НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	В.о. завідувача кафедри
Інформаційних технологій	Комп'ютерних систем, мереж та кібербезпеки
_____ Глазунова О.Г., д.пед.н, проф.	_____ Касаткін Д.Ю., к.п.н., доц.
підпис ПІБ, вчене звання і ступінь	підпис ПІБ, вчене звання і ступінь
«___»_____2022 р.	«___»_____2022 р.

МАГІСТЕРСЬКА РОБОТА

На тему: «Системи моніторингу та управління елементами IoT»

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерні системи та мережі

Орієнтація освітньої програми _____

Керівник дипломного проекту: _____ / Сагун А. В. /

підпис ПІБ

Виконав: _____ / Ковіня В.В . /

підпис ПІБ

КИЇВ-2022

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
в.о. завідувача кафедри
комп'ютерних систем, мереж та кібербезпеки
_____ / Касаткін Д.Ю., к.п.н., доц. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 20__ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ

Ковіня Владислав Вікторович
(прізвище, ім'я, по батькові)

Спеціальність (~~напрям підготовки~~): комп'ютерна інженерія
Освітня програмая комп'ютерні системи та мережі
Орієнтація освітньої програми

Тема магістерської роботи «Системи моніторингу та управління елементами IoT»

затверджена наказом ректора НУБіП України від "__1__" ____11____ 2021р. № _1859_ «С»
Термін подання завершеної роботи на кафедру
Вихідні дані до магістерської роботи: використання для системи моніторингу
VMWare - vCenter, vSphere Client, VM Encryption, Secure Boot, Integrated Containers

для виявлення збоїв ОС хоста або гостьової ОС Red Hat RHEV

Перелік питань, що підлягають дослідженню:

1. Структура та основні елементи IoT
2. Принципи моніторингу за елементами IoT
3. Система моніторингу та управління елементами IoT

Перелік графічного матеріалу (за потреби) _____

Дата видачі завдання "_____"_____2022 р.

Керівник магістерської роботи _____ Сагун А. В., к.т.н., доц.
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Ковіня В.В.
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі магістерської роботи	18.10.2021	Виконано
2	Аналіз предметної області	12.07.2022	Виконано
3	Проектування системи	23.08.2022	Виконано
4	Реалізація системи	15.10.2022	Виконано
5	Тестування системи	30.10.2022	Виконано
6	Оформлення пояснювальної записки	01.11.2022	Виконано
7	Оформлення графічного матеріалу	01.11.2022	Виконано

Студент _____ **Ковіня В.В**
(підпис) (ініціали та прізвище)

Керівник проекту (роботи) _____ **Сагун А.В.**

ЗМІСТ ВСТУП ..... **Ошибка! Закладка не определена.**
РОЗДІЛ 1 АСПЕКТИ ДОСЛІДЖЕННЯ ЗАСОБІВ МОНІТОРИНГУ ТА 7
УПРАВЛІННЯ ЕЛЕМЕНТАМИ ІОТ 7
1.1 IoT: поняття, сутність, генезис 7
1.2 Структура та основні елементи IoT 12
1.3 Проблематика та постановка завдань дослідження 20
Висновки до розділу 25
РОЗДІЛ 2 МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ЗАСОБІВ 26
МОНІТОРИНГУ ТА УПРАВЛІННЯ ЕЛЕМЕНТАМИ ІОТ 26
2.1 Методологія управління елементами IoT 26
2.2 Принципи моніторингу за елементами IoT 34
2.3 Алгоритм управління елементами IoT 41
Висновки до розділу 49
РОЗДІЛ 3 ПРАКТИЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ЗАСОБІВ МОНІТОРИНГУ
ТА УПРАВЛІННЯ ЕЛЕМЕНТАМИ ІОТ 49
3.1 Архітектура IoT 50
3.2 Система моніторингу та управління елементами IoT 50
3.3 Верифікація результатів дослідження 62
Висновки до розділу 70
ВИСНОВКИ 71
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 72
ДОДАТКИ 77
Додаток А Функціональна схема IoT-рішення 77
Додаток Б Електрична принципова схема IoT-рішення 79

ВСТУП

Актуальність теми. Інтернет речей – це комплексна концепція, що стрімко розвивається, що включає в себе дослідження в галузі інформатики, мережевих технологій, мікроелектроніки і сенсорної техніки. Дана парадигма є основним напрямом розвитку мережевих технологій у майбутньому і дозволить вирішити багато рутинних завдань людства, починаючи від вимірювання екологічних показників і закінчуючи збільшенням ефективності виробництва.

Інтернет речей (Internet of Things, IoT) визначається як концепція, в якій більшість пристроїв, що використовуються людьми, буде забезпечена мікроконтролерами для управління та мережевими інтерфейсами для цифрової передачі даних та спілкування між собою. Група RFID визначає IoT як всесвітню мережу доступних об'єктів, унікальна адресація якої базується на стандартних протоколах зв'язку .

Можна виділити такі сфери використання Інтернету речей: промисловість та виробництво; транспорт та перевезення; контроль технічного стану конструкцій будівель, якості повітря, шумового фону та споживаної енергії; керування відходами; розумні паркування та надання даних про дорожні пробки; розумне вуличне освітлення та використання в побуті.

З технічної точки зору IoT є не новою технологією, а сукупністю вже існуючих засобів, які надають наступні можливості:

- зв'язок та взаємодія – об'єкти можуть створювати з'єднання з інтернет-ресурсами або один з одним і оновлювати свій стан. Першочергове значення мають бездротові технології, такі як GSM і UMTS, Wi-Fi, Bluetooth, ZigBee та інші стандарти бездротової мережі, що розробляються в даний час;

- адресованість – в Інтернеті речей об'єкти розподілені у просторі та повинні мати однозначну адресацію;
- ідентифікація дозволяє однозначно асоціювати дані з конкретним об'єктом та вилучати їх. Стандарти RFID та NFC є прикладами технологій, за допомогою яких можна ідентифікувати навіть пасивні об'єкти, які не мають вбудованих енергетичних ресурсів;
- зондування – IoT пристрої збирають інформацію про навколишнє середовище за допомогою датчиків, обмінюються нею або змінюють свій стан під її впливом;
- вбудована обробка інформації – об'єкти можуть бути оснащені процесором або мікроконтролером для миттєвого аналізу та обробки інформації;
- локалізація – пристрої знають про своє фізичне місцезнаходження, що досягається за рахунок використання GPS або мережі мобільного зв'язку, а також радіомаяків (наприклад, WLAN або RFID рідерів з відомими координатами).

Мета і завдання дослідження. Метою даної роботи виступає дослідження засобів моніторингу та управління елементами Інтернету речей.

Для досягнення поставленої мети у роботі необхідно виконати низку завдань:

- розкрити методологію управління елементами IoT;
- навести принципи моніторингу за елементами IoT;
- розробити алгоритм управління елементами IoT;
- сформувати та описати архітектуру IoT;
- запропонувати систему моніторингу та управління елементами IoT;
- здійснити верифікацію результатів дослідження.

Об'єкт дослідження – інноваційні напрямки технології Інтернет речей.

Предмет дослідження – процес дослідження засобів моніторингу та управління елементами Інтернету речей.

Методи дослідження. Методологічну основу складають наступні методи наукового пізнання: індукція, дедукція, методи термодинаміки, математичної статистики, програмування.

