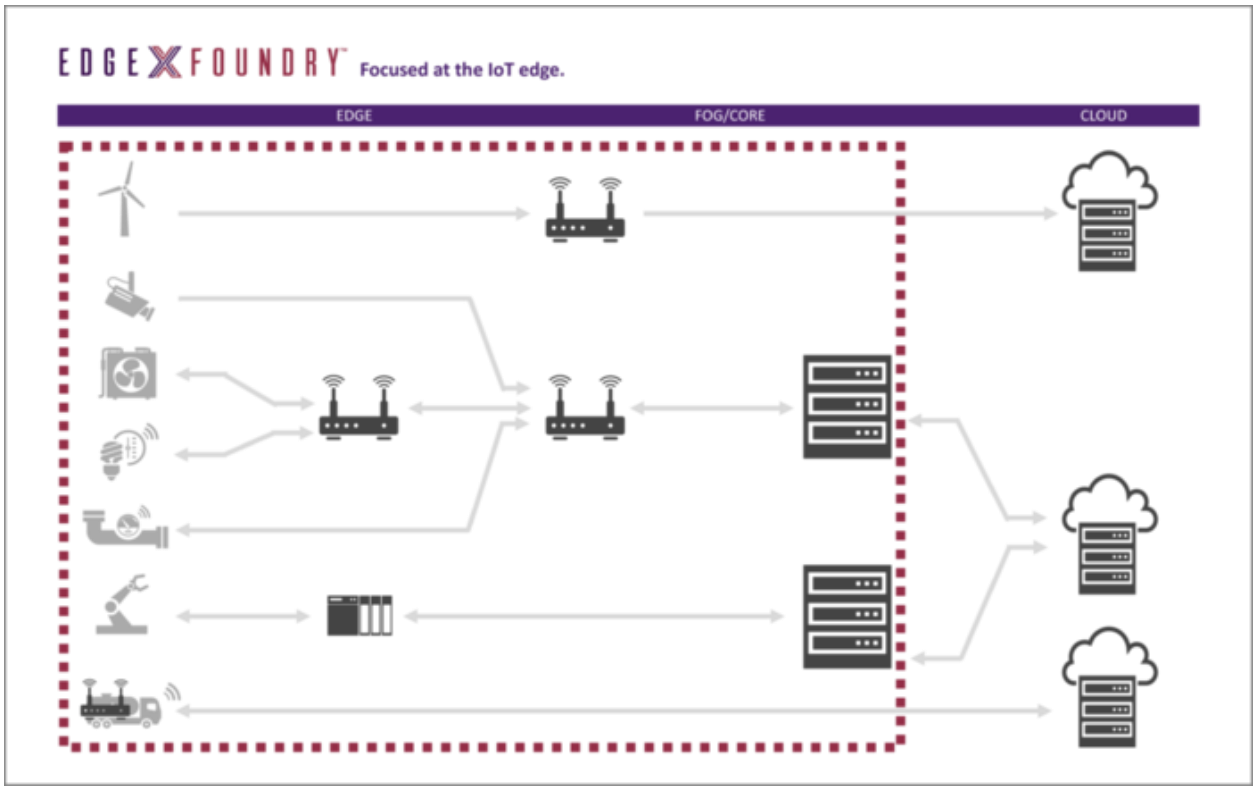

Рисунок 3.1 - Структура платформи Linux Foundation [32]

Шлюзи різного призначення можуть об'єднуватися в ланцюжки, наприклад, шлюз першої ланки може вирішувати завдання з управління пристроями (system management) і забезпечення безпеки, а шлюз другої ланки (fog-сервер) зберігати дані, що надходять, виконувати аналітику і надавати сервіси (рис. 3.2). Система модульна, тому поділ функціональності на окремі вузли виконується в залежності від навантаження, в простих випадках достатньо одного шлюзу, а для великих IoT-мереж може бути розгорнутий цілий кластер.

В якості основи EdgeX виступає IoT-стек Fuse, який застосовується в шлюзах для IoT-пристроїв Dell Edge Gateway. Компанія Dell відкрила всі пов'язані з Fuse напрацювання під ліцензією Apache 2.0 і передала права на проект під піклування

Linux Foundation. Консорціум Linaro увійшов в число учасників проекту і вважає, що EdgeX доповнює ініціативу LITE (Linaro IoT and Embedded), зосереджену на низькорівневих компонентах для IoT-пристроїв. Згадується також робота по інтеграції EdgeX з ОС реального часу Zephyr, що розвивається Linux Foundation для Інтернету речей.

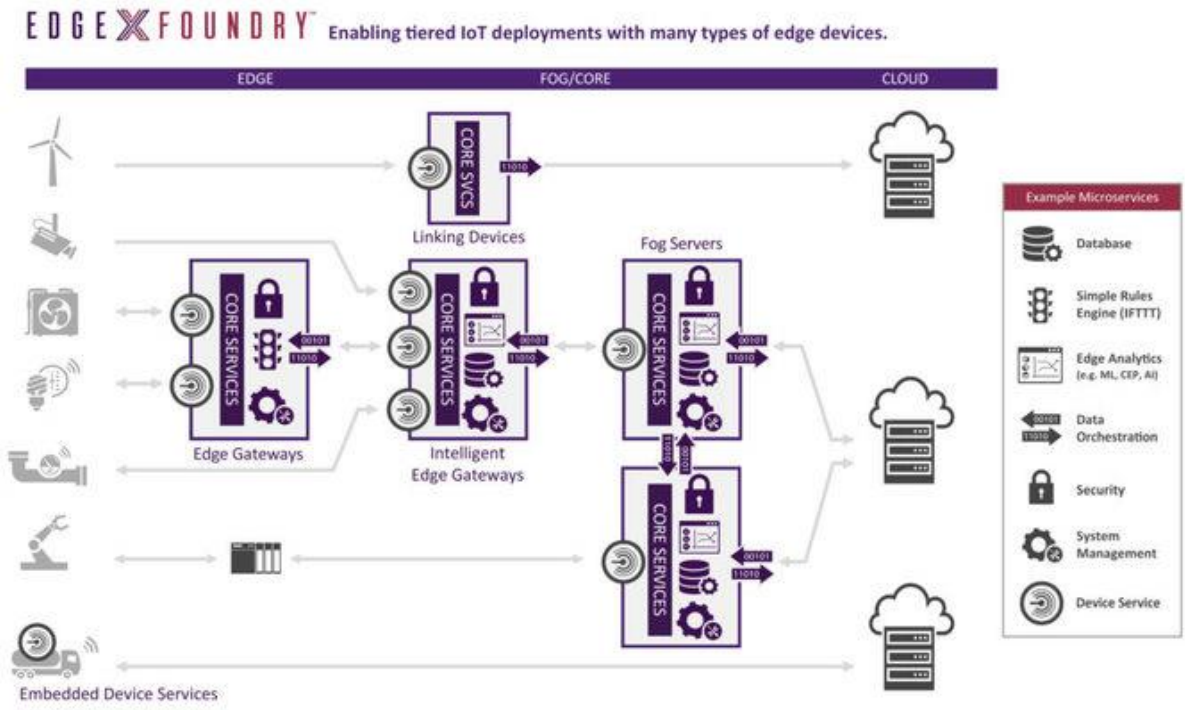

Рисунок 3.2 - Ланцюжки із шлюзів з різною функціональністю [32]

Проект EdgeX налічує понад 125 тисяч рядків коду і включає в себе добірку готових мікросервісів для аналізу даних, забезпечення безпеки, управління і вирішення різних завдань. Платформа може бути встановлена на будь-яке обладнання, включаючи сервери на базі CPU x86 і ARM, що працюють під управлінням Linux, Windows або MacOS. Для розробки мікросервісів можуть використовуватися мови Java, Javascript, Python, Go і C / C ++. Для розробки драйверів для IoT-пристроїв і датчиків пропонується SDK.

Отже EdgeX не притримується рекомендацій, що зазначенні в моделях Всесвітнього форуму IoT та моделі від MCE-T. Ця платформа сильно розширює можливості шлюзу додаючи до можливості «перепакування» даних ще й функції

туманних обчислень, таких як: первинної обробки даних та прийняття рішень в режимі реального часу (а не в часі транзакції при використанні хмарних сховищ), збереження, захист та аналіз даних.

Платформа має доволі широке поле застосування: безпека та спостереження, енерговиробництво, промисловість, розумний будинок, логістика. Для роботи с цією платформою найкраще підходять шлюзи від фірми Dell, адже вони використовують той самий стек Fuse.

3.2 Огляд платформи AggreGate

AggreGate - це інтеграційна платформа для Інтернету речей, що пропонує швидке рішення п'яти головних завдань будь-якої IoT програми: отримання, зберігання, обробка, візуалізація даних та інтеграція з додатками рівня підприємства. На відміну від інших рішень, що надають базову інфраструктуру і комплекти розробника ПЗ для розробки вертикальних додатків, AggreGate пропонує не тільки інструменти візуальної розробки для побудови інтерфейсів кінцевих користувачів, а й ланцюжок обробки даних на сервері.

Незалежна від постачальника M2M платформа включає сотні драйверів пристроїв, що роблять можливим підключення будь-якого промислового або призначеного для користувача IoT пристрою. Крім застосування нормалізації даних на базі драйверів, AggreGate уможливлює отримання даних через зовнішні або вбудовані Агенти, конвертери протоколів пристроїв, що забезпечують буферизацію даних і підключення до серверів, оптимізовані для ненадійних стільникових і супутникових каналів з низькою пропускною здатністю.

AggreGate підлаштовує існуючі технології M2M, віддаленого моніторингу та обслуговування під новий світ IoT, що ґрунтується на відкритих стандартах, впровадженні хмарних додатків, засобах зберігання і обробки великих даних, багатому інтерфейсі користувача в браузері на базі HTML5 і інші тенденції. Це економить роки розробки і мільйонні інвестиції в розробку масштабованих і надійних рішень для Інтернету речей, інтегрованих в підприємство.

У той час як більшість вендорів IoT платформ пропонують інфраструктуру

нижнього рівня для збору і зберігання даних, а також пропонують кінцевому користувачеві API і SDK для розробки додатків, IoT платформа AggreGate пропонує комплексне візуальне конфігурування, яке включає налаштування ланцюжків обробки даних, правил прийняття рішень, географічних карт, інструментальних панелей продуктивності, форм введення даних і навіть динамічних компонентів інтерфейсу без необхідності написання програмного коду.

Платформа AggreGate скорочує капітальні витрати і термін впровадження для виробників обладнання та системних інтеграторів, що створюють нові рішення для Інтернету речей. Вона являє собою міцну основу для підключення IoT пристроїв до додатків управління і веб-інтерфейсів кінцевого користувача. Платформа гарантує високий показник повернення інвестицій для будь-яких IoT проектів, оскільки скорочує час простою системи і експлуатаційні витрати, підвищує ефективність і загальну задоволеність клієнтів.

Основними перевагами AggreGate є:

- *Широкі можливості підключення IoT пристроїв:* AggreGate підтримує великий набір комунікаційних протоколів, включаючи M2M / IoT, IT та протоколи автоматизації, а також такі загальні протоколи, як SQL і SOAP. Якщо операції запису і контролю підтримуються протоколом, AggreGate може їх використовувати.
- *Адаптована для M2M комунікацій:* Агенти встановлюють вихідні повідомлення з самим сервером. Це є ідеальним рішенням для стільникових і супутникових мереж, що не присвоюють білі статичні IP-адреси. Та ж технологія вирішує будь-які проблеми з брандмауерами і перетворенням мережевих адрес типових промислових мереж.
- *Єдина модель даних:* Єдина модель даних AggreGate надає загальний гнучкий підхід до конфігурації, контролю і моніторингу будь-яких пристроїв, джерел даних і системних об'єктів, незалежно від вендора, моделі, типу і цілі.

- *Модульна, масштабована і надійна IoT архітектура:* Модульна архітектура хмарної IoT платформи AggreGate гарантує, що нові модулі зберігання, обробки і візуалізації даних можуть встановлюватися в ядро сервера як плагіни. Наприклад, додавання можливостей відстеження транспорту в існуючу M2M систему є справою звичайного встановлення пакета розширення.
- *Пакетна відкладена конфігурація пристроїв:* Не потрібно чекати, поки всі вони одночасно перейдуть у режим онлайн, достатньо внести зміни в конфігурацію і вони вступлять в силу в якомога більш стислі терміни.
- *Централізоване управління вбудованим ПО:* Централізоване оновлення вбудованого ПЗ та конфігурації вкрай важливо для будь-якої програми Інтернету речей. Ці оновлення можуть доставлятися пристроям користувача через центральний сервер за допомогою стандартних і приватних комунікаційних протоколів. Планування розподілу на нічні години не порушує роботу сервісів.
- *Дизайнер планів віддалених об'єктів:* Платформа для M2M додатків має вбудований візуальний редактор інтерфейсів. Це засіб побудови форм, графіків, звітів, таблиць, інтерфейсів і карт за допомогою миші. Не потрібно ніякого програмування навіть при побудові компонентів інтерфейсу з даними серверів / пристроїв.
- *Динамічні карти:* Відображають пристрої, групи, маршрути, геозони, з'єднання та інші об'єкти на географічних картах, що використовують будь-який ресурс, наприклад Google Maps, Bing Maps, OpenStreetMap та інші. Додайте до карт шари, елементи управління і вибору і візуально побудуйте будь операторський інтерфейс.
- *Зведені інструментальні панелі станів:* Візуалізують групи пристроїв і КПЕ (ключові показники ефективності) в масштабі системи на інструментальних панелях операторів верхнього рівня, що мають багаторівневу деталізовану навігацію по індивідуальних пристроях і сервісах. Звіти користувача запускаються за кілька кліків.

- *Безпечні зв'язку між пристроями:* Всі зв'язки між серверами і агентами можуть встановлюватися через безпечні SSL з'єднання і стискатися, щоб відповідати GPRS / 3G / LTE і супутниковим каналам. Агенти досить розумні, щоб при необхідності відправляти тільки важливі події замість необроблених значень метрик.
- *Зберігання великих даних в хмарі:* Незважаючи на те, що всі реляційні бази даних корпоративного рівня підтримуються як системи зберігання даних пристроїв, потоки подій зі світу Інтернету речей можуть направлятися в хмару великих даних. Інтегроване сховище типу NoSQL може працювати як всередині сервера, так і в якості окремого кластера зберігання, що складається з декількох вузлів.
- *Тривоги і обробка подій:* Гнучкі можливості керування пристроями, що включають фільтрацію, агрегування, маскування, кореляцію, підтвердження подій і аналіз першопричин. Настроюються тривоги, що підтримують різні типи тригерів, повідомлень (звукові, спливаючі повідомлення, e-mail, SMS і т.д.), ескалацію і коригувальні дії.
- *Графіки і тренди:* Підтримка графіків надає величезний список типів графіків, включаючи динамічно оновлювані. Тисячі властивостей графіків, що налаштовуються. Підтримка ліній трендів, що автоматично розраховуються.
- *Докладні звіти:* Інструмент створення звітів з розширеними можливостями, автоматичне створення звітів на базі будь-яких даних. Вбудований редактор звітів, роздруківка та експорт звітів в різні формати.
- *Безкоштовний комплект розробника ПЗ:* можна використовувати API з відкритим вихідним кодом для Java, .NET, C / ++ і мобільних пристроїв з метою розширення можливостей рішення для Інтернету речей та інтегрувати IoT сервіси в будь-які інші корпоративні системи.
- *Гнучка модель безпеки:* З самого початку AggreGate розроблявся із застосуванням багатоклієнтського, розрахованого на багато

користувачів підходу. Тонко налаштовуються права доступу і рольовий контроль доступу нерозривно вбудовані в усі аспекти системи.

- *Відмовостійка кластеризація:* Всі головні технології IoT покладаються на сервіси високої доступності, що забезпечуються багатовузловим ВІДМОВОСТІЙКИМ кластером. Два рівня кластерів гарантують захист сервера AggreGate і лежить в основі бази даних. Власна технологія кластеризації не залежить від стороннього ПЗ або підтримки кластеризації операційною системою.
- *Розподілена архітектура:* На відміну від багатьох M2M платформ, AggreGate масштабується до тисяч мікросерверів, що працюють на одноплатних комп'ютерах Linux на базі ARM, а також до мільйонів пристроїв в хмарі пристроїв. Унікальна багаторівнева розподілена архітектура дозволяє встановити дійсно пірингові відносини між усіма вбудованими та звичайними серверами. Це гарантує необмежену масштабованість за допомогою балансування функціоналу системи між багатьма серверами, розділеними на кілька рівнів.

3.3 Огляд платформи Everyware Cloud

Everyware Cloud (EC) від Eurotech (рис. 3.3) є M2M / IoT-платформою, яка спрощує управління пристроями і збором даних шляхом підключення розподілених пристроїв через безпечні і надійні хмарні сервіси. Після того як пристрої будуть розгорнуті, Everyware Cloud дозволяє користувачам підключати пристрої, конфігурувати і управляти ними протягом всього життєвого циклу проекту [24].

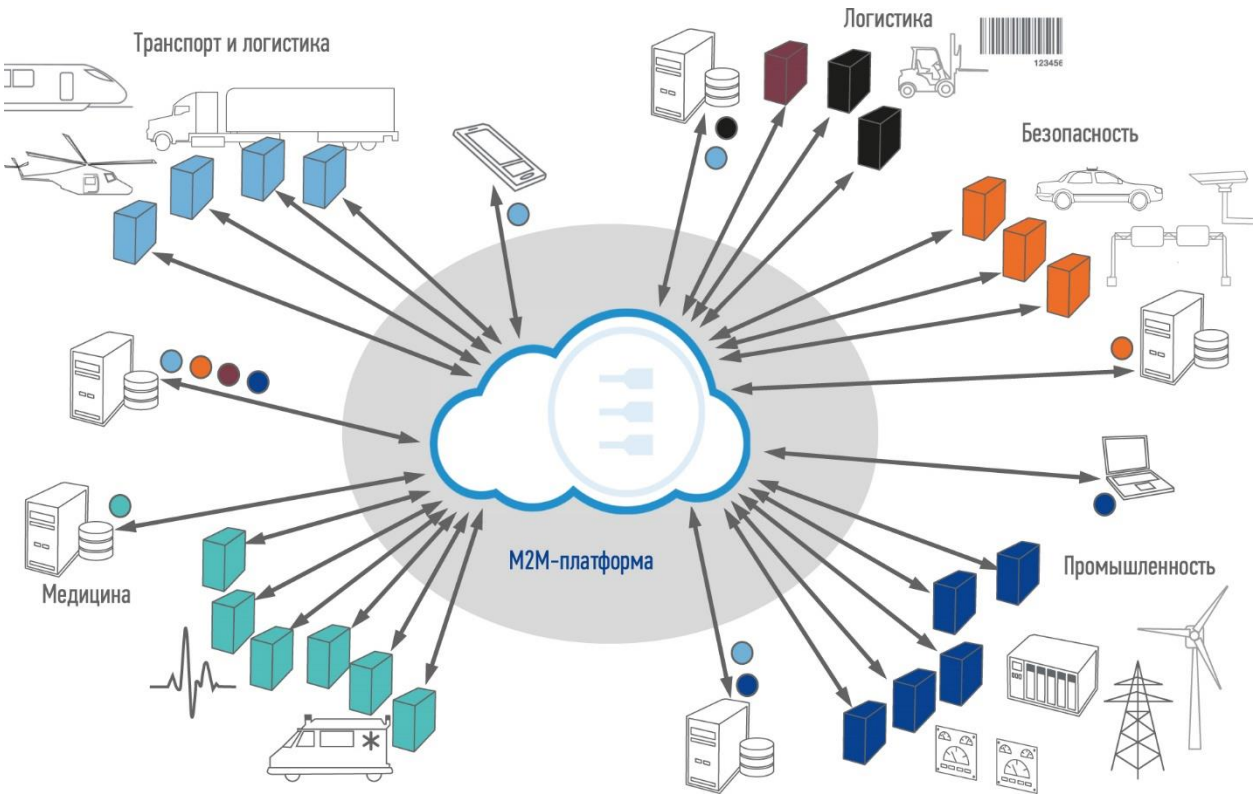

Рисунок 3.3 - Хмарна платформа Everyware Cloud [24]

Платформа Everyware Cloud може розгортатися як у публічній хмарі, так і в приватній. Для організації приватної хмари Eurotech пропонує спеціалізований Everyware Server - інтеграційну платформу M2M, розроблену для забезпечення додаткового рівня безпеки та конфіденційності за допомогою громадських хмарних технологій або без них, що охоплює всі можливості технології Everyware Cloud, виконану у вигляді надійного апаратного пристрою для забезпечення зручного і повного контролю в центрі обробки даних.

Everyware Server полегшує управління пристроями і даними при підключенні розподілених пристроїв до бізнес-додатків підприємства, з використанням безпечних і надійних протоколів зв'язку та обміну даними.

Everyware Cloud (рис. 3.4) представляє собою програмну платформу, яка швидко з'єднує пристрої для створення і підтримки закінченого M2M-додатку. Вона забезпечує легкий шлях для підключення пристроїв до IT-систем і / або додатків.

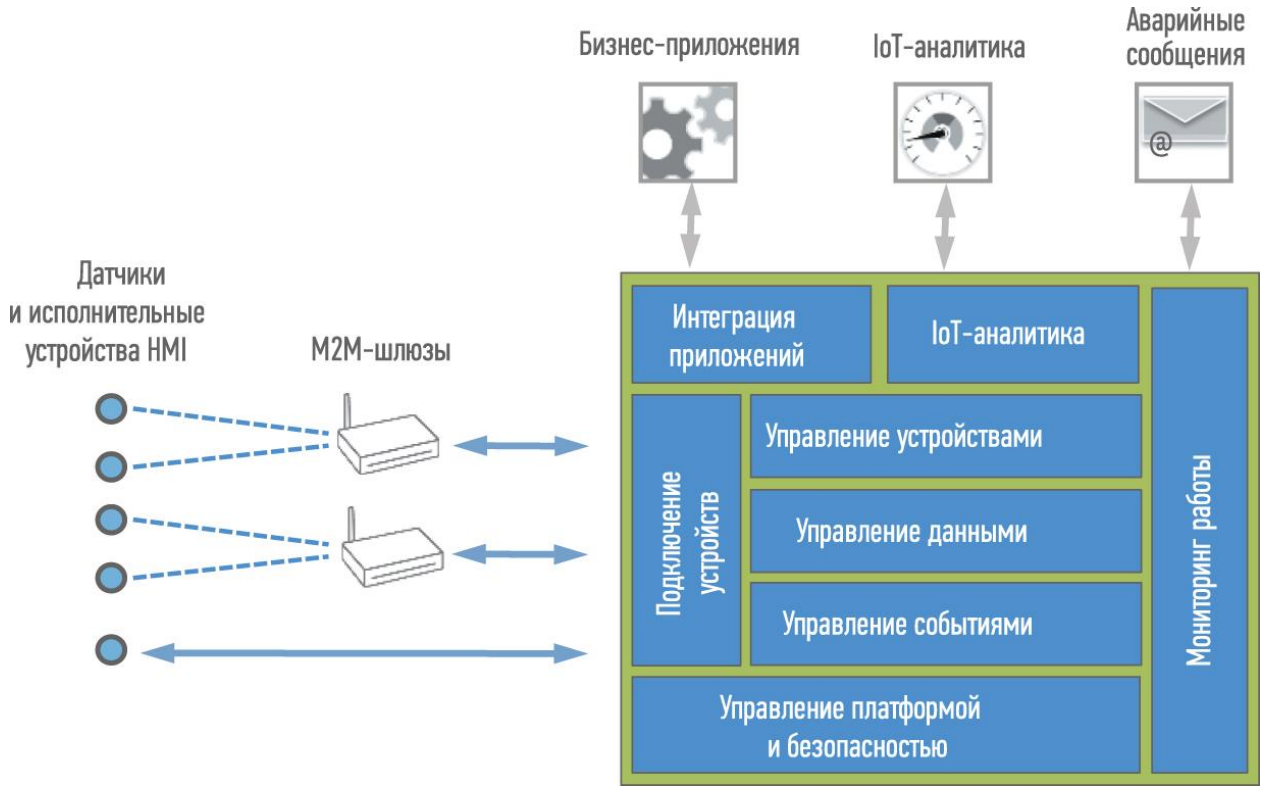

Рисунок 3.4 - Структура Everyware Cloud [24]

Eurotech Everyware Device Cloud (EDC) - повністю закінчене рішення, яке містить спеціалізовані апаратні засоби, підключення і управління пристроями за допомогою Eurotech Software Framework і хмарні сервіси Everyware Device Cloud Client і M2M для обміну даними між польовими пристроями та бізнес-додатками підприємства.

IoT-платформа компанії Eurotech дає можливість спростити реалізацію складних проектів, дозволяючи отримати готове рішення швидше, ніж будь-коли раніше. Повна пропозиція включає:

- вбудовані комп'ютери і процесорні плати Eurotech, виконані на базі продуктивних процесорних платформ з низьким енергоспоживанням;
- операційну систему Linux (Wind River, Yocto, Red Hat) з повним набором інструментів для розробки і підтримки продуктів;
- програмний пакет Everyware Software Framework (ESF), щоб спростити розробку додатків і підключення до мережі;

- хмарний клієнт Everyware Device Cloud для впровадження ефективних, надійних і захищених протоколів, що забезпечують дієвий зв'язок навіть в складних умовах;
- хмарний сервіс Everyware Cloud для миттєвого доступу до даних і управління пристроями через хмарні платформи.

3.4 Висновки

Отже IoT платформи об’єднують речі та Інтернет. Основними вимогами до IoT платформи за IoT Analytics є:

- Зв’язок і нормалізація
- Управління пристроями
- База даних
- Обробка та управління діями
- Аналітика
- Візуалізація
- Додаткові інструменти
- Зовнішні інтерфейси

Було розглянуто ряд платформ, як відкриті, так і комерційні проекти. Роль шлюзів варіюється від звичайних маршрутизаторів для перепакування даних для роботи в мережі Інтернет до міні серверів, що знаходяться на межі між речами та Інтернетом і виконують функції агрегування та аналізу, реагують на певні події незалежно від хмари, тобто займаються туманними обчисленнями.

4 ОГЛЯД МОДЕЛЕЙ ШЛЮЗІВ ВІДОМИХ ВИРОБНИКІВ

Узагальнюючи аналіз еталонних моделей IoT можна виділити перелік наведених нижче функцій шлюзів і характеристик шлюзів. Важливо підкреслити, що сьогодні переважна більшість виробників, особливо у старших моделях своїх шлюзів, забезпечують можливості як первинної обробки даних, до якої зазвичай відносять обробку подій і прийняття рішень в режимі реального часу, нормалізацію і фільтрацію даних для подальшої передачі на хмарний сервер, так і повноцінну аналітику зі зберіганням і візуалізацією даних. Основними критеріями при виборі шлюзу для Інтернету речей можна назвати:

Підтримка перефирійних/туманних обчислень.

В цьому випадку у якості критеріїв вибору слід звернути увагу на наступне:

- Підтримка шлюзом надійної спеціалізованої ОС (наприклад, від Wind River, Cisco, Microsoft).
- Наявність у фірми розробника шлюзу готових додатків для обробки даних, якість і можливості цих додатків, а також можливість підтримки їх даною моделлю шлюзу.
- Наявність у фірми розробника платформ для розробки замовником власного додатку зі зручними інтерфейси прикладного програмування (API) та комплектами розробки ПЗ.
- Можливості вибору ОС, мов та засобів програмування для реалізації власного додатка забезпечують адаптацію до потреб проекту.