Наукова новизна отриманих результатів.

1) Розроблене комплексне рішення для комплексного моніторингу та управління елементами IoT.

2) Розроблена інформаційно-аналітична модель системи моніторингу та управління елементами IoT.

Практичне значення отриманих результатів.

Розроблена інформаційно-аналітична модель системи моніторингу та управління елементами IoT може бути впроваджена на базі реального підприємства.

Структура роботи. У своєму складі робота має: вступ, три розділи, висновки, перелік використаної літератури, з 30 найменувань. Загальний обсяг роботи становить 76 сторінок.

РОЗДІЛ 1 АСПЕКТИ ДОСЛІДЖЕННЯ ЗАСОБІВ МОНІТОРИНГУ ТА УПРАВЛІННЯ ЕЛЕМЕНТАМИ ІОТ

1.1 IoT: поняття, сутність, генезис

Розвиток мікроелектроніки призвів до мініатюризації та здешевлення електроних компонентів, завдяки чому стало можливим вбудовувати комп'ютерні чіпи в різні речі, а також використовувати безліч мініатюрних датчиків. Комунікаційні компоненти таких пристроїв дозволили об'єднувати їх в одну мережу для обміну даними та командами. Так виникла концепція Інтернету речей.

Кожна річ окремо може запропонувати деяку частку автоматизації: наприклад, лампочка в кімнаті може включатися за датчиком руху – проте в Інтернеті речей предмети об'єднані в таку систему, яка може враховувати більшу кількість факторів одночасно. Наслідком такої конфігурації є широка доступність інформації для аналізу та прийняття рішень. Таким чином, Інтернет речей дозволяє автоматизувати та оптимізувати процеси, до яких він застосовується, що багато в чому знімає навантаження та відповідальність з користувача, що особливо корисно у сферах, що потребують постійного контролю. Найчастіше системи Інтернету речей призначені для надання фонової підтримки або стеження за різними щоденними процесами.

Як модель для опису роботи систем Інтернету речей пропонується обробка потоку даних. Центральною частиною робочого циклу системи є реакція на події, що приходять, проте варто відзначити, що не всі датчики працюють за такою моделлю: іноді контролюючий пристрій отримують спостережувані дані через фіксовані проміжки часу. Таким чином, система поступово пропускає через себе дані, приймаючи рішення про відправлення команд підконтрольним пристроям по необхідності. Крім того, найчастіше окремою вимогою є зберігання одержуваних даних, щоб пізніше використовувати їх для аналізу.

Уникаючи абстракції потоку даних, варто відзначити, що системи Інтернету речей зазвичай працюють у неоднорідному середовищі, де пристрої як складові елементи являють собою мобільні гетерогенні об'єкти, оснащені датчиками та маніпуляторами. Кожен пристрій може відрізнятись від інших за функціоналом та доступними ресурсами, причому роль грає як програмне, так і апаратне забезпечення. Для зв'язку елементів використовується комунікативно-обчислювальна інфраструктура Інтернету. Отже, потрібно забезпечення коректності як обробки даних, і взаємодії між різними частинами аналізованої розподіленої системи.

Враховуючи перелічені особливості, цікавить перевірка правильності функціонування такої комунікативно-обчислювальної системи та її відповідності заданим вимогам. При цьому часто можливо відокремити технічні аспекти реалізації, такі як вибір конкретних пристроїв або протоколів взаємодії, щоб сконцентруватися на забезпеченні коректної поведінки програмної частини. Відзначимо також подібне завдання визначення придатності того чи іншого підходу, що виникає у процесі проведення досліджень у сфері Інтернету речей. Інакше кажучи, потрібно розробити метод, який дозволив би залежно від конкретної ситуації:

1. перевірити систему або її прототип на відповідність заздалегідь визначеним критеріям,
2. дати оцінку якості роботи системи шляхом обчислення заданих показників.

Процес вирішення однієї з обох перерахованих задач для даного програмного продукту або прототипу називатимемо тестуванням.

Враховуючи, що центральне місце в процесі тестування в контексті даної роботи займає обчислення деяких показників для деякої системи, слід визначити, які вимоги пред'являються до подібних продуктів.

Існує безліч варіантів класифікації та систематизації можливих вимог до програмного забезпечення, так само як і показників, за якими визначається відповідність цією вимогою. У стандарті ISO/IEC TR 9126-2:2003 пропонується шість категорій метрик для оцінки поведінки програмних продуктів: функціональність, надійність, зручність використання, ефективність, можливість супроводу та переносимість. Для розрахунку цих показників систему необхідно помістити до умов реального використання [1]. Усі перелічені метрики можуть бути використані для тестування будь-якого програмного забезпечення, однак у конкретній сфері, зокрема у сфері Інтернету речей, деякі категорії більш корисні, ніж інші.

Перевірка програмного забезпечення на функціональність найчастіше займає основне місце у тестуванні. За однією з класифікацій вимоги поділяються на функціональні та не функціональні, тобто всі інші. Фундаментально, під функціональністю розумітимемо відповідність результатів роботи системи очікуванням користувача. До цієї ж категорії відносять показники зовнішньої сумісності та безпеки системи [1]. Таким чином, поняття функціональності саме по собі включає багато з основних критеріїв оцінки системи.

Функціональні вимоги можна назвати найважливішими й у контексті Інтернету речей. Завданням систем Інтернету речей є автоматизація та оптимізація різних процесів, нерідко у сферах з високим ступенем відповідальності, де потрібна точна відповідність розробленим приписам, інакше наслідки можуть бути тяжкими. Тому потрібно забезпечити відсутність помилок у поведінці системи настільки, наскільки це можливо. Стороннє втручання також може бути проблемою: успішна атака, наприклад, на «розумний дім», потенційно може призвести до контролю зловмисником таких важливих для якості життя систем, як опалення або освітлення. Крім того, через системи Інтернету речей нерідко проходять конфіденційні дані, з яких можна робити висновки про користувачів.

Серед не функціональних вимог як особливо важливих можна виділити вимоги до надійності та ефективності. Незважаючи на те, що більшість систем Інтернету речей не вимагають прийняття рішень у жорсткому реальному часі, реакція на події, що відбуваються, має бути своєчасною, а відмова може призвести до катастрофічних наслідків. Для оцінки надійності пропонуються метрики зрілості, стійкості до відмов, здатності до відновлення, а для оцінки ефективності – метрики своєчасності реакції системи та завантаження ресурсів [1]. Додатковою причиною використання вимог ефективності є обмеженість ресурсів більшості пристроїв Інтернету речей.

Інші категорії вимог, такі як зручність використання, можливість супроводу, переносимість, можуть також застосовуватися до систем Інтернету речей, проте їхня автоматизація розрахунку таких показників можлива значно меншою мірою. Наприклад, під зручністю використання розуміється простота розуміння, вивчення та управління роботою системи [2], що важливо і у сфері Інтернету речей, проте для оцінки цих показників необхідне тестування реальними користувачами.

Підсумовуючи, відзначимо, більшість описаних вимог є широкими категоріями, а конкретній системі чи принаймні предметній області необхідно уточнення обраних метрик.

Як було описано раніше, у контексті даної роботи під тестуванням розуміється обчислення деяких показників, на підставі яких оцінюється якість роботи системи, можливо з проміжним кроком у вигляді перевірки відповідності її заздалегідь заданим вимогам. Така задача може виникати як за наявності готового продукту, для якого необхідно забезпечити коректність його поведінки, так і при попередньому дослідженні предметної галузі визначення найбільш перспективних підходів.

Середовище роботи систем Інтернету речей часто таке, що зміни можна простежити лише на великих проміжках часу. Наприклад, для перевірки коректної реакції на сезонні фактори необхідно тестувати систему протягом року або більше, тому що менший час не охопить весь можливий спектр. Водночас деякі події настільки рідкісні, що вони можуть не зустрітися навіть у такому довгому дослідженні. Як приклад можна навести екстремально високі або екстремально низькі температури, які можуть зустрічатися один раз на кілька років.

Іноді можна протестувати готову систему з урахуванням усіх особливостей її фізичної реалізації. З іншого боку, нерідко продукт існує тільки у вигляді прототипу або взагалі не існує, а необхідно протестувати той чи інший теоретично розроблений підхід. Зазначимо, що навіть у разі

існування готової системи може мати сенс відокремлення її апаратної реалізації від програмного забезпечення. Зокрема, можна відтворити деякі задані ситуації, щоб перевірити коректність деяких змін. Крім того, як було зазначено раніше, час дослідження може становити проблему, якщо потрібно відстежити зміни, що відбуваються на великих часових проміжках. У такому разі може мати сене використання технологій, що дозволяють прискорити цей процес.

Незважаючи на ці складності, неможливо недооцінити значущість тестування у сфері Інтернету речей. Високі вимоги до функціональності, надійності, ефективності роблять цю стадію необхідною. З іншого боку, може бути зручним, особливо на початкових етапах розробки, відійти від фізичної реалізації системи та використовувати програмні технології.

У разі використання тих чи інших технологій симуляції, емуляції чи імітації варто звернути увагу на те, що потрібна побудова окремої тестової інфраструктури для вирішення цього завдання. Нерідко потрібна певна адаптація систем, що тестують і тестуються, для їх спільної роботи.

Нарешті, зазначимо, що складність може представляти розробка таких вимог чи критеріїв тестування, які б враховували кілька цілей, що конфліктують між собою. Найчастіше завдання систем Інтернету речей включають кілька приписів, між якими потрібно визначити компроміс, причому на етапі дослідження нерідко саме співвідношення ще не визначено. Таким чином, необхідно забезпечення певної гнучкості системи тестування, щоб було можливо без труднощів переходити між різними показниками якості.

1.2 Структура та основні елементи IoT

Інтернет речей (англ. Internet of Things, IoT) – концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями

для взаємодії один з одним або із зовнішнім середовищем, що розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає із частини дій та операцій необхідність участі людини.

Базові елементи поділяються на кілька типів: сенсори, актуатори та гейти.

Сенсори

Стандартні: різноманітні термометри, мікрофони, камери та десятки інших, менш поширених пристроїв. Деякі з них можна побачити на рисунку 1.1 Sensors Starter Kit для Arduino.

Гейти

Це пристрої, куди зазвичай покладають логіку поверхневого аналізу інформації, що надходить від підключених до них сенсорів. У певних ситуаціях аналіз даних може вимагати малої кількості обчислювальних ресурсів, так що гейти цілком здатні приймати деякі рішення самостійно. Приймаючи такі рішення, вони відправляють певні команди управління на актуатори, які, своєю чергою, виконують свої функції.

Рисунок 1.1 – Sensors Starter Kit для Arduino

Актуатори

Даний тип елементів призначається у тому, щоб впливати на довкілля, чи певний об'єкт у ньому. Що роль можуть виконувати найрізноманітніші пристрої: від сервоприводів та динаміків до замків (звичайно, електронних) з освітлювальними приладами.

Рисунок 1.2 – Актуатори

Якщо ж обробка інформації вимагає великих витрат, або ця інформація підлягає збору, гейти відправляють її на сервери, де з нею проводиться подальша робота. Цілком можливе використання в ролі гейтів мікрокомп'ютерів (вгорі) або мікропроцесорів (внизу) рис. 1.3.

Для того, щоб побудувати моніторингову систему, достатньо буде використання лише сенсорів та деякого сервера, який виступатиме в ролі гейту. Наприклад, завдяки сенсору руху, можна без особливих зусиль організувати облік кількості людей, які проходять через якусь прохідну.

Додавши в раніше сконструйовану модель актуатор в особі динаміка, можна домогтися того, щоб прохід кожного n-го, що проходить, був під звуччий.

Рисунок 1.3 – Гейти

Так, ускладнювати конструкцію подібного осередку можна досить довго. Однак у певний момент неминуче з'явиться потреба у довгостроковому зберіганні зібраної статистики, її аналізі візуалізації тощо. Тут знадобляться вже повноцінні сервери, яким можна буде делегувати ці обов'язки. Такі сервери разом утворюють хмари, до яких і підключаються гейти.

Тепер, коли вже більш-менш ясно які пристрої використовуються для створення інфраструктури, можна подивитися на те, якими засобами ці пристрої взаємодіють один з одним. Як видно на рисунку 1.4, є 2 умовні групи – хмара та периферія.

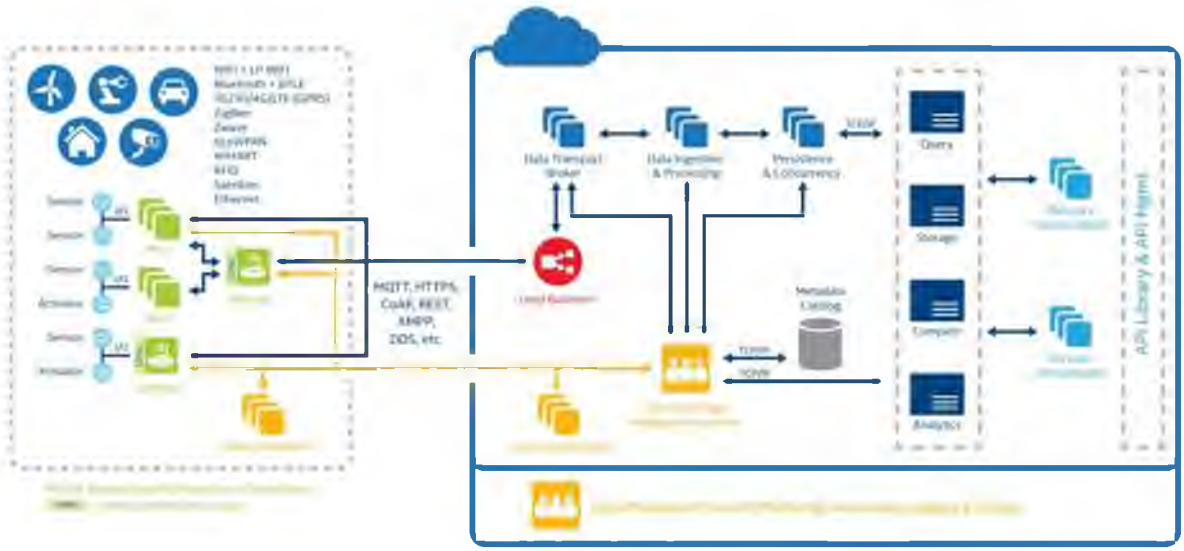


Рисунок 1.4 – Взаємодія елементів Інтернету речей

Комірки, що складаються з перелічених вище типів пристроїв, як можна помітити, знаходяться в периферії і для комунікації використовують спеціальні протоколи взаємодії. Найбільш поширені LoRa та ZigBee. Обидві ці мережі дуже повільні в порівнянні, наприклад, з 4G або навіть з 3G, однак мають і свої переваги.