Підтримуванні технології обміну даними

Підтримка необхідних технологій доступу до пристроїв для обміну даними між ними та з корпоративними або хмарними додатками IoT. Тут відображуються можливості збору даних з різних джерел, їх інтеграції, уніфікації представлення протоколів і форматів даних. В даному пункті слід звернути увагу на наступне:

- Максимальна кількість пристроїв, з якими може взаємодіяти шлюз:
- Перелік інтерфейсів з пристроями, в який можуть входити як сучасні

протоколи дротових і бездротових мереж (Ethernet, Wi-Fi, Zigbee, 6LoWPAN, Bluetooth Low Energy та ін.), так і успадковані протоколи (BACNet, Modbus і CANbus та ін.).

- Перелік інтерфейсів зовнішнім сервером додатків, в який можуть входити протоколи дротових і бездротових мереж: Ethernet, Wi-Fi, протоколи стільникового зв'язку та ін.
- Підтримка GPS разом із стільниковим зв'язком забезпечить ефективну роботи з мобільними об’єктами з географічною прив'язкою, наприклад, транспортом.
- Наявність хорошого інтерфейсного профілю, заснованого на реалізації універсального само налаштування (UPnP, Universal Plug and Play), що визначає протокол для взаємодії з різними пристроями.

Функції маршрутизатора.

Оскільки шлюз є вузлом стандартної IP мережі при взаємодії з сервером, то він зобов'язаний підтримувати мінімальні функції маршрутизатора. У той же час ряд виробників (наприклад, Cisco, Intel, Huawei), позиціонують ряд моделей своїх шлюзів як повноцінні багато портові маршрутизатори. В цьому випадку можна виділити наступні можливості:

- Підтримка маршрутизації між декількома провідними чи Wi-Fi локальними IoT мережами.
- Підтримка поширених функції IP маршрутизаторів - протоколів маршрутизації, DHCP, таблиць доступу, міжмережевих екранів і т.д.

Функції управління кінцевими пристроями мережею і додатками:

- Управління пристроями включає можливості їх виявлення і автентифікації, конфігурацію, діагностику, оновлення прошивки і/або ПЗ, управління робочим статусом пристрою.
- Управління мережею включає можливості управління її моніторингом і конфігурацією, виявлення і керування перевантаженнями, керування трафіком, вимогами QoS.
- Управління додатками включає можливості керування їх

встановленням і видаленням, виконанням оновлень, резервним копіюванням, відслідковуванням і усуненням несправностей.

Функції безпеки пристроїв, мережі і додатків.

Як підкреслюється усіма без винятку авторами, наступні функції для IoT є життєво важливими.

- Захист на рівні ПЗ включає авторизацію, автентифікацію, конфіденційність і цілісність даних програми, захист недоторканності приватного життя, аудит безпеки і антивірусний захист.
- Захист на рівні мережі включає авторизацію, автентифікацію, конфіденційність даних, конфіденційність і цілісність даних сигналізації.
- Захист на рівні пристрою включає автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

Функції управління і безпеки всі крупні вендори забезпечують засобами власних платформ, власних ОС таких як Wind River Linux, Windows 10 IoT, Cisco IOS, додатковими апаратними засобами (Dell, Cisco), власними пакетами ПЗ, а також підтримкою стандартних рішень і сертифікованих рішень від сторонніх компаній.

Інші характеристики.

У рамках подібної функціональності шлюзи можуть відрізнятися такими технічними характеристиками, серед яких можна виділити наступні.

- Обчислювальна потужність, об’ємами пам’яті і її типами, що важно врахувати при плануванні реалізації на шлюзі додатків.
- Форм фактор – компактність і форма конструктивного виконання, що важливо враховувати при плануванні місця розташування шлюзу.
- Умови експлуатації. Одні пристрої придатні лише для роботи у звичайних приміщеннях, інші - розраховані на роботу в широкому діапазоні температур, в умовах підвищеної вологості, запиленості.

Слід також звернути увагу на те, ринок послуг та пристроїв IoT зазвичай

поділяють на два великі сегменти: *промисловий* і *споживчий* та сегмент, які відрізняються вимогами до ціни, надійності, безпеки, потужності, масштабованості. У цих рамках вендори можуть надавати як універсальні пристрої так і пристрої для конкретних вертикалей ринку в складі комплексних рішень. Більшість виробників орієнтуються на промисловий ринок, хоча молодші моделі їх рішень, наприклад, Intel цілком підходять для простих економних рішень. А продукція таких компаній як Google чи Samsung в першу чергу орієнтована на споживчий ринок.

Визначивши основні параметри, котрі повинен задовольняти шлюз можна провести огляд пропозицій від лідерів ринку IoT, а також від декількох компаній, що вийшли на ринок недавно. Перелік 15 перших вендорів з традиційного списку CRN/США «IoT 50» за 2017 рік можна знайти у [23].

4.1 Огляд шлюзів компанії Eurotech

Компанія Eurotech в першу чергу відома своєю хмарної IoT платформою Everyware, яка покликана спростити адміністрування пристроїв і керування даними, забезпечуючи підключення розподілених пристроїв через захищені хмарні сервіси. Використовуючи цю платформу, замовники можуть відслідковувати, конфігурувати свої пристрої і керувати ними протягом всього життєвого циклу.

Практично всі шлюзи компанії Eurotech призначені для промислового застосування та експлуатації в жорстких умовах. Також компанія пропонує рішення, в тому числі шлюзи, для таких вертикалей ринку як транспорт і роздрібна торгівля. Всі шлюзи мають досить великий набір інтерфейсів вводу/виводу і польових шин, а також необхідний набір дротових і бездротових мережевих інтерфейсів для організації надійного зв'язку: Fast або Gigabit Ethernet, стільниковий зв'язок, Wi-Fi, Bluetooth, ZigBee. Для підключення шлюзів до локальних хмарних сервісів можна використовувати Ethernet або Wi-Fi, а до віддалених - технології стільникових мереж. Завдяки підтримці стільникового зв'язку з GPS більшу частину шлюзів можна використовувати для геолокації об'єктів, що переміщаються.

Широка лінійка шлюзів містить як компактні пристрої з низьким енергоспоживанням, так і високопродуктивні вбудовані ПК з широким функціональним набором. Пристрої серій *ReliaGATE 10-20, ReliaGATE 10-11 і ReliaGATE 10-05* можуть служити малопотужним шлюзом для легких промислових застосувань. Їх основні функції - агрегування даних, одержуваних з польових пристроїв, перетворення повідомлень і протоколів, маршрутизація пакетів, організація двобічного зв'язку з хмарним сервером, де дані збираються, зберігаються і обробляються за допомогою бізнес-додатків.

Шлюзи серій *ReliaGATE 20-25, ReliaGATE 20-26, DynaGATE 15-10* пропонують додаткові можливості по обробці і зберіганню даних для надання послуг в автономному режимі, а при підключенні до хмарних додатків забезпечують контроль і управління в реальному часі. Вони часто застосовуються для виконання аналітичних функцій або завдань попередньої обробки, зокрема для передачі даних, що відповідають заданим параметрам.

Практично всі шлюзи, крім ReliaGATE 20-26, який використовує Red Hat Linux, поставляються з попередньо встановленою операційною системою Yocto Linux. Велика частина шлюзів забезпечується програмним забезпеченням Everyware Software Framework (ESF) на базі Eclipse Kura і Java/OSGi. Крім того, в якості шлюзів можуть виступати і процесорні плати в різних форм-факторах, на які також встановлюється спеціалізоване програмне рішення.

ESF - це промислова версія Eclipse Kura (версія з відкритим вихідним кодом) з додатковими можливостями з безпеки, діагностики, конфігурації і віддаленого доступу, повністю інтегрована в платформу Everyware Cloud. ESF/Kura дозволяє розробникам зосередити свою увагу на аналітиці та специфіці додатків і полегшити контроль і управління роботою шлюзу (змінювати параметри в реальному часі, оновлювати ПЗ, робити моніторинг пристрою, діагностику, забезпечувати безпеку і т. д.) [24].

4.2 Огляд шлюзів компанії Intel

Шлюзи Intel для IoT дуже різноманітні і здатні задовольнити розробників

проектів будь-якої складності. Їх оснащують процесорами Quark, Atom, Core, Xeon. Шлюзи на базі Intel Quark, засновані на платі Intel Galileo, є гнучким, малопотужним і недорогим рішенням для організації нескладних обчислень і інтеграції пристроїв IoT. Процесори Intel Atom і Intel Core останніх поколінь забезпечують більш високу продуктивність, хорошу графіку і багату інтеграцію введення-виведення. Сімейство Intel Xeon допомагає створювати шлюзи для інфраструктури з обчисленнями в пам'яті, аналізу в режимі реального часу, підвищеною оперативністю і безпекою. Шлюзи оснащують сховищами даних і оперативною пам'яттю, які відповідають вимогам процесора і призначень пристроїв.

Шлюзи технології Intel IoT Gateway випускаються більш ніж десятком фірм. Вони забезпечуються засобами для створення власних додатків первинної обробки даних, збору даних з безлічі пристроїв, функціями перетворення протоколів і керування різними пристроями. Шлюзи Intel для IoT можуть підтримувати різні операційні системи, включаючи Windows 10 IoT і кілька мов програмування.

Більшість моделей поставляється з встановленою ОС Wind River Linux, в якій передбачений захист пристроїв від внутрішнього або зовнішнього несанкціонованого доступу. При цьому, в області захисту даних, тут є шифрування і безпечний обмін інформацією з зовнішніми системами. У Wind River Linux в систему вбудовано керуюче ПО, яке дозволяє управляти не тільки локальними, але і віддаленими пристроями. Контролювати їх можна або вручну, або в автоматичному режимі, ґрунтуючись на критеріях, заданих адміністраторами і програмістами. Крім того, підтримка платформ Wind River Helix Device Cloud і Wind River Helix App Cloud, дають великі можливості по управлінню пристроями, додатками і хмарними сервісами.

Шлюзи Intel володіють великими мережевими можливостями. Вони можуть підключатися відразу до двох локальних дротових мереж, одночасно працювати в декількох Wi-Fi-мережах, і, не перериваючи зв'язок, взаємодіяти зі спеціалізованими пристроями, використовуючи інші типи мереж. Різноманітність підтримуваних мережевих інтерфейсів дозволяє рішенням для IoT створювати

мережі на базі технологій Bluetooth, ZigBee, 6LoWPAN і ін., підключатися до хмарних сервісів, організовувати різні схеми управління. У список підтримуваних мережевих інтерфейсів входять і мобільні мережі: GPRS, 2G, 3G. LTE [25].

4.3 Огляд шлюзів компанії Huawei

У компанії Huawei є цілий спектр продуктів, який формує середовище передачі, зберігання і обробки даних IoT за допомогою різних аналітичних систем. Складовими платформи для зберігання і обробки великих даних є Huawei FusionStorage і FusionInsight.

Шлюзи серії AR від Huawei працюють як високопродуктивні маршрутизатори IoT, і особливо підходять для відеоспостереження, виробництва, транспортування, електропостачання та інших зовнішніх операцій. Лінійка дуже різноманітна и може задовольнити будь-які потреби як у плані обчислювальної здатності, так і у вимогах до різноманітних інтерфейсів підключення. Легкість зв’язку із речами та шлюзами забезпечується платформою IoT Connection Management Platform.

У лінійки в наявності є безліч типів інтерфейсів, які підходять до різноманітних терміналів. Шлюзи підтримують різні протоколи бездротового зв’язку: Wi-Fi, ZigBee, Bluetooth та RF. Також наявна підтримка сотового зв’язку у мережах GSM, 3G та 4G/LTE, що разом із підтримкою GPS робить шлюз працездатним при перегонах транспорту. Маршрутизація трафіку може бути гнучко налаштована політикою маршрутизацій, статичними маршрутами та підтримкою динамічних протоколів RIP, OSPF, IS-IS, BGP. Підтримується перетворення різних галузевих протоколів та побудова єдиної мережевої платформи.

Більша частина шлюзів лінійки зроблена відповідно до вимог промисловості, тому витримує роботу у екстремальних умовах, таких яких велика кількість пилу в повітрі, вологість і т.д. Відтак шлюзи можуть працювати при температурах від -40 °C до +70 °C при відносній вологості від 5 до 95 %. При чому певним пристроям, наприклад AR550E, навіть не потрібен вбудований вентилятор для охолодження.

Шлюзи виконані відповідно до вимог стандарту IEEE1613 і нормально функціонують навіть в умовах великих електромагнітних перешкод. Відповідність до стандартів віброзахисту надає право шлюзам компанії Huawei повноцінно працювати у сфері транспортування товарів.

У лінійці використанні високопродуктивні ARM процесори, що доповнюються великими об’ємами постійної пам'яті, в якості операційної системи використовується Wind River LINUX. Підтримка віртуалізації і можливість гнучкої масштабованої інтеграції додатків прискорюють розгортання послуг. Платформа надає управління повним життєвим циклом ІКТ-ресурсів: розгортання, моніторинг і видалення додатків через Agile Controller.

Платформа від Huawei надає зручне та об’єднане управління терміналами, шлюзами, програмами та даними. Запуск розгортання можна запустити всього лиш відсканувавши серійний номер пристрою (ESN). Це дозволяє дуже швидко вводити пристрої у експлуатацію. Завдяки уніфікованій системі керування мережею (NMS), пристрої можна об’єднувати в певні групи та масово ними керувати. Є можливість встановлення ПЗ із USB-накопичувача та майже моментальний початок користування завдяки функції «plug-and-play».

Для керування через Ethernet та розширених операцій Smart Grid, найкраще підходять AR2500 Agile Gateways, тоді як AR502 Gateways ідеально підходять для роботи в умовах екстремальних температур, високої вологості та електромагнітних перешкод. Для мережевої інтеграції та обміну через віртуалізацію корисні шлюзи AR3600 (з дизайном x86). Модель AR510 є потужним шлюзом для мультимедійних і відеосервісів у різних приміщеннях та на відкритому повітрі (включаючи "зв’язані автомобілі").