Одним із головних є їхня енергоефективність. Справа в тому, що ідея інтернету речей полягає у створенні середовища пристроїв, що комунікують між собою без участі людини. Варто зауважити, що в деяких випадках уникнути втручання людини не вдасться. Наприклад, у системі підрахунку кількості минулих людей є сенсор руху. Йому, як і будь-якому іншому електричному пристрої, потрібне живлення. Проводити дроти з живленням до кожного такого сенсора (якщо їх більше 5 і вони сильно розкидані у просторі) здається не найкращою ідеєю. Відповідно, працюватимуть вони від батарейок або акумуляторів. Якщо споживання заряду буде надмірним, елементи живлення їм потрібно буде міняти часто. А це призведе до того, від чого прагне п'ти інтернет речей – змінне електроживлення.

Таблиця 1.1 – Порівняльна характеристика LoRa та ZigBee

Основні порівняльні характеристики	LoRa	ZigBee
Топологія	зірка	прості та mesh
Частотний діапазон (залежить від країни)	2,4 ГГц, 868/915 МГц, 433 МГц, 169 МГц	2,4 ГГц, 915 МГц, 868 МГц
Коди мережі	• базова станція • хост	• роутер • координатор (один із роутерів) • хост

Дальність на відкритому просторі	10 - 15 км	~ 500 м (залежить від потужності передавача)
Швидкість	0.3 - 50 кбіт/с	5 - 250 кбіт/с

Ще однією перевагою цих мереж є висока завадостійкість. Кожен біт інформації у цих мережах відправляється окремим радіосигналом, тому його досить легко виділити. У таблиці 1.1 наведено порівняння LoRa та ZigBee.

А ось між периферією та хмарою, а так само і всередині хмари, використовуються, зазвичай, знайомі та звичні всім wi-fi з ethernet, стільникові та супутникові мережі тощо. На рисунку 1.5 наведено порівняння різних видів мереж на основі швидкості та дальності.

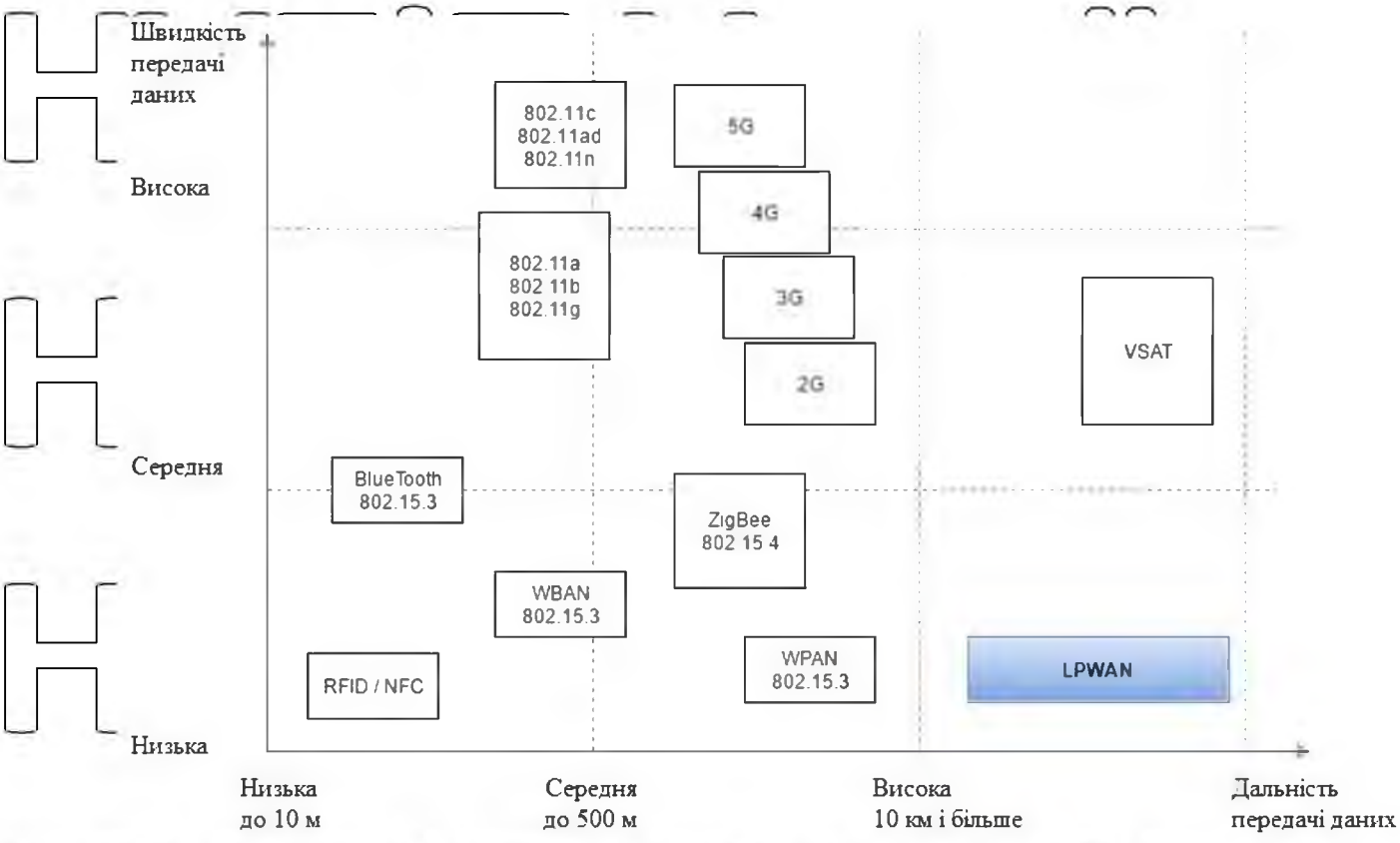


Рисунок 1.5 – Порівняння різних видів мереж на основі швидкості та дальності

Тепер, розглянувши влаштування мереж інтернету речей, можна точно сказати, що в плані апаратної частини немає нічого загадкового і складного. Зробити просту IoT-мережу може будь-який бажаючий, здатний купити досить дешеві на сьогоднішній день компоненти і написати код з кількох рядків. Однак для того, щоб розробити та втілити в життя серйозні проекти, як, наприклад, реалізацію концепції розумного будинку або навіть розумного міста, потрібно докласти величезної кількості зусиль. Адже для того, щоб всі ці пристрої працювали між собою потрібна платформа, здатна контролювати всі процеси, що протікають.

1.3 Проблематика та постановка завдань дослідження

Концепція Інтернету речей є комплексною та має на меті об'єднання таких областей як апаратні засоби, мережі та програмне забезпечення. В результаті виникає велика кількість проблем та завдань, які є як технологічними, так і соціально-правовими.

Основним завданням IoT є розробка та вибір правильної архітектури системи, оскільки від рішень на початкових етапах досліджень залежатиме весь подальший процес розробки. На даний момент не існує конкретної угоди з архітектури IoT, яка була б затверджена та використовувалася повсюдно.

Найбільш поширеними є три та п'ять рівнів моделі архітектур. Перша з них є базовою і включає рівень сприйняття, мережевий та прикладний рівень. Ця модель визначає основну ідею IoT, але вона недостатньо деталізована, що необхідно для більш глибоких досліджень. Тому в літературі пропонуються архітектури з великою кількістю рівнів. Наприклад, п'ятирівнева модель, яка додатково включає рівні обробки і транспортний рівень.

Іншими прикладами є хмарна та туманна архітектури. На думку дослідників, останнім часом з'явилася тенденція розвитку туманних

обчислень, у яких датчики та мережеві шлюзи виконують частину завдань з обробки та аналізу даних.

Туманні та хмарні обчислення найчастіше використовуються спільно, оскільки це необхідно для оптимальної продуктивності IoT додатків. Для реалізації туманних обчислень шлюз може бути вбудований між локальними мережами та «хмарою». Тут застосовується багаторівневий підхід, в якому надаються функції моніторингу (контроль використовуваної потужності та ресурсів), попередньої обробки (фільтрація, обробка та аналіз даних), зберігання (реплікація даних, поширення та зберігання) та забезпечення захищеності даних (шифрування та забезпечення цілісності та конфіденційності даних)). На даний момент ця архітектура становить найбільший інтерес, і, на думку дослідників, є найбільш перспективною.

Важливим завданням IoT є електроживлення пристроїв, які постійно переміщаються і не мають постійного джерела енергії. У багатьох випадках батареї та блоки живлення є проблемними через їх розмір, вагу та вимоги до обслуговування. Надії розробників та дослідників покладаються на майбутнє малопотужних процесорів для вбудованих систем, які можуть споживати значно меншу енергію. Існують бездротові акумуляторні датчики, які можуть передавати свої показання на відстань в кілька метрів. Як і RFID системи, вони отримують енергію або віддалено, або від процесу вимірювання, наприклад, за допомогою п'єзоелектричних або піроелектричних матеріалів. Також для зменшення витрат на живлення необхідно сформувати стек протоколів з найменшим обсягом даних, що передаються.

Звідси випливають завдання розробки та вибору стандарту бездротового зв'язку. З точки зору енергетичних витрат, стандартні технології, такі як GSM, Wi-Fi та Bluetooth, є невідповідними – вони мають широку смугу пропускання і використовують неприпустимий для IoT систем обсяг енергії.

Для вирішення цієї проблеми були розроблені стандарти, що

відповідають вимогам Інтернету речей, наприклад, IEEE 802.15.4, IEEE 802.11 Low Power, Bluetooth Low Energy, 6LoWPAN, RFID, NFC, ZigBee, Sigfox, LoraWAN та інші протоколи для бездротових мереж енергії та сумісні з існуючими протоколами транспортного та мережевого рівнів.

Розробка веб-стека для IoT вимагає грамотної побудови його структури, яка буде відповідати як вимогам комунікаційної інфраструктури (сумісність з існуючими стандартами), так і вимогам Інтернету речей. Прикладами таких стандартів є: на рівні подання – CoAP; транспортний рівень – UDP; мережевий рівень – IPv6/6LoWPAN.

Дані стандарти взаємодіють з комунікаційною інфраструктурою так само, як і протоколи необмеженого стека, проте обсяг даних, що передаються значно менше. Цей факт сприяє зменшенню споживаної IoT пристроями потужності та збільшенню часу їхньої роботи.

Схеми адресації є критичним аспектом щодо унікальності адрес, що присвоюються пристроям IoT, оскільки вони повинні однозначно ідентифікувати інші пристрої і обмінюватися з ними інформацією. Найбільш важливими особливостями створення унікальної адреси є: його однозначність, надійність, стійкість та масштабованість.

Існуючий та повсюдно використовуваний протокол IPv4 дозволяє ідентифікувати лише групу пристроїв, що знаходяться у певній географічній зоні, але не має можливості виділити кожен окремий вузол IoT. Полегшити проблеми ідентифікації пристроїв може протокол IPv6, проте неоднорідність бездротових вузлів, змінні типи даних, одночасні операції та злиття даних з різних пристроїв ще більше ускладнюють проблему.

Наступною проблемою IoT є масштабованість. За оцінками Cisco, у 2022 році до "хмари" буде підключено 50 мільярдів пристроїв, а згідно з оцінками Gartner – 26 мільярдів. IoT має ширший загальний обсяг, ніж звичайний Інтернет. Тому масштабованість простору IoT буде складнішою, ніж у

звичайних веб-додатків. Однак більшість даних, отриманих пристроями IoT, можуть бути оброблені локально і негайно відкинуті.

Веб-користувачі допускають змінну затримку звичайних веб-служб, проте тимчасова недоступність датчиків або виконавчих пристроїв IoT безпосередньо впливатиме на фізичний світ. Необхідний керований, оптимальний підхід до обслуговування різних мережевих трафіків, кожен із яких має власні потреби.

Ще одним аспектом IoT є постійне функціонування мережі для повсюдної та невтомної передачі даних. Хоча стек TCP/IP гарантує це шляхом маршрутизації більш надійним та ефективним способом, від джерела до точки призначення, IoT стикається з вузьким місцем в інтерфейсі між шлюзом та бездротовими сенсорними пристроями. Додавання мереж і пристроїв не повинно знижувати продуктивність мережі, функціонування пристроїв, надійності передачі даних по мережі або ефективного використання пристроїв з інтерфейсу користувача.

На додаток до аспектів безпеки, таких як справжність і надійність каналу зв'язку, і цілісність повідомлень, IoT будуть мати важливе значення та інші вимоги. Потрібно буде надати пристрою вибірковий доступ до кола послуг, або у певний час запобігти спілкуванню з іншими пристроями. Проміжне програмне забезпечення має мати вбудовані механізми для вирішення цього завдання, поряд з автентифікацією користувачів та реалізацією контролю доступу. Багато завдань захисту інформації можуть бути вирішені за допомогою криптографічних методів і вимагають більше досліджень, перш ніж вони можуть бути широко використані.

Міжнародна діяльність в галузі Інтернету речей набирає обертів, і багато ініціатив здійснюються в галузях промисловості, наукових колах та на різних рівнях державного управління. У Європі докладаються значні зусилля щодо об'єднання діяльності дослідницьких груп та організацій, що охоплює M2M, WSN та RFID, у єдину систему IoT для визначення еталонної моделі взаємодії

систем Інтернету речей та ключових складових блоків для досягнення цієї мети. У Японії, Кореї, США та Австралії реалізуються масштабні ініціативи, де промисловість та урядові відомства співпрацюють за різними програмами в галузі IoT. Інтенсивна робота у сфері IoT також ведеться і в Китаї у його 12й п'ятирічці, в якій зазначено, що ресурси та інвестиції мають бути орієнтовані на розробку IoT у різних галузях.

Звідси випливає необхідність створення єдиного для всіх країн союзу щодо вирішення проблем IoT, щоб збільшити темпи розвитку сфери та визначити шлях для скоординованої реалізації цієї технологічної ідеї.

З безперервним розквітом нових технологій IoT концепція Інтернету речей скоро неабиякою розвиватиметься у дуже великих масштабах. Ця нова парадигма мережевої взаємодії впливатиме на кожну частину нашого життя, починаючи від автоматизованих будинків до інтелектуального моніторингу здоров'я та довкілля шляхом впровадження «інтелекту» в об'єкти довкола нас.