Безпека підтримується міжмережевим екраном із поділом на зони та відстеженням стану, автентифікацією на основі 802.1X та автентифікацією по MAC-адресі та веб-автентифікація. Наявний захист ARP і захист від атак ICMP. Додаткова безпека досягається завдяки відстеженню пакетів DHCP і відстеженню пакетів DHCPv6 CPCAR, чорному списку і відстеженню джерела атаки PKI і KPM [26].

4.4 Огляд шлюзів компанії Cisco

Стратегія Cisco в області IoT будується на шести стовпах технології: рішення з передачі даних в IoT-мережі, прикладна середу IOx і fog-додатки, а також IT-безпека, аналітика даних, засоби автоматизації та підтримка додатків. Саме Cisco ввів поняття туманних обчислень та Інтернету всього (IoE, Internet of Everything). Зокрема, компанія пропонує шлюзи, комутатори промислового класу і вбудовуються маршрутизатори для IoT з підтримкою платформи туманних обчислень IOx. IOx - це середа для додатків, яка допомагає мережевим пристроям, які її підтримують, контролювати і управляти пристроями IoT. Ця середа поєднує в собі найпопулярнішу відкриту ОС Linux, мережеву ОС Cisco IOS та потужні сервіси для швидкої та надійної інтеграції із сенсорами IoT, що дозволяє клієнтам створювати і запускати програми безпосередньо на промислових мережевих пристроях Cisco. Компанія Cisco створює та підтримує відкрите середовище для заохочення розробників переносити існуючі програми та створювати нові в різних галузях промисловості.

Компанія Cisco створює шлюзи для різноманітних вертикалей ринку: промисловість, енергозабезпечення, транспорт та логістика, розумні міста, навчання, охорона здоров’я та ін.

Також існує лінійка безпровідних шлюзів для мереж пристроїв LoRaWAN, що складається зі шлюзів IXM-LPWA-800-16-K9 (підтримує частоти 863–870 МГц) та IXM-LPWA-900-16-K9 (підтримує частоти 902–928 МГц). Цей тип зв’язку забезпечує M2M взаємодію на відстанях до 15 км при мінімальному енергоспоживанні, що забезпечує декілька років автономної роботи на одному акумуляторі AA. Вони підтримують до 16 каналів LoRa та захищені по стандарту IP67. Ці шлюзи вкрай зручні при використанні на рухомих об’єктах в автономному режимі роботи, а за рахунок волого- та пилозахищеності не потребують додаткових захисних коробів.

Широкий вибір маршрутизаторів у промисловому виконанні забезпечує функціональні можливості корпоративного класу, включаючи високоякісну

передачу даних, можливості голосового та відео зв'язку зі стаціонарними і мобільними вузлами мережі через дротові та бездротові канали зв'язку. Маршрутизатори Cisco надають доступну функціональність, що необхідна при створенні корпоративних рішень:

- динамічний багатоточковий VPN (DMVPN);
- аналіз якості обслуговування (QoS) для стільникового зв'язку;
- мульти-віртуальна переадресація маршрутів (VRF) для стільникового зв'язку;

Cisco IOx для маршрутизаторів 809 і 829, що забезпечує виконання граничного додатків в мережах IoT

Основною лінійкою IoT шлюзів від Cisco є Cisco 800, які позиціонуються як маршрутизатори промислової інтегральної мережі. На шлюзах Cisco встановлена операційна система Cisco IOS, що забезпечує просте управління, дає змогу створювати еластичні комунікації та підтримувати високий рівень безпеки.

Всі маршрутизатори серії 800 мають інтегроване 4G/LTE бездротове з'єднання WAN та підтримують більш старі версії стільникового зв’язку. Дві зовнішні антени забезпечать максимально якісний зв’язок, а дві різні, одночасно активні, SIM карти допоможуть підтримувати зв’язок різних операторів в залежності від якості сигналу.

Маршрутизатор 829 також забезпечує високоякісні з'єднання бездротової локальної мережі Wi-Fi, підтримуючи 2.4ГГц та 5ГГц діапазони. Також у наявності вбудований 2x2 MIMO, що забезпечує швидкість з’єднання до 300 Мб/сек. Доступні й стандартні Ethernet порти, що підтримують також і PoE/PoE+ з передачею потужності до 30 Вт.

Для забезпечення роботи в умовах виробництва шлюзи підтримують розширений діапазон температур від -40 º С до 60 º С. Для безперешкодної інтеграції із системами SCADA підтримуються протоколи DNP3, DNP3 IP та IEC від T101 до T104. Багатогалузева сертифікація шлюзів Cisco надає їм перевагу у корпоративних рішеннях, де велика увага приділяється надійності постачальника [27].

4.5 Огляд шлюзів компанії NEXCOM

Серія NEXCOM CPS складається зі шлюзів IoT, готових до застосування, які легко встановлювати та налаштовувати. Заздалегідь встановлена за допомогою NEXCOM Industrial IoT Studio допоможе полегшити розробку додаткового ПЗ. У лінійки наявна широка підтримка різноманітних операційних систем. Відтак на шлюзи можуть бути встановленні Windows 10 IoT, Ubuntu 14.04, FreeRTOS та інші Linux системи.

Встановлені процесори Intel Atom надають достатню потужність для обробки даних на краю при цьому мають гарну енергоефективність. Для більш потужних обчислень можна обрати моделі із використанням повноцінних та більш енергоємних процесорів Intel Celeron. Вид жорсткого диску та його об'єм варіюється від 16 ГБ e-MMC до 128 ГБ SSD із підтримкою порту розширення SD карткою.

Серія CPS може витягувати та аналізувати дані PROFIBUS, PROFINET та Ethernet, надсилати попереджувальні повідомлення, зберігати дані в локальні та віддалені бази даних та виконувати інші функції обробки даних після декількох кліків мишею. Серія CPS також підтримує API хмарних інтерфейсів для підключення до хмарних серверів через бездротові 3G/Wi-Fi (додатковий модуль) та/або дротові локальні мережі. За допомогою серії CPS виробники можуть визначати потоки даних, завантажувати дані з кінцевих пристроїв у платформи хмарної служби, включаючи Microsoft Azure та IBM Bluemix.

Завдяки надійному дизайну, серія CPS може бути встановлена поряд з PLC, датчиками та пристроями вводу-виводу в жорстких середовищах. На зосередженість у сфері промисловості та транспорту вказує захист від вібрацій та ударів, а також можливість роботи в температурному діапазоні від -20°C до +65°C при високій вологості [28].

4.6 Огляд шлюзів Edge Gateway компанії Dell

Компанія Dell просуває свої шлюзи серії Edge Gateway як економічне за

витратами рішення підвищеної надійності, призначене для агрегації, передачі даних і організації їх аналізу безпосередньо на периметрі мережі. Компанія пропонує два модельних ряди - Edge Gateway серія 5000 і Edge Gateway серії 3000. Шлюзи серії 5000 передбачають модульне розширення, орієнтовані на стаціонарні системи, великі сенсорні мережі і більш серйозну аналітику в прикордонних сегментах IoT мережі. Серія 3000 ідеально підходить як для фіксованих, так і мобільних варіантів використання, які потребують менших сенсорних мереж, менше місця, а також більш просту аналітику.

Шлюзи промислового класу Edge Gateway серії 5000 мають двоядерний процесор Intel Atom E3800, оперативну пам'ять ємністю від 2 Гбайт до 8 Гбайт, твердотільні накопичувачі ємністю 32 або 64 Гб і можуть працювати під управлінням різних ОС на вибір замовника Ubuntu Snappy, Wind River Linux або Windows 10 IoT Enterprise. Віддалене управління може здійснюватися для платформи WindRiver за допомогою Helix Device Cloud або Windows IoT Industry, а для Snappy Ubuntu - Dell Cloud Client Manager (CCM) або Dell Client Command Suite, Шлюзи серії 5000 є ідеальною платформою для засобів інтеграції внутрішніх даних і аналітики від компанії Dell, також вони сумісні зі сторонніми рішеннями, в тому числі від сертифікованих незалежних постачальників ПЗ з числа партнерів компанії Dell. Захист мережевої периферії і датчиків забезпечується завдяки вбудованим засобам IT-безпеки Dell.

Шлюзи виконані в промисловому формфакторі, відрізняється надійністю і тривалим терміном служби. Вони також придатні для експлуатації в умовах підвищеної вологості, запиленості та здатні працювати в широкому діапазоні температур. Модель Dell Edge Gateway 5100 можна експлуатувати при температурах від -30 ° C до + 70 ° C.

Універсальна підсистема вводу-виводу, яку легко розширити, дозволяє підключати, об'єднувати, передавати і відслідковувати дані з використанням практично будь-яких датчиків і мережевих протоколів від успадкованих протоколів (BACNet, Modbus і CANbus) до сучасних мереж (Zigbee, 6LoWPAN і Z-Wave). Мережеві можливості шлюзів підтримуються двома портами Gigabit

Ethernet і модулями 802.11n Wi-Fi, Bluetooth Low Energy, модулем зв'язку 3G або LTE.

Серія 3000 включає три моделі, які призначені для використання в якості вбудованих рішень в сфері промислової автоматизації, енергетики, транспорту і в системах цифрових табло. Вони дозволяють безпечно передавати важливі дані про функціонування фізичного обладнання на периферії мережі в реальному часі. Пристрої також розраховані на роботу в широкому діапазоні, стійкі до сильних ударів і вібрації.

Всі три моделі включають в себе: процесор Intel Atom, оперативна пам'ять ємністю 2 Гбайт і сховище eMMC на 8 Гбайт (32 Гбайт в конфігурації з WWAN). Вони оснащені інтерфейсами Fast Ethernet з функцією живлення PoE, портами USB 2.0. і 3.0, підтримкою стандартів підключення Wi-Fi, Bluetooth LE, стільникового зв'язку. Всі моделі мають вбудований модуль GPS, акселерометр і датчики атмосферного тиску для забезпечення ефективної мобільної роботи і управління ресурсами з географічною прив'язкою. У всіх моделях використовуються апаратні засоби захисту для забезпечення безпеки і конфіденційності даних.

Опціональне ПЗ Dell Edge Device Manager (EDM) допомагає з легкістю управляти віддаленими пристроями і гарантувати безпеку кожного з них.

Крім того, кожна модель шлюзів лінійки орієнтована на певну область застосування за рахунок додаткових можливостей. Модель 3001 орієнтована на застосування в сучасних виробничих середовищах, транспортних системах і периферійних мережах. Багатофункціональний порт GPIO (8-канальний) і програмовані послідовні порти (2 x RS-232, RS-422 або RS-485) дозволяють працювати з успадкованими системами, а також розширюють можливості підключення. Є можливість вибору ОС - Ubuntu Core 16.0 і Microsoft Windows 10 IoT. Модель 3002 орієнтована на застосування на транспорті і в логістиці. Стійкість до перебоїв живлення, підтримка інтерфейсу CANbus, наявність вбудованих адаптерів ZigBee дозволяє організувати стабільний зв'язок з самими різними системами і датчиками на різних видах транспорту. Модель 3003 розроблена для установки в цифрових табло і терміналах роздрібної торгівлі. Вона має вихід

DisplayPort 1.1 для відеодисплеїв (2560 x 1600) і роз'єм лінійного входу/виходу 3,5 мм для високоякісної потокової передачі аудіо.

Всі моделі обслуговуються службою підтримки Dell. Наприклад, пакет послуг Dell ProSupport передбачає автоматизоване визначення проблем, цілодобовий доступ до інженерів служби підтримки і швидкої заміни компонентів для мінімізації простоїв; послуги розгортання Dell Deployment; програма Dell IoT Solutions Partner Program для управління рішеннями IoT; Dell Financial Services для оцінки вартості проекту (фінансових можливостей) [29].

4.7 Огляд Enterprise шлюзів компанії Hewlett Packard

В області IoT компанія HP активно просуває рішення, що дозволяють перенести обробку даних з хмарних центрів обробки даних на периферію мережі (на кордон між OT і IT). Спеціалізовані IoT системи представлені в лінійці HPE Edgeline. Лінійка HPE Edgeline Intelligent Gateway призначена для збору, передачі даних і обробки подій, а лінійка HPE Edgeline Converged IoT System - для рівня первинного аналізу даних і потокової аналітики.

Шлюзи HPE Edgeline Intelligent Gateway є компактною і надійною апаратно-програмною платформою, що дозволяє об'єднати дані з вбудованих контролерів і цифрових датчиків і виконати обчислювальні функції початкового (GL10) і середнього (GL20) рівня для сучасних рішень IoT. Шлюзи призначені для роботи в промислових середовищах, наприклад на заводах, в розумних містах, на нафтових або газових об'єктах. Замовники можуть аналізувати потоки даних в реальному часі і приймати продумані рішення на основі достовірної інформації. Шлюзи відрізняються підвищеною міцністю і можливістю роботи в діапазоні температур від -20 ° C до + 60 ° C.

Конфігурація HPE GL10 IoT включає процесор lntel Atom, 4 Гбайт ОЗУ, твердотільний накопичувач 32 Гбайт, а HPE GL20 IoT - процесор lntel i5, 8 Гбайт ОЗУ, твердотільний накопичувач 64 Гбайт. Операційні системи - Microsoft Windows IoT Core, Microsoft Windows Server, Canonical Ubuntu Snappy Core, CentOS.

Обидва шлюзи мають широкий набір модулів вводу-виводу, в тому числі чотири порти живлення по мережі Ethernet (PoE) і модуль ЦАП/АЦП. Кілька слотів для плат mini-PCIe дозволяють користувачам самостійно підключати різні пристрої і забезпечують можливість розширення ресурсів відповідно до майбутніх потреб. Шлюзи GL10/GL20 мають можливість комунікацій по Wi-Fi, через мобільні стільникові мережі, мають по 2 порти Gigabit Ethernet.