Інтернет речей є комплексною сферою, яка потребує розробки стандартів у різних галузях. Внаслідок складності та структурності концепції на шляху її розвитку виникає безліч завдань, пов'язаних із різними областями. Промисловість може отримати вигоду з розвитку Інтернету речей, який тісно пов'язаний із телекомунікаційною, апаратною, програмною та сервісною галузями.

Метою даної роботи виступає дослідження засобів моніторингу та управління елементами Інтернету речей.

Для досягнення поставленої мети у роботі необхідно виконати низку завдань:

- розкрити методологію управління елементами IoT;
- навести принципи моніторингу за елементами IoT;
- розробити алгоритм управління елементами IoT;
- сформувати та описати архітектуру IoT;
- запропонувати систему моніторингу та управління елементами

IoT;

- здійснити верифікацію результатів дослідження.

Висновки до розділу

У межах першого розділу наведено аспекти дослідження засобів моніторингу та управління елементами Інтернету речей, сформовано поняття та сутність IoT, визначено структуру та головні компоненти Інтернету речей, висвітлено проблематику та виконано постановку завдань дослідження.

Середовище роботи систем Інтернету речей часто таке, що зміни можна простежити лише на великих проміжках часу. У разі використання тих чи інших технологій симуляції, емуляції чи імітації варто звернути увагу на те, що потрібна побудова окремої тестової інфраструктури для вирішення цього завдання. Нерідко потрібна певна адаптація систем, що тестують і тестуються, для їх спільної роботи. Інтернет речей (англ. Internet of Things, IoT) – концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або із зовнішнім середовищем, що розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає із частини дій та

операцій необхідність участі людини. Базові елементи поділяються на кілька типів: сенсори, актуатори та гейти. Основним завданням IoT є розробка та вибір правильної архітектури системи, оскільки від рішень на початкових етапах досліджень залежатиме весь подальший процес розробки. На даний момент не існує конкретної угоди з архітектури IoT, яка була б затверджена та використовувалася повсюдно.

РОЗДІЛ 2 МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ЗАСОБІВ МОНІТОРИНГУ ТА УПРАВЛІННЯ ЕЛЕМЕНТАМИ ІОТ

2.1 Методологія управління елементами IoT

Завдання системи управління та моніторингу за елементами IoT полягає у комплексному моніторингу за життєзабезпеченням підприємства чи окремого житлового будинку.

З урахуванням складності IoT має сенс створення архітектури, яка б охоплювала всі специфіковані основні компоненти і здійснювала їх взаємозв'язок. Архітектура IoT може надати такі переваги:

- дати адміністратору 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.

Наведемо огляд моделі на основі даних з IoT.

На відміну від більшості інших моделей і архітектурних моделей, описаних в літературі, модель на основі даних з IoT деталізує фактичні фізичні компоненти екосистеми IoT. Це корисно, тому що висвічує елементи системи IoT, які повинні бути з'єднані, інтегровані, керовані і надані додаткам.

Детальна специфікація системи описує вимоги до можливостей IoT.

Один з важливих аспектів, який загострює модель, – той факт, що IoT на ділі не є мережею фізичних речей. Це скоріше мережа пристроїв, що взаємодіє з фізичними речами, разом з прикладними платформами – такими як комп'ютери, планшети і смартфони, – які взаємодіють з цими пристроями.

Управління окремими елементами та всією системою загалом здійснюється за допомогою хмари.

«Хмара» – це система, що складається з декількох пристроїв, комп'ютерів і серверів, з'єднаних між собою через Інтернет. Така система обчислення може бути образно розділена на дві частини:

- зовнішній інтерфейс – пристрої клієнта (комп'ютери, планшети, мобільні телефони);
- внутрішній інтерфейс – зберігання даних і обробні системи, які можуть бути віддалені від пристроїв клієнта і самої хмари.

Ці дві частини системи безпосередньо взаємодіють один з одним за допомогою бездротових з'єднань.

Технологія хмарних обчислень надає різні види послуг, які діляться на три групи:

- послуги інфраструктури (IaaS) – віддалений центр обробки даних з такими ресурсами як: місткість зберігання даних, обчислювальна потужність, і мережі;
- платформа як послуга (PaaS) – розвиток платформи з пристроями і компонентами для створення, тестування і запуску додатків;

- послуги програмного забезпечення (SaaS) – готове програмне забезпечення, відповідне виробничими потребами.

Доступність – це головна перевага. Крім того, немає необхідності підтримувати місцеві послуги та переживати через час простою.

Інтеграція інтернету речей з хмарою – це вигідне рішення в бізнесі. Віддалені сервери забезпечують необхідну місткість і гнучкість для управління та аналізу зібраних даних з підключених пристроїв, в той час як спеціалізовані платформи, такі як Asure IoT, Suite, IBM Watson, AWS, Google Cloud для IoT, дають розробникам створювати якісні програми без величезних вкладень в програмне забезпечення і ОЗУ.

Так як підключення пристрою обмежує місткість і обчислювальну потужність, інтеграція з хмарними обчисленнями допоможе забезпечити:

- поліпшення роботи (швидкий зв'язок між датчиками інтернету речей і системами обробки даних);
- місткість (добре масштабується і необмежене місце для зберігання в змозі об'єднати, з'єднати і розподілити величезний обсяг даних);
- можлива обробка (віддалені центри обробки даних забезпечують необмежені віртуальні можливості обробки на вимогу);
- зменшення витрат (ліцензійні збори нижче, ніж вартість обладнання на початковому рівні, і його безперервне обслуговування).

Недоліки використання хмарних обчислень:

- високий час очікування (додатки інтернету речей все більше вимагають, щоб час очікування був якомога нижче, але хмара не може цього гарантувати через відстані між пристроями клієнта і центрами обробки даних);
- час простою (технічні проблеми і збої в мережах можуть статися з будь-якої причини в будь-якій системі, що використовує Інтернет, і

дані клієнта можуть постраждати при відключенні електрики; щоб уникнути проблем, багато компаній використовують кілька каналів зв'язку з автоматизованою відмовостійкістю;

- безпека і особиста інформація (особиста інформація передана через глобально пов'язані канали разом з тисячею гігабайтів інформації інших користувачів, не дивно, що система стає вразливою для втрати даних або кібератак; проблема може бути частково вирішена за допомогою гібридної хмари або створення особистого хмарного сховища).

Термін туманні обчислення (або затуманення) був придуманий CISCO в 2014 році, тому він є новим для більшості людей. Туманні і хмарні обчислення взаємопов'язані між собою. У природі туман ближче до землі, ніж хмари, в світі технологій відбувається те ж саме, туманні обчислення ближче до кінцевого користувача, передаючи можливості хмарних обчислень кінцевому користувачеві.

Ухвала може звучати так: туманне обчислення - це розширення хмарних обчислень, що складається з декількох граничних вузлів, безпосередньо підключених до фізичних пристроїв.

Такі вузли фізично набагато ближче до пристроїв в порівнянні з централізованими центрами обробки даних, тому вони здатні забезпечувати миттєві з'єднання. Значна обчислювальна потужність периферійних вузлів дозволяє їм самостійно виконувати обчислення великого обсягу даних, не відправляючи їх на віддалений сервер.

Туманні обчислення також включають хмарні обчислення – невеликі і досить потужні центри обробки даних, розташовані на граничному сегменті мережі. Їх метою є підтримка ресурсоємних додатків інтернету речей, які вимагають низького часу затримки.

Основна відмінність між туманними і хмарними обчисленнями полягає в тому, що хмара являє собою централізовану систему, а туман являє собою розподілену децентралізовану інфраструктуру.

Туманні обчислення є посередником між обладнанням і віддаленими серверами. Туманні обчислення визначають, яка інформація буде відправлена на сервер, і яку інформацію можна буде редагувати локально. Таким чином, туман – це інтелектуальний шлюз, який розвантажує хмару, забезпечуючи більш ефективну, обробку та аналіз даних.

Слід зазначити, що туманна мережа не є окремою архітектурою і не замінює хмарні обчислення, а скоріше доповнює їх, максимально наближаючись до джерела інформації.

Нова технологія, можливо, надасть найбільший вплив на інтернет речей, вбудовані рішення штучного інтелекту і 5G, оскільки вони, як ніколи раніше, вимагають швидкої і безперебійної роботи.

Переваги туманних обчислень:

- низький час відгуку (туман географічно ближче до користувачів і здатний забезпечити миттєвий відгук);
- немає проблем з пропускною спроможністю (частина інформації агрегується в різних точках, а не відправляється в один центр по одному каналу);
- неможливість втрати з'єднання (через безліч з'єднаних каналів);
- високий рівень безпеки (так як дані обробляються величезною кількістю вузлів в складній розподіленій системі);
- покращений інтерфейс користувача (миттєвий відгук і відсутність простоїв радують користувачів);
- енергетична ефективність (периферійні вузли використовують в роботі високоефективні протоколи, такі як Bluetooth, Zigbee або Zхвиля).

Недоліки туманних обчислень:

- система туманних обчислень більш складна (туман – додатковий шар в системі обробки і зберігання даних);
- додаткові витрати (компанії повинні купувати периферійні пристрої-роутери, маршрутизатори, шлюзи);
- обмежений масштаб (на відміну від хмари).

Концепції туманних і хмарних обчислень дуже схожі. Але все ж між ними є різниця по деяким параметрам. Розглянемо точкове порівняння туманних і хмарних обчислень:

У хмарних обчисленнях обробка даних відбувається у віддалених центрах обробки даних. Обробка і зберігання туманних обчислень здійснюється на граничному сегменті мережі, ближького до джерела інформації, що має вирішальне значення для контролю в режимі реального часу.

Хмара є більш функціональною, ніж туман щодо обчислювальних ресурсів і можливостей зберігання.

В туманних обчисленнях виконується короткостроковий аналіз на граничному сегменті мережі через миттєвий відгук, в той час як в хмарних обчисленнях буде довгостроковий глибокий аналіз через більш повільний відгук.

При туманних обчисленнях час затримки – низький, при хмарних обчисленнях – високий.

Хмарна система може зруйнуватися при збоях мережі Інтернет. Туманні обчислення використовують різні протоколи і стандарти, тому ризик збою набагато нижче.

Туман є більш безпечною системою, ніж хмара з-за його розподіленої архітектури.

Нові вимоги до сучасних технологій є рушійною силою розвитку інформаційних технологій. Інтернет речей – це постійно зростаюча індустрія,

яка вимагає більш ефективних способів управління передачею інформації і обробкою даних.

Туманні обчислення є одним з рішень в роботі з пристроями інтернету речей, так як вони можуть задовольнити потреби постійно зростаючого числа підключених пристроїв. Вони використовують локальні, а не видалені комп'ютерні ресурси, що робить продуктивність більш ефективною і потужною, і зменшуються проблеми з пропускною спроможністю.

Компанії повинні порівнювати хмарні і туманні обчислення, щоб використовувати по максимуму доступні можливості, і використовувати високий потенціал.

Розглянемо метод розподіленої обробки даних для Інтернету Речей який використовує хмарні обчислення і безліч сенсорів для даних. Зокрема, спосіб реалізації розподіленого виконання алгоритмів обробки даних.

Всі пристрої IoT, використані в проекті, мають відносно середні характеристики і недорогі в ціні.

В останні роки, мережі і сенсорні технології стали швидко розвиватися, і сприймають все більше даних [4]. Подальші дослідження розширюють можливості машинного навчання, включаючи глибоку взаємодію безпосередньо з Інтернетом Речей.

Рівні інтеграції системи на основі даних з IoT представлено на рис. 2.1.

Рисунок 2.1 – Рівні інтеграції системи управління на основі даних з IoT

У багатьох традиційних вбудованих пристроях програмне забезпечення реалізовано на одному апаратному засобі і одна задача запускається на незалежному пристрої (рис. 2.2, а).

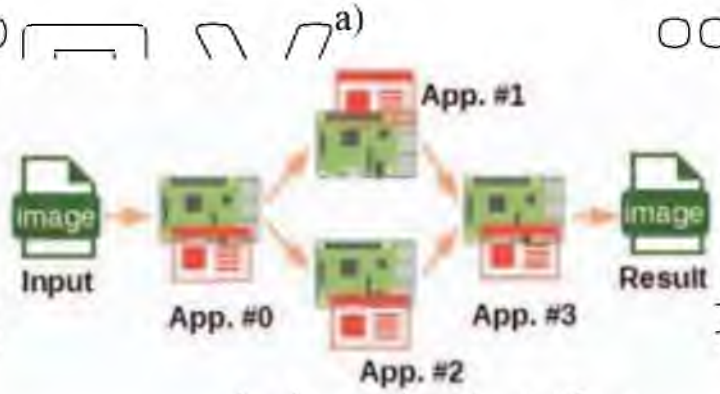
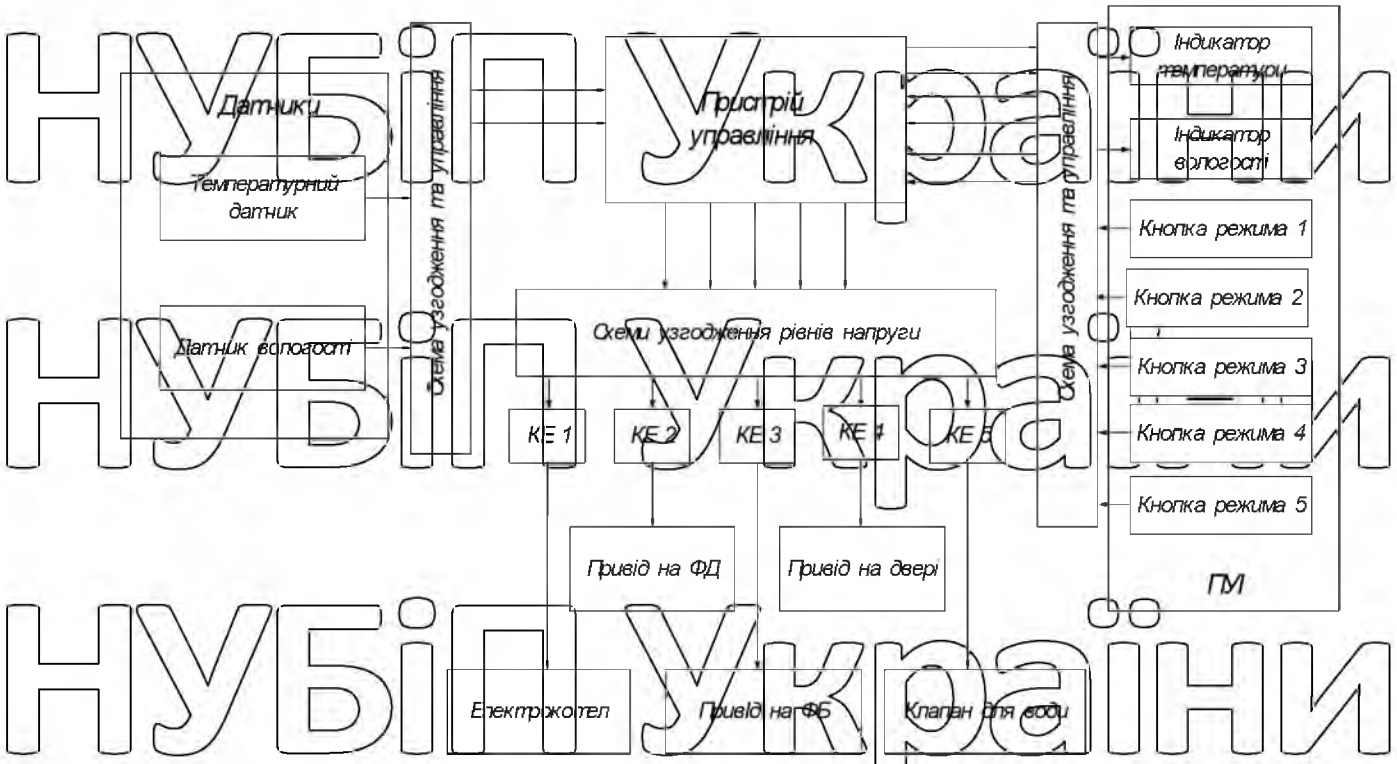