Пристрої HPE Edgeline Converged IoT System представляються компанією HPE як перші в галузі конвергентні системи для промислового Інтернету речей. Системи Edgeline EL1000 і EL4000 можна представити як шлюзи 2-го рівня, які об'єднують дані з HPE Edgeline Intelligent Gateway.

Системи HPE Edgeline оптимізовані для високопродуктивного аналізу, інтерпретації, візуалізації даних і надання інформації в режимі реального часу на периферійних ділянках мережі. Вони об'єднують обчислювальні ресурси, сховища, засоби захоплення і контролю даних, операційне середовище рівня підприємства і надають розробникам платформу для доступу до структурованої і неструктурованої інформації, а також забезпечують автоматизацію роботи з цими даними.

Іншою важливою особливістю HPE Edgeline є унікальна інтеграція збору точних даних з вимірювальних систем і їх управління, заснована на базі відкритих PXI стандартів. Коли вони доповнюються автоматичним машинним навчанням, це відкриває нові можливості в моніторингу і управлінні, прогностичній аналітиці для виявлення можливих поломок, а також доповнену реальність для мінімального ручного обслуговування. HPE Edgeline приносить всі можливості управління віддаленими системами, які надає Integrated Lights Out (iLO).

HPE Edgeline повністю сумісні з такими популярними IoT системами безпеки як Aruba ClearPass для автоматизації автентифікації, запобігання загрозам злому і функцій відновлення систем в умовах підвищеного ризику поза ЦОДами. Aruba Virtual Intranet Access (VIA) дозволяє організувати безшовні Virtual Private Network (VPN) тунелі для безпечних з'єднань між вузлами на кордоні IT-мереж і корпоративною мережею.

Ці міцні і компактні системи працюють в розширеному діапазоні робочих температур від 0 ° C до + 55 ° C і здатні справлятися з підвищеним ударним та вібраційним навантаженням.

Важливою особливістю HPE Edgeline є безпрецедентні обчислювальні можливості. У EL1000 можна встановити один обчислювальний модуль (до 16 ядер Xeon D або Xeon E3) з двома відсіками для дисків SATA SFF, двома портами Gigabit Ethernet або 10 Gigabit Ethernet. Широкі можливості підключення периферійних пристроїв забезпечуються за допомогою двох слотів PCIe або PXI/PXIe разом з бездротовими модулями Wi-Fi або 3G. У EL4000 можна розмістити 4 обчислювальних модуля, кожен з яких може отримати свій модуль розширення PCIe або PXIe і два 10G Ethernet порти для прямого підключення до мережі.

Модель Edgeline 4000 також надає можливість організувати відмовостійку розподілену систему зберігання даних, а також працювати з аналітичною платформою на базі SQL HPE Vertica для отримання, обробки і завантаження готових даних від мільйонів «розумних лічильників» в секунду, з затримками в наносекунди [30].

4.8 Висновки

Були виділенні основні критерії, що необхідно розглядати при виборі IoT шлюзів. Основники характеристиками, на які необхідно спиратись є:

- Підтримка перефирійних/туманних обчислень.
- Підтримуванні технології обміну даними
- Функції маршрутизатора.
- Функції управління кінцевими пристроями мережею і додатками
- Функції безпеки пристроїв, мережі і додатків

Якщо декілька шлюзів задовольняють умовам описаним вище, то необхідно дивитись на такі характеристики, як: обчислювальна потужність, форм-фактор та умови, в яких шлюз можна використовувати.

Як можна побачити, лідери ринку IoT Intel, Hewlett Packard, Cisco, Dell Technologies, а також компанії, які на цьому ринку недавно Huawei, NEXCOM, Monnit, Davra Networks та ін., підтримують весь спектр перерахованих функцій. Всі з розглянутих виробників пропонують як універсальні шлюзи для використання у різних галузях промисловості, так і рішення для окремих вертикалей ринку. Лінійки шлюзів, що пропонуються, включають як малопотужні енергоефективні моделі для легких економних проектів, наприклад, NEXCOM, молодші моделі Dell та Intel, так і промислові моделі, спрямовані на аналітику та зберігання великих об'ємів даних, самим яскравим представником яких є конвергентні системи Hewlett Packard. Серйозні постачальники наділяють свої шлюзи ПЗ для інтеграції у власні (Eurotech, Davra Networks) або сторонні хмарні платформи, наділяють шлюзи власними платформами і ПЗ для захисту та управління пристроями і мережею (Hewlett Packard, Cisco, Dell, Huawei) або підтримують рішення від сторонніх компаній. Деякі виробники (Hewlett Packard, Cisco, Huawei) пропонують власні рішенні для аналітики, обробки, зберігання і візуалізації великих обсягів даних, інші – забезпечують програмно-апаратні платформи для сторонніх рішень, що вже зарекомендували себе на ринку IoT.

Слід також зауважити, що на ринку IoT присутня велика кількість менш відомих виробників і щороку з'являються нові. Тому, гадаємо, що запропоновані критерії класифікації і порівняння допоможуть вибрати шлюзи необхідної функціональності і технічних характеристик за пропозиціями різних постачальників.

5 ПРИКЛАД ПРАКТИЧНОЇ РЕАЛІЗАІЇ

Хорошим прикладом використання шлюзу для Інтернету речей може послужити шлюз, що керує розумним будинком, адже це та сфера, яку на собі може відчути кожна людина. Шлюзи від лідерів ринку, що були описані у попередній главі загалом являються промисловими, тому вони мають можливості, що не потрібні звичайним користувачам-мешканцям будинку. Наявність додаткової функціональності та відповідність сертифікатам збільшує собівартість шлюзу. Для локальної реалізації шлюзу для розумного будинку краще зібрати його самому з менш дорогих компонентів. Дана схема реалізації розумного будинку більше підійде для невеликих компаній для подальшого продажу, проте її можна реалізувати самому, якщо мати достатньо вільного часу та відповідні кваліфікаційні навички.

Перш за все необхідно побудувати модель архітектури, яку можна використовувати як прототип для створення власного рішення. Для розумного будинку доцільно спиратися на модель Всесвітнього форуму IoT. Також слід при реалізації шлюзу передбачити можливість роботи без з’єднання з Інтернетом, для покращення автономності системи. У цій моделі шлюз займається організацією зв’язку із датчиками, трансформуванням даних між стеками протоколів, аналізом даних, що йдуть від датчиків, та управляє ними.

Шлюз повинен відповідати критеріям, що були виділені раніше, а саме:

- Підтримувати крайові обчислення.
- Підтримувати необхідні технології обміну даними
- Мати функції маршрутизатора.
- Мати функції управління кінцевими пристроями, мережею і додатками
- Мати функції безпеки пристроїв, мережі і додатків.

В якості основної плати для шлюзу можна використати Pine A64-LTS (рис. 5.1) із 2 ГБ оперативної пам’яті та 64-бітним процесором ARM Cortex-A53 із чотирма ядрами по 1.152 ГГц, так як для забезпечення крайових обчислень необхідне продуктивне апаратне забезпечення, проте розумний дім не потребує

тисячі датчиків, тому необхідність у більш потужних процесорах таких як Intel Core або Xeon відпадає. Ще одним вагомим аргументом для вибору цієї плати є її низька ціна, відтак при ціні рівній ціні Raspberry Pi, вона має вдвічі більше оперативної пам’яті і такий самий процесор. Для збереження даних використовується SD-карта.

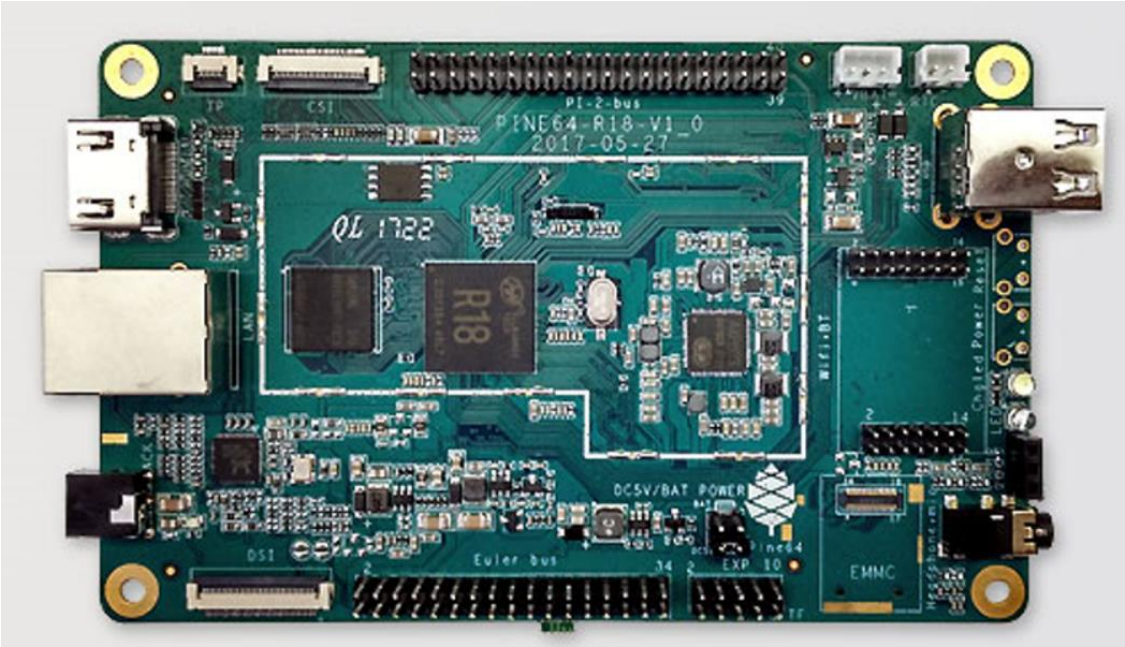

Рисунок 5.1 – Плата Pine A64-LTS

Для забезпечення зручності підключення датчиків краще використовувати безпровідні технології тому, що підключення усіх датчиків за допомогою дротів потребує проведення додаткових комунікацій. Серед безпровідних технологій, що є зручними для розумного будинку можна виділити Bluetooth, Wi-Fi або RF.

Bluetooth гарантує зв’язок на відстані не більше 10-15 метрів на відкритому просторі, а із стінами ще менше. Тому ця технологія не підходить. Wi-Fi краще працює крізь стіни, проте його дальності все ще може бути недостатньо, а датчики можуть стояти у місцях, де люди майже не знаходяться, тому й покриття Wi-Fi в тій точці не гарантується. Крім того Wi-Fi споживає набагато більше енергії (в 40 разів більше), а це зменшить час автономної роботи датчика приблизно у стільки ж разів. Найкращим вибором слугуватиме зв’язок за допомогою модулів, що працюють у радіодіапазоні. Для обраної плати існує модуль, що підтримує зв’язок на частотах 300-930 МГц - CC1310F128RSMT. Максимальна швидкість передачі

даних сягає 50 кб/сек, що є цілком достатнім для прийому даних від датчиків. Енергоспоживання під час відправки даних всього лиш в 3 рази більше ніж у Bluetooth, при цьому радіо частотний діапазон гарантує передачу даних на сотні метрів і в два рази рази меншу відстань при наявності стін.

Цей модуль використовує радіохвилі і GFSK (Gaussian Frequency-Shift Keying, модуляція з частотним зміщенням) – схема частотної модуляції, в якій цифрова інформація передається через дискретні зміни частоти. Ця модуляція фільтрує дані, щоб зробити плавні переходи. Перевагою є зниження потужності побічної смуги та перешкод із сусідніми каналами. За допомогою цієї методики модуляції можна створити свій власний приймач і передавач, зосереджуючись на потребах, таких як швидкість передавання даних або відстань. У разі, коли інформаційний символ приймає два значення, модуляція називається двійковою. Двійкова GFSK використовується в пристроях з технологій DECT, Bluetooth та ін.

Датчики, що працюють на цьому радіочастотному діапазоні можна зробити самому на базі мікроконтролера STM32 та модуля радіозв'язку для відповідного діапазону. Даний контролер є дешевим і має контакти, за допомогою яких до нього можна підключити різні сенсори, такі як: сенсор температури або вологості, сенсор тиску, сенсор угарного газу, сенсор контакту (для перевірки закритості вікон) та ін.

Для забезпечення функцій маршрутизації, управління кінцевими пристроями та безпеки на шлюз потрібно встановити ОС. Найкращим вибором буде безкоштовна Linux система Ubuntu. Для з'єднання із мережею Інтернет можна використати Ethernet порт, або під’єднати модуль сотового зв’язку через USB порт.

Для реалізації роботи з датчиками необхідно створити програмне забезпечення, що буде займатись обміном та аналізом даних. Приймаючи дані від датчиків програмне забезпечення може порівнювати їх із певними критичними значеннями (для температури, вологості, концентрації угарного газу) або із станом, який повинен спостерігатися на даний момент (для датчиків контакту). При невідповідності виставленим умовам, інформацію можна зберегти в постійній пам’яті та організувати певні дії керування і повідомлення. Для полегшення процедури підключення нових датчиків, ПЗ для шлюзу та датчиків краще одразу

розробити з урахуванням автоматичного підключення.

Для покращення роботи із користувачем на шлюзі можна розгорнути веб-сервер, а за рахунок використання системи Ubuntu, легко налаштувати фаєрвол, для більшої безпеки. За рахунок паралельного підключення і до домашнього роутера і до сотової мережі, користувач буде мати веб доступ із локальної мережі та із Інтернету. Найлегшим варіантом реалізації веб-серверу є використання мови програмування Go. Вона була розроблена спеціально для роботи із веб-додатками і надає змогу розробити повноцінний веб-сервер без використання сторонніх бібліотек. На веб сторінці можна відображати останні події, або показники датчиків, що вийшли за допустимі границі значень та їх поточний стан. Також за допомогою веб додатку можна вимикати та вмикати необхідні датчики.

Результуюча схема роботи розумного будинку виглядає наступним чином (рис. 5.2):

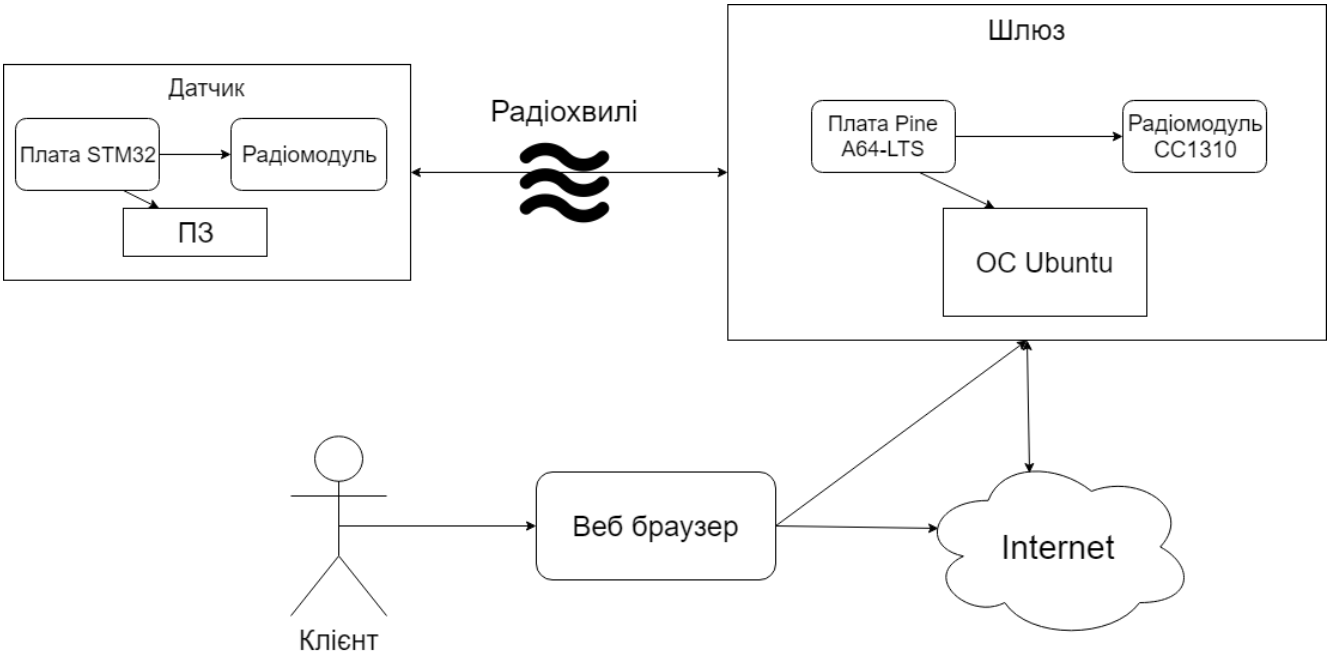

Рисунок 5.2 – Структура розумного будинку

В центрі реалізації лежить саморобний шлюз, що відповідає всім критеріям, виділеним у даній роботі. Основною конкурентною перевагою даного шлюзу є його ціна, адже за рахунок використання більш дешевих компонентів вдалося

значно знизити її. Також перевагою є можливість легкого підключення, яка була закладена на етапі розробки програмного забезпечення для роботи шлюзу та датчиків. Важливо відмітити, що дана реалізація є завершеною в тому сенсі, що функціонувати без хмарного серверу.

6 РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ «ІОТ ШЛЮЗ»

Метою даного розділу є проведення аналізу стартап-проекту для визначення можливості його ринкового просування та доцільності реалізації.

6.1 Опис ідеї проекту

У даному розділі описано економічне обґрунтування стартап-проекту на тему «IoT шлюз». Даний стартап-проект розрахований на полегшення створення розумного будинку людьми, що не мають спеціальних навичок та не володіють значними коштами для купівлі шлюзів від великих виробників. Основні ідеї проекту описані в табл. 6.1.

Таблиця 6.1 - Опис ідеї стартап-проекту

Зміст ідеї	*Напрямки застосування*	*Вигоди для користувача*
	1. Для людей, що проживають у квартирах	З'являється можливість контролювати показники температур у різних кімнатах та автоматично вмикати кондиціонер. Також можна контролювати чи відкриті вікна та двері
	2. Для людей, що проживають у власних будинках	З'являється додаткова можливість контролювати параметри подвір'я. Можливе автоматичне включення поливу рослин та ін.

Отже при використанні системи розумного будинку заснованій на IoT шлюзі можна полегшити контроль за станом будинку/квартири та прибудинкової території. Це полегшить життя людей у цих приміщення та зробить життя безпечнішим завдяки контролю стану вікон та дверей. Автоматичний полив значно полегшить догляд за садом.

Таблиця 6.2 - Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№ п/п	*Техніко-економічні характеристики ідеї*	*(Потенційні) товари/концепції конкурентів*				*W (слабка сторона)*	*N (нейтральна сторона)*	*S (сильна сторона)*
		Мій проект	*Конкурент1*	*Конкурент2*	*Конкурент3*			
1.	Робота з пристроями різних виробників	Можлива	Неможлива	Неможлива	Можлива			+
2.	Собівартість	Низька	Висока	Середня	Середня			+
3.	Необхідність Інтернету для прийняття рішень	Не треба	Необхідний	Не треба	Необхідний			+
4.	Можливість оновлення	Наявна (ручна)	Наявна (ручна/автоматична)	Наявна (ручна/автоматична)	Наявна (автоматична)		+	
5.	Наявність готової платформи	Ні	Так	Так	Так	+		

Основними позитивними характеристиками товару є його низька ціна, можливість працювати із пристроями різних виробників та можливість прийняття рішень у режимі реального часу без зв’язку із сервером. Негативною рисою є відсутність готової Інтернет платформи. Отже проект може конкурувати із існуючими рішеннями.

6.2 Технологічний аудит проекту

Необхідно визначити наскільки реально створити проект та обрати технології

за допомогою яких він буде реалізовуватись. Для шлюзу IoT необхідно врахувати як апаратурну, так і програмну реалізацію. Результати аудиту показані у таблиці 6.3.

Таблиця 6.3 - Технологічна здійсненність ідеї проекту

№ п/п	*Ідея проекту*	*Технології її реалізації*	*Наявність технології*	*Доступність технології*
1.	Створення апаратної частини	Raspberry pi	Наявна	Доступна, наявна велика кількість бібліотек
		Arduino	Наявна	Доступна, наявні бібліотеки
2.	Створення програмної частини	C++	Наявна	Доступна, безкоштовна, легка у реалізації
		C	Наявна	Доступна, безкоштовна, Середня важкість реалізації

Виходячи з аналізу можна сказати, що усі вибрані технології реалізації як апаратної, так програмної частини є доступними. Проте для створення апаратної частини краще обрати Raspberry pi, адже для нього створено більше готових бібліотек, що облегшить створення програмної частини. Для реалізації програмної частини краще підійде мова програмування C++, оскільки вона є більш високорівневою, що також полегшить реалізацію.

6.3 Аналіз ринкових можливостей

Для того щоб спланувати напрямки розвитку проекту необхідно визначити ринкові можливості та ринкові загрози. Також необхідно визначити потреби

потенційних клієнтів та пропозицій конкурентів. Попередня характеристика ринку наведена у таблиці 6.4

Таблиця 6.4 - Попередня характеристика потенційного ринку стартап-проекту

№ п/п	*Показники стану ринку (найменування)*	*Характеристика*
1.	Кількість головних гравців, од	3
2.	Загальний обсяг продаж, грн/ум.од	10000 грн./ум.од
3.	Динаміка ринку (якісна оцінка)	Зростає
4.	Наявність обмежень для входу (вказати характер обмежень)	Немає
5.	Специфічні вимоги до стандартизації та сертифікацій	Немає
6.	Середня норма рентабельності в галузі (або по ринку), %	R = (3000000 * 100) / (1000000 * 12) = 25%

Було проаналізовано обсяг ринку та динаміку його розвитку, а також наявність попиту. За результатами аналізу можна сказати, що обмежень для входу на ринок немає, динаміка ринку зростає, ринок є рентабельним.

Для визначення ключових елементів реалізації проекту, необхідно чітко визначити цільову аудиторію, особливості поведінки цільових груп та вимоги, що користувачі висувають до продукту. У таблиці 6.5 наведена характеристика потенційних клієнтів.

Таблиця 6.5 - Характеристика потенційних клієнтів стартап-проекту

№ п/п	*Потреба, що формує ринок*	*Цільова аудиторія (цільові сегменти ринку)*	*Відмінності у поведінці різних потенційних цільових груп клієнтів*	*Вимоги споживачів до товару*
1.	Система контролю та автоматизації будинку	Будь-які люди, що проживають у квартирах та власних будинках	Цільова група – це мешканці власних будинків та квартир, перші мають додаткову необхідність у можливості контролю не тільки внутрішньобудинкових параметрів, а також і факторів зовнішнього середовища	Рішення має буди простим, надійним та інтуїтивно зрозумілим

Виходячи з проведеного аналізу можна сказати, що для охоплення всіх потенційних споживачів, необхідно одразу підтримувати датчики і пристрої, що можуть працювати у жорстких умовах зовнішнього середовища. Також одним з головних критеріїв має бути простота експлуатації шлюзу.

Для вдалого майбутнього проекту необхідно врахувати ситуації, що можуть виникнути в майбутньому та бути готовими до активних дій у разі їх появи. Аналіз загроз наведений у таблиці 6.6.

Таблиця 6.6 - Фактори загроз

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
1.	Конкуренція	Випуск великою компанією пристроїв бюджетного сегменту	вихід з ринку; запропонувати великій компанії поглинути себе; передбачити додаткові переваги власного сервісу для того, щоб повідомити про них саме після виходу міжнародної компанії на ринок Розроблення гибкої архітектури програмного забезпечення для легшого впровадження нового функціоналу, що допоможе виграти конкурентну боротьбу
2.	Зміна потреб користувачів	Користувачам необхідний сервіс з більшим/новим функціоналом	Розроблення гибкої архітектури програмного забезпечення для легшого впровадження нового функціоналу. Апаратне забезпечення також моє бути легко модифікованим
3.	Економічні чинники	Зменшення купівельної здатності цільової аудиторії, зростання цін на апаратні частини проекту	Спроба перейти на більш дешеві пристрої
4.	Політичні чинники	Заборона на ввезення запчастин у країну, де виробляється апаратна частина проекту	Спроба перенести виробництво у країну, куди можна ввозити запчастини

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
5.	Соціальні чинники	Зловмисники отримали доступ до баз даних та вкрали особисті дані користувачі	Розміщення баз даних на захищених хмарних середовищах. Посилення безпеки баз даних.

З можливих ризиків найвірогіднішими є вихід конкуренту у бюджетний сегмент ринку та зміна потреб користувачів. Обидва можуть бути ліквідовані описаними вище діями (табл. 6.6). Останні ж 3 ризики є менш вірогідними.

Також необхідно врахувати позитивні фактори, що можуть виникнути. При виникненні таких ситуацій завдяки правильним діям можна значно збільшити кількість клієнтів рішення. Можливі ситуації, що грають на руку проекту, наведені у таблиці 6.7.

Таблиця 6.7 - Фактори можливостей

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
1.	Зростання купувальних можливостей людей	Зростання середнього фінансового стану населення	Запропонувати їм свої послуги
2.	Зниження довіри до конкурента	У конкурента вкрали інформацію із сховища	Проведення маркетингової компанії, що вказує на надійність рішення
3.	Поява нових бібліотек	З’явилися нові бібліотеки, що покращують процес розробки та оптимізують рішення	Використання нової бібліотеки для розробки програмного рішення. Проведення маркетингової компанії, що вказує на підтримку інновацій рішенням
4.	Поява нових датчиків	З’явилися нові типи датчиків або на ринок датчиків вийшла нова компанія	Реалізувати підтримку нових датчиків. Проведення маркетингової компанії, що вказує на підтримку нових

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
			виробників або нових типів датчиків
5.	Побудова нових житлових комплексів	Будуються нові житлові приміщення	Проведення маркетингової компанії серед майбутніх власників житла

Основною дією для збільшення аудиторії, що користується нашим рішенням є проведення правильної маркетингової компанії окремо або у зв'язці із правильною реалізацією рішення у певній ситуації. Відтак можлива потреба у дороблені програмного забезпечення для використання останніх технологій або для успішної взаємодії із новими датчиками.

Для збільшення шансів виграти конкуренцію, необхідно провести ступеневий аналіз ринку. Це допоможе обрати стратегію поведінки на ринку та дозволить врахувати ключові особливості ринку. Результати аналізу зображено у таблиці 6.8.

Таблиця 6.8 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	*В чому проявляється дана характеристика*	*Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)*
1. Вказати тип конкуренції: - досконала	Існує 3 фірми-конкуренти на ринку	Необхідно врахувати можливості, що надають інші компанії, їх доцільність та вартість їх рішення. Проведення маркетингової компанії, метою якої є відображення переваг над конкурентами
2. За рівнем конкурентної боротьби: - міжнародний	Компанії із різних країн	Додавання локалізації у інтерфейс. Додати можливість дзеркального відображення інтерфейсу

Особливості конкурентного середовища	*В чому проявляється дана характеристика*	*Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)*
		для арабських та інших країн.
3. За галузевою ознакою: - внутрішньогалузева	Конкуренти мають апаратно-програмне рішення, що може використовуватись лише всередині галузі	Закласти у рішення можливість доробки для використання у інших галузях
4. Конкуренція за видами товарів: - товарно-видова	Види товарів є однаковими, апаратно-програмна реалізація	Створити рішення враховуючи недоліки конкурентів та напрямок розвитку галузі
5. За характером конкурентних переваг: - нецінова	Оптимізація процесів розробки та використання оптимальних апаратних рішень	Використання широко розповсюджених бібліотек для полегшення розробки. Вибір апаратного забезпечення, що має широке поширення та достатню кількість бібліотек для створення програмного забезпечення, що буде на ньому функціонувати.
6. За інтенсивністю: - немарочна	Бренди є, проте їх роль не відіграє особливого значення	Зосередитись на розробці продукту, а не на рекламі бренду

Проаналізувавши конкурентів та види конкурентної боротьби на ринку можна зробити висновок, що найважливішим фактором є сучасність рішення, його швидка доробка та зосередження уваги аудиторії на перевагах реалізації над виробами конкурентів. Також треба надати уваги створенню інтерфейсу різними мовами.

Необхідно виділити сильні позиції стартап-проекту у кожному з факторів: існуючі конкуренти, потенційні конкуренти, товари-замінники, постачальники,

споживачі. Це допоможе оцінити привабливість реалізації. Результати аналізу наведені у таблиці 6.9.

Таблиця 6.9 - Аналіз конкуренції в галузі за М. Портером

Складові аналізу	*Прямі конкуренти в галузі*	*Потенційні конкуренти*	*Постачальники*	*Клієнти*	*Товари-замінники*
	Навести перелік прямих конкурентів	*Визначити бар'єри входження в ринок*	*Визначити фактори сили постачальників*	*Визначити фактори сили споживачів*	*Фактори загроз з боку замінників*
Висновки	Існує 3 конкуренти на ринку. Найбільш схожим за виконанням є конкурент 2, так як його рішення також може працювати без підключення до мережі Інтернет та його собівартість не набагато більша.	Так, можливості для входу на ринок є, бо наше рішення використовує відкриті для доступу апаратні та програмні засоби та не потребує великих капіталовкладень.	Постачальники відсутні	Низька ціна товару допомагає охопити більший ринок споживачів. А зосередження на якості роботи основних функцій надає перевагу у продуктивності системи.	Товари-замінники можуть використати більш дешеві технології створення апаратно-програмної реалізації та зменшити собівартість товару. Проте це може вплинути на якість та ефективність роботи пристрою

Виходячи з аналізу можна сказати, що у проекту є можливості для входу на ринок. На ринку існують три конкуренти, найбільш схожою є реалізація конкуренту 2. Ринок відкритий і постачальники не диктують правил, бо відсутні. Основні вимоги користувачів покриваються даною реалізацією, тому можна сказати, що проекту є шанси витримати конкуренцію.

На основі аналізу конкуренції на ринку, вимог, що ставляться користувачами перед продуктом, та основними характеристиками ідеї проекту можна визначити та обґрунтувати основні фактори конкурентоспроможності рішення (представленні у таблиці 6.10).

Таблиця 6.10 - Обґрунтування факторів конкурентоспроможності

№ п/п	*Фактор конкурентоспроможності*	*Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)*
1.	Низька ціна рішення	Дозволяє охопити аудиторію, що не може собі дозволити рішення конкурента.
2.	Використання відкритих бібліотек	Дозволяє знизити ціну розробки та підтримувати рішення актуальним, адже бібліотеки постійно доповнюються та оновлюються завдяки спеціалістам, що з ними працюють.
3.	Підтримка датчиків від різних виробників	Дозволяє споживачу використовувати датчики від виробника, котрого вони оберуть. Надає гнучкості рішенню, та не нав’язує споживачу постачальників датчиків.
4.	Наявність готової платформи	Дозволяє споживачу використовувати додатковий функціонал від використання пристрою

Можна сказати, що у стартап-проекту є достатньо факторів конкурентоспроможності, що надають йому переваги у боротьбі за споживачів. Також важливо відмітити, що низька ціна та відкритість у роботі із різними датчиками є ключовими побажаннями майбутніх користувачів, адже це надає більше свободи у виборі.

Надалі необхідно оцінити наскільки фактори конкурентоспроможності (табл. 6.10) та провести аналіз сильних та слабких сторін проекту. Основними сильними сторонами можна назвати низьку ціну та підтримку датчиків різних виробників, адже реалізація конкурентів зроблена для роботи в інфраструктурі одного

постачальника датчиків (табл. 6.11).

Таблиця 6.11 - Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	*Фактор конкурентоспроможності*	*Бали 1-20*	*Рейтинг товарів-конкурентів у порівнянні з нашим підприємством*						
			-3	*-2*	*-1*	*0*	*+1*	*+2*	*+3*
1.	Низька ціна рішення	20	+						
2.	Використання відкритих бібліотек	12			+				
3.	Підтримка датчиків від різних виробників	15		+					
4.	Наявність готової платформи	2							+

Із результатів можна зробити висновок, що рішення має як і значні переваги, такі як низька ціна та підтримка датчиків від різних виробників, так і свої недоліки, що проявляються у відсутності готової платформи. Проте фінальний продукт має бути конкурентоспроможним.

На основі проведеного раніше аналізу можна зробити аналіз факторів загроз, що можуть бути створенні як конкурентом, так і самим ринком, і аналіз факторів можливостей, що можуть виникнути у результаті помилок конкурентів, або в результаті змін складу цільової аудиторії (табл. 6.12).

Таблиця 6.12 - SWOT-аналіз стартап-проекту

Сильні сторони: робота з пристроями різних виробників, низька собівартість, використання відкритих бібліотек	**Слабкі сторони:** відсутність готової платформи
Можливості: розширення аудиторії споживачів за рахунок збільшення платіжної спроможності населення, розширення підтримуваних датчиків, втрати довіри до конкурента через ненадійність	**Загрози:** конкуренція, зміна потреб користувачів, зміна цін внаслідок економічно-політичний чинників, несанкціонований доступ до баз даних зловмисниками

На основі SWOT-аналізу розробляються альтернативи ринкової поведінки (перелік заходів) для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок. Визначені альтернативи аналізуються з точки зору строків та імовірності отримання ресурсів.

Таблиця 6.13 - Альтернативи ринкового впровадження стартап-проекту

№ п/п	*Альтернатива (орієнтовний комплекс заходів) ринкової поведінки*	*Ймовірність отримання ресурсів*	*Строки реалізації*
1.	Використання REST API для взаємодії пристроїв із шлюзом	60%	4 місяців
2.	Використання gRPC та protobuf для взаємодії пристроїв із шлюзом	30%	3 місяців

Отже можна зробити висновки: з означених альтернатив обирається та, для якої: а) отримання ресурсів є більш простим та імовірним; б) строки реалізації – більш стислими. Оскільки у альтернативи 1 в два рази більша вірогідність отримати кошти, а строки реалізації відрізняються всього на 25%, то буде логічним вибрати альтернативу 1.

6.4 Розробка ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів.

Таблиця 6.14 - Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1.	Власники квартир	Можливість збільшити безпеку та рівень контролю за внутрішніми приміщення-ми	Середній		Низька ціна, простий інтерфейс
2.	Власники будинків	Можливість збільшити безпеку та рівень контролю як за внутрішніми приміщення-ми так і за всією ділянкою	Середній		Низька ціна, простий інтерфейс
3.	Власники підприємств	Можливість збільшити контроль за виробництвом	Високий		Стійкість до жорстких умов зовнішнього середовища
Які цільові групи обрано: обираємо квартир та будинків					

Виходячи із необхідностей різних цільових аудиторій, можна сказати, що характеристики фінальної реалізації найкраще підходять для власників будинків та квартир, бо мають низьку ціну. Для підприємств, що висувають вимоги до витримки доволі екстремальних зовнішніх чинників (висока вологість та температура, постійні вібрації), результат стартап-проекту не підходить.

Проілюструвати базову стратегію розвитку можна у вигляді таблиці 6.15

Таблиця 6.15 - Визначення базової стратегії розвитку

№ п/п	*Обрана альтернатива розвитку проекту*	*Стратегія охоплення ринку*	*Ключові конкурентоспроможні позиції відповідно до обраної альтернативи*	*Базова стратегія розвитку*
1.	Використання REST API для взаємодії пристроїв із шлюзом	Ринкове позиціонування	Простота у користуванні, надійність технологій	Диференціація та спеціалізація

Було обрано наступний варіант розвитку проекту: використання REST API для взаємодії пристроїв із шлюзом, адже використовуючи ці технології можна досягти конкурентоспроможних позицій на ринку.

У таблиці 6.16 наведено базову стратегію конкурентної поведінки

Таблиця 6.16 - Визначення базової стратегії конкурентної поведінки

№ п/п	*Чи є проект «першопроходьцем» на ринку?*	*Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?*	*Чи буде компанія копіювати основні характеристики товару конкурента, і які?*	*Стратегія конкурентної поведінки*
1.	Ні	Компанія буде шукати нових споживачів у власниках новобудівель та намагатися відбити споживачів у конкурентів зосереджуючи увагу на їх недоліках	Буде копіювати та удосконалювати	Зайняття конкурентної ніші

Продукт не є першопроходьцем, адже конкуренти уже існують на ринку, і рішення буде частково скопійованим у них, проте буде мати свої особливості. Проте оскільки ринок розвиваючийся, то кількість нових клієнтів, що лише шукають рішення для себе досить велика, тому компанія буде шукати як нових клієнтів, так і відбивати клієнтів конкурента. Через це найкращим варіантом конкурентної поведінки буде зайняття конкурентної ніші, адже ця ніше задовольняє таким умовам: є досить прибутковою і реалізація намагається зайняти малу нішу не підприємницького сегменту.

Визначимо стратегію позиціонування у таблиці 6.17, що полягає у формуванні ринкової позиції (комплексу асоціації), за яким споживачі мають ідентифікувати торгівельну марку/проект.

Таблиця 6.17 - Визначення стратегії позиціонування

№ п/п	*Вимоги до товару цільової аудиторії*	*Базова стратегі я розвитку*	*Ключові конкурентоспром ожні позиції власного стартап-проекту*	*Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)*
1.	Низька ціна, простий інтерфейс	Диференціаці я та спеціалізація	Спеціалізація на потребах власників будинків та квартир, низька ціна, простий інтерфейс	Дешевизна, простота, ефективність

Вимоги цільової аудиторії співпадають із основними конкурентними якостями проекту. Стратегі розвитку полягає у спеціалізації на потребах власників будівель та квартир та удосконалені реалізації функцій, які вони потребують, що і буде основною відмінністю від конкурентів.

6.5 Розробка маркетингової програми

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього у табл. 6.18 потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару.

Таблиця 6.18 - Визначення ключових переваг концепції потенційного товару

№ п/п	*Потреба*	*Вигода, яку пропонує товар*	*Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)*
1.	Низька ціна	Товар має найнижчу вартість на ринку	Нижча ціна
2.	Простота користувацького інтерфейсу	Простота роботи шлюзу	Користувачі мають інтерфейс, що більш зручний для використання у квартирі або будинку

Реалізація задовольняє основні потреби аудиторій, тим саме отримуючи конкурентну перевагу. Зв’язок реалізований за допомогою RESTfull API допоможе стандартизувати методи доступу до інформації та полегшить розробку, завдяки використанню широкорозповсюдженної технології.

Далі у таблиці 6.19 проілюстрована трирівнева маркетингова модель товару: уточняється ідея продукту та/або послуги, його фізичні складові, особливості процесу його надання.

Таблиця 6.19 - Опис трьох рівнів моделі товару

Рівні товару	*Сутність та складові*		
I. Товар за задумом	Апаратно-програмна реалізація, що допомагає слідкувати за будинком та автоматизувати процеси		
	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	Низька ціна Простота роботи	1. М 2. Нм	1. Економічна 2. Технологічна
	Якість: згідно до стандарту ISO 4444 буде проведено тестування		

	Маркування відсутнє
	Моя компанія: “PizTech”
	Знижки при закупівлі товару для певних об’єднань мешканців
	Постійна підтримка для користувачів
За рахунок чого потенційний товар буде захищено від копіювання: ліцензія	

Було розглянуто три рівні моделі товару, з чого можна зробити висновок, що властивості є як економічні та матеріальні, так і технологічні і нематеріальні. Також було надано сутність та складові товару у задумці та товару з підкріпленням. Після формування маркетингової моделі товару слід особливо відмітити – чим саме проект буде захищено від копіювання. У даному випадку найбільш вірогідним гарантом буде ліцензія.

Наступним кроком є визначення цінових меж, якими необхідно керуватись при встановленні ціни на потенційний товар (остаточне визначення ціни відбувається під час фінансово-економічного аналізу проекту), яке передбачає аналіз ціни на товари-аналоги або товари субститути, а також аналіз рівня доходів цільової групи споживачів (табл. 6.20). Аналіз проводиться експертним методом.

Таблиця 6.20 - Визначення меж встановлення ціни

№ п/п	*Рівень цін на товари-замінники*	*Рівень цін на товари-аналоги*	*Рівень доходів цільової групи споживачів*	*Верхня та нижня межі встановлення ціни на товар/послугу*
1.	14000 грн	15000 грн	>300000 грн/рік	7500-12000 грн

Далі необхідно визначити основні системи збуту, в межах яких приймається рішення (табл. 6.21).

Таблиця 6.21 - Формування системи збуту

№ п/п	*Специфіка закупівельної поведінки цільових клієнтів*	*Функції збуту, які має виконувати постачальник товару*	*Глибина каналу збуту*	*Оптимальна система збуту*
1.	Купують одноразово готове рішення	Продаж	0(напряму), 1(через одного посередника)	Власна та через посередників

Система буде приносити прибуток за рахунок постійного притоку клієнтів.

Останньою складовою маркетингової програми є розроблення концепції маркетингових комунікацій, що спирається на попередньо обрану основу для позиціонування, визначену специфіку поведінки клієнтів (табл. 6.22).

Таблиця 6.22 - Концепція маркетингових комунікацій

№ п/п	*Специфіка поведінки цільових клієнтів*	*Канали комунікацій, якими користуються цільові клієнти*	*Ключові позиції, обрані для позиціонування*	*Завдання рекламного повідомлення*	*Концепція рекламного звернення*
1.	Використання у власних будинках та квартирах, внаслідок купівлі через мережу Інтернет або у офісі компанії	Інтернет	Низька ціна, простота використання, універсальність	Показати переваги рішення над конкурентами, виділити ключові особливості	Розповсюдження у мережі Інтернет відеороликів.

Було визначено, що придбання продукту буде проводитись через мережу Інтернет або при безпосередньому спілкуванні із представниками компанії.

Розповсюдження інформації про продукт буде проводитись виключно через Інтернет, адже аудиторія даного продукту активно користується всесвітньою мережею.

6.6 Висновки

Провівши дослідження можна сказати, що проект можна комерціалізувати. Проект моє перспективи на ринку, бо бар'єрів майже не існує, ринок хаотично розвиваючийся і не має монополістів та правил, що диктуються постачальниками. Також дана реалізація має значні переваги порівняно із конкурентами, хоча наявні і недоліки. Для успішного виконання проекту найкращим вибором є реалізація апаратної частини на Rastberry Pi із програмним забезпеченням написаним на мові програмування C++. Для успішного виходу на ринок та зайняття на ньому впевнених позицій, продукт повинен мати наступні характеристики:

- Мати низьку собівартість і як наслідок фінальну вартість
- Мати можливість працювати із датчиками різних виробників
- Бути самостійним і незалежним від підключення до глобальної мережі Інтернет

Було проведено аналіз потенційних ризиків і можливостей, а також розраховані основні фінансово-економічні показники проекту. Отримані результати кажуть про те, що реалізація проекту є доцільною.

Було визначено сильні сторони проекту: наявність RESTfull API, що дає змогу універсального спілкування між шлюзом і датчиками; використання оптимальних апаратних технологій для реалізації саме у будинках та квартирах. Серед слабких сторін проекту можна виділити відсутність хмарної платформи.

Можливості для створення конкурентногоспроможного продукту включають зниження цін на апаратні запчастини та появу нових бібліотек, що спростять створення та підтримку програмного рішення. Серед загроз особливо важливими є різка зміна направленості ринку та поява нових лінійок конкурентів, що займають цільову бюджетну нішу. Менш небезпечними є політичні та

економічні чинники, що можуть призвести до збільшення собівартості виготовлення апаратної частини продукту.

ВИСНОВКИ

Інтернетом речей називається набір безлічі датчиків та хмарних чи туманних ресурсів. Датчики та пристрої можуть обмінюватись даними між собою та відправляти свої дані на обробку на більш потужні пристрої для обробки.

Завдяки своїй універсальності можливе використання IoT майже у будь-якій сфері: IT і мережі, безпека та охорона, роздрібна торгівля, транспорт, промисловість, охорона здоров'я та науки про життя, споживчий сектор та розумний будинок, виробництво енергії. При аналізи ринку було виявлено недоліки, котрі має хмарна структура при великій кількості датчиків, такі як: необхідність підтримки IP стеку технологій речами, великі вимоги до пропускної здатності каналів зв'язку, відсутність прийняття рішень у режимі реального часу, тільки в режимі транзакції.

Для підвищення ефективності використання мережі Інтернет з'являється необхідність у проміжній ланці, що буде агрегувати, перетворювати пакети у стандартні TCP/IP пакети, та реагувати на події у режимі реального часу, а не у часі транзакції, при безпосередньому підключенні до хмари. Цю ланку займає шлюз Інтернету речей.

Було проаналізовано основні моделі архітектури IoT рішень. Серед них можна виділити: модель IoT від MCE-T, модель Всесвітнього форуму IoT, модель Національного інституту стандартів і технології Міністерства торгівлі США, модель консорціум промислового інтернету. Всі з перечислених організацій віддають шлюзу функцію створення локальних мереж для підключення неінтелектуальних "речей" і узгодження протоколів при взаємодії між OT та IT. Мережа може мати як стандартний TCP/IP стек протоколів, так і бути не IP мережею та підключати датчики за допомогою таких технологій як Bluetooth, ZigBee або 6LoWPAN та ін. Також всі вони визначають функції безпеки і управління, проте вони можуть відрізнятися, відтак у моделі ITU ці функції обмежені лише на рівні пристрою, а у інших моделях вони забезпечуються ще й на рівні мережі. Всі організації окрім ITU до функцій шлюзу відносять ще й

функції аналітики даних від речей. У IWF шлюз класифікують, як мережевий пристрій, проте в архітектурі на суміжному рівні виділяються функції перефирійних/туманних обчислень. Cisco, котрий бере активну участь у IWF, явно позиціонує свої шлюзи, як пристрої, що проводять аналітику даних та реагують на події. IIC для шлюзів виділяє функції аналітики краю, що по факту є додаванням рівню туманних обчислень (з моделі IWF) до можливостей шлюзу. В моделі національного інституту стандартів шлюз одразу називається агрегатором і являється частиною апаратного забезпечення, що займається дослідженням даних від датчиків. Він являється певним сервером, що знаходиться у безпосередній близькості до речей. Відтак шлюз перестає бути лише конвертором з одних протоколів у інші, він набуває здібностей аналізувати дані, оброблювати їх і зберігати/надсилати у більш стислій формі. Можливе реагування на показники певних датчиків або певні події у режимі реального часу, а не у часі транзакції, як при безпосередньому підключені речей до хмари.

Було розглянута необхідність IoT платформ у проектуванні рішень і можна сказати, що IoT платформи об’єднують речі та Інтернет. Слід виділили вісім компонентів повноцінної IoT-платформи: зв'язок і нормалізація, управління пристроями, база даних, обробка та управління діями, аналітика, візуалізація, додаткові інструменти, зовнішні інтерфейси. Були розглянуті як відкриті вільні платформи, так і комерційні проекти. Роль шлюзів варіюється від звичайних маршрутизаторів для перепакування даних для роботи в мережі Інтернет до міні серверів, що знаходяться на межі між речами та Інтернетом і виконують функції агрегування та аналізу, реагують на певні події незалежно від хмари, тобто займаються туманними обчисленнями.

Були виділенні основні критерії, що необхідно розглядати при виборі IoT шлюзів. Основники характеристиками, на які необхідно спиратись є:

- Підтримка перефирійних/туманних обчислень.
- Підтримуванні технології обміну даними
- Функції маршрутизатора.
- Функції управління кінцевими пристроями, мережею і додатками

- Функції безпеки пристроїв, мережі і додатків

Якщо декілька шлюзів задовольняють умовам описаним вище, то необхідно дивитись на такі характеристики, як: обчислювальна потужність, форм-фактор та умови, в яких шлюз можна використовувати.

Усі лідери ринку та декілька маловідомих компанії, що були розглянуті у даній роботі підтримують основні вимоги, що ставляться до IoT шлюзу. Серйозні постачальники наділяють свої шлюзи ПЗ для інтеграції у власні (Eurotech, Davra Networks) або сторонні хмарні платформи, наділяють шлюзи власними платформами і ПЗ для захисту та управління пристроями і мережею (Hewlett Packard, Cisco, Dell, Huawei) або підтримують рішення від сторонніх компаній. Деякі виробники (Hewlett Packard, Cisco, Huawei) пропонують власні рішенні для аналітики, обробки, зберігання і візуалізації великих обсягів даних, інші – забезпечують програмно-апаратні платформи для сторонніх рішень, що вже зарекомендували себе на ринку IoT.

Слід також зауважити, що на ринку IoT присутня велика кількість менш відомих виробників і щороку з’являються нові. Тому можна сказати, що запропоновані критерії класифікації і порівняння допоможуть вибрати шлюзи необхідної функціональності і технічних характеристик за пропозиціями різних постачальників.

Виходячи з аналізу архітектур та рішень IoT шлюзів, було розроблено практичну реалізацію розумного будинку. За базову архітектуру було обрано модель Всесвітнього форуму IoT тому, що вона передбачає виконання крайових обчислень. Розроблений шлюз відповідає всім критеріям, що були виділені у ході даної роботи. Таке рішення є конкурентоспроможним за рахунок дешевизни та можливості легкого підключення нових датчиків.

ПЕРЕЛІК ПОСИЛАНЬ

1. Lake, D., Rayes, A., and Morrow, M., “The Internet of Things,” The Internet Protocol Journal, Volume 15, No. 3, September 2012.
2. Cisco Systems, “Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion,” White Paper, 2013. http://www.cisco.com/web/about/ac79/docs/innov/IoT_ Economy_Insights.pdf
3. McKinsey Global Institute, “The Internet of Things: Mapping the Value Beyond the Hype,” June 2015. http://www.mckinsey.com/insights/ business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world
4. ITU-T, “Overview of the Internet of Things,” Recommendation Y.2060, June 2012.
5. McEwen, A., and Cassimally, H., Designing the Internet of Things, ISBN-13: 978-1118430620, Wiley, 2013.
6. Sutaria, R., and Raghunath, G., “Making sense of interoperability: Protocols and Standardization initiatives in IoT,” International Conference on Recent Trends in Communication and Computer Networks – ComNet 2013, 2013.
7. Ferguson, J., and Redish, A., “Wireless Communication with Implanted Medical Devices Using the Conductive Properties of the Body,” Expert Review of Medical Devices, Volume 6, No. 4, 2011, http://www.expert-reviews.com.
8. ITU-T, “Common Requirements and Capabilities of a Gateway for Internet of Things Applications,” Recommendation Y.2067, June 2014.
9. Cisco Systems, “The Internet of Things Reference Model,” White Paper, 2014. http://www.iotwf.com/
10. Frahim, J., et al., “Securing the Internet of Things: A Proposed Framework,” Cisco White Paper, March 2015.
11. Vaquero, L., and Rodero-Merino, L., “Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing,” ACM SIGCOMM Computer Communication Review, October 2014.
12. Wei Q., Zhu S., Du C. Study on key technologies of internet of things perceiving mine // Procedia Eng. 2011. Vol. 26.
13. Domingo M. C. An overview of the internet of things for people with disabilities // J. Netw. Comput. Appl. 2012. Vol. 35, No. 2.
14. Alemdar H., Ersoy C. Wireless sensor networks for healthcare: A survey // Comput. Netw. 2010. Vol. 54, No. 15.
15. Plaza I., Martin L., Martin S., Medrano C. Mobile applications in an aging society: Status and trends // J. Syst. Softw. 2011. Vol. 84, No. 11.
16. Pang Z., Chen Q., Tian J., Zheng L., Dubrova E. Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-

things // Proc. 2013, 15th Int. Conf. Adv. Commun. Technol. (ICACT). Korea, Pyeongchang.
17. Pang Z., Chen Q., Han W., Zheng L. Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion // Inf. Syst. Front. To be published.
18. Zhang Y. C., Yu J. A study on the fire IOT development strategy // Procedia Eng. 2013. Vol. 52.
19. Ji Z., Qi A. The application of internet of things (IOT) in emergency management system in China // Proc. 2010 IEEE Int. Conf. Technol. Homeland Security (HST).
20. ITU : список стран-участниц https://www.itu.int/online/mm/scripts/mm.list?_languageid=1&_from=&_search=ITUstates&regionvarnam=ctry_councilregion&_territories=&_map=n&_sort=1&_f1=CHECKED&_f7=CHECKED&_f8=CHECKED&_f9=CHECKED&_f16=CHECKED&_f20=CHECKED
21. Модель NIST Special Publication 800-183 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
22. Модель Industrial Internet of Things Reference Architecture http://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf
23. 15 найбільш продвинутых виробників одляднання Інтернету речей. Линдзи О'Доннелл. Перевірено 07.05.2018 за посиланням http://www.pcweek.ua/themes/detail.php?ID=155790
24. Хмарні технології в автоматизації.: комплексний підхід від Eurotech. Олексій П'ятницьких. (2016, Жовтень). Control Engineering Росія. Перевірено 04.04.2018 за посиланням http://controleng.ru/wp-content/uploads/CE_IoT_Listalka.pdf
25. Технологія Intel IoT Gateways. (2018). Офіційний сайт компанії Intel. Перевірено 07.05.2018 за посиланням https://software.intel.com/ru-ru/iot/hardware/gateways
26. Huawei AR Series Agile Gateways Brochures. (2017). Офіційний сайт компанії Huawei. Перевірено 07.05.2018 за посиланням http://www.huawei.com/minisite/iot/img/hw_ar_series_agile_gateways_brochure_en.pdf
27. Cisco IoT Networking. (2017). Офіційний сайт компанії Cisco. Перевірено 07.05.2018 за посиланням https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/brochure-c02-734481.pdf
28. IoT Gateway. (2018). Офіційний сайт компанії NEXCOM. Перевірено 07.05.2018 за посиланням http://www.nexcom.com/Products/industrial-computing-solutions/iot-solutions/iot-gateway
29. Dell змінює економіку Інтернету речей з новими компактними шлюзами Edge Gateway. (1 березня 2017). Офіційний сайт компанії Dell. Перевірено

07.05.2018 за посиланням www.dell.com/learn/ua/ru/uacorp1/press-releases/dell-changing-economy-of-iot-with-new-compact-gateways-edge-gateway

30. Короткий огляд апаратних платформ, типових архітектурних рішень і послуг для корпоративних інформаційних систем. (2018, весна). Офіційний сайт компанії Hewlett Packard. Перевірено 07.05.2018 за посиланням https://h20195.www2.hpe.com/v2/GetPDF.aspx/c04771945.pdf
31. The Internet of Things: Mapping the Value Beyond the Hype. (2015, Червень). Офіційний сайт McKinsey Global Institute. Перевірено 30.03.2018 за посиланням http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world
32. Linux Foundation розвиває EdgeX, нову платформу для Інтернету речей. (25 квітня 2017). Перевірено 07.05.2018 за посиланням https://www.opennet.ru/opennews/art.shtml?num=46446