Рисунок 2.2 – Одно ланкова (а) та багатоланкова (б) структура засобів

Відповідно до еволюції технології LSI, недавно випущені пристрої Інтернет Речей є багатофункціональними, виконуючи функції отримання і передачі даних. Проте, через обмежене енергоспоживання і низьку вартість, можливості по обробці даних на IoT-пристроях складають від ¼ до 1/100 від можливостей сучасних комп'ютерів. Паралельні обчислювальні системи, що використовують залізо з низькими характеристиками, можуть використовувати методу високошвидкісної передачі даних, проте необхідна програмна модель такого алгоритму, яка має на увазі роздільну програмну розробку для кожного пристрою (рис. 2.2, б). У більшості випадків програми для паралельної системи обробки складні. Крім того, через довгий період розробки, налагодження і високі витрати, реалізація паралельної системи обробки даних була утруднена.

2.2 Принципи моніторингу за елементами IoT

Структурна схема моделі на основі даних з IoT представлена на рис. 2.3.



КЕ – ключовий елемент; ФБ – фрамуга бокова; ФД – фрамуга в даху; ПУІ – пульт управління та індикації

Рисунок 2.3 – Структурна схема моделі на основі даних з IoT

Схема взаємодії всіх складових моделі на основі даних з IoT наведена на рис. 2.4.

Інтерфейс моделі на основі даних з IoT наведено на рис. 2.5

Рисунок 2.4 – Схема взаємодії всіх складових моделі на основі даних з IoT

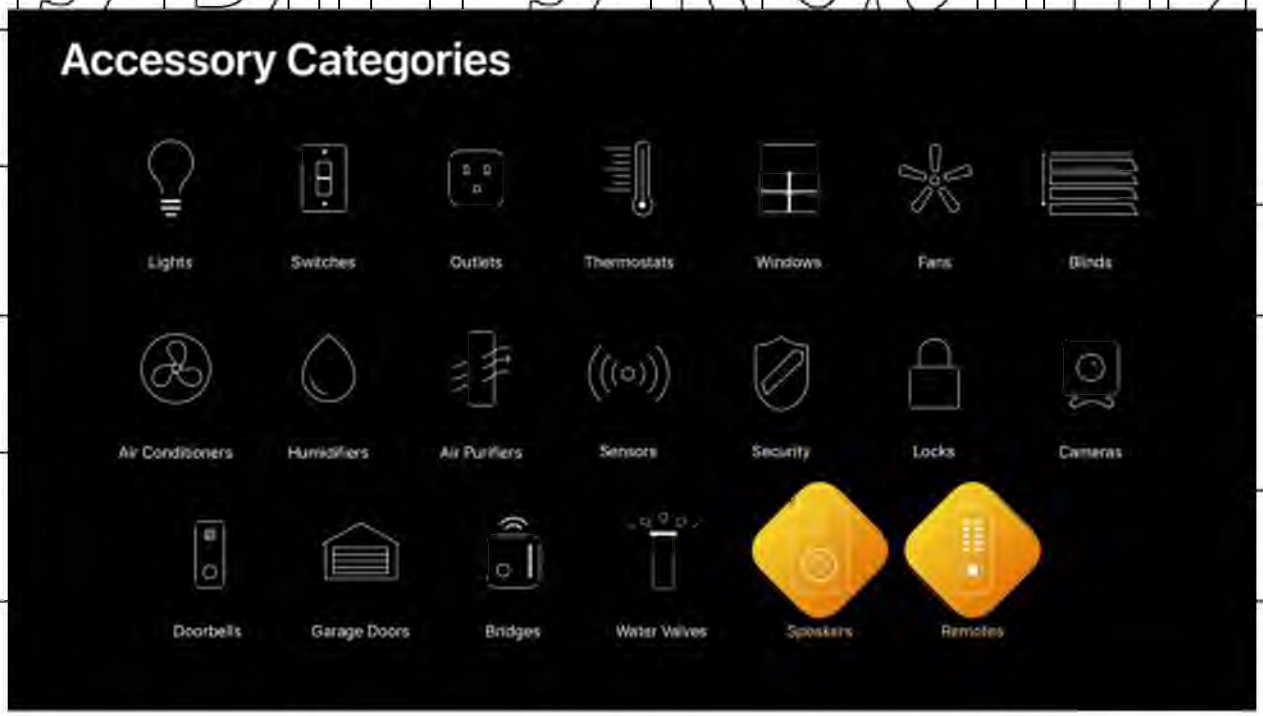


Рисунок 2.5 – Інтерфейс моделі на основі даних з IoT

Налаштування моделі на основі даних з IoT

```
[self.homeManager addHomeWithName:@"My Home" completionHandler:^(HMHome *home, NSError *error) {
    if (error != nil) {
        // Failed to add a home
    } else {
        // Successfully added a home
    }
}];
```

```
NSString *roomName = @"Living Room";
[home addRoomWithName:roomName completionHandler:^(HMRoom *room, NSError *error) {
    if (error != nil) {
        // Failed to add a room to a home
    } else {
        // Successfully added a room to a home
    }
}];
```

Протокол управління моделі на основі даних з IoT, додаги властивості браузера до інтерфейсу класу.

```
@interface EditHomeViewController () <HMAccessoryBrowserDelegate>

@property HMAccessoryBrowser *accessoryBrowser;

@end
```

Здійснити налаштування моделі на основі даних з IoT.

```
self.accessoryBrowser = [[HMAccessoryBrowser alloc] init];
self.accessoryBrowser.delegate = self;
```

знайти аксесуари управління моделі на основі даних з IoT.

```
[self.accessoryBrowser startSearchingForNewAccessories];
```

Сформувати колекцію управління моделі на основі даних з IoT.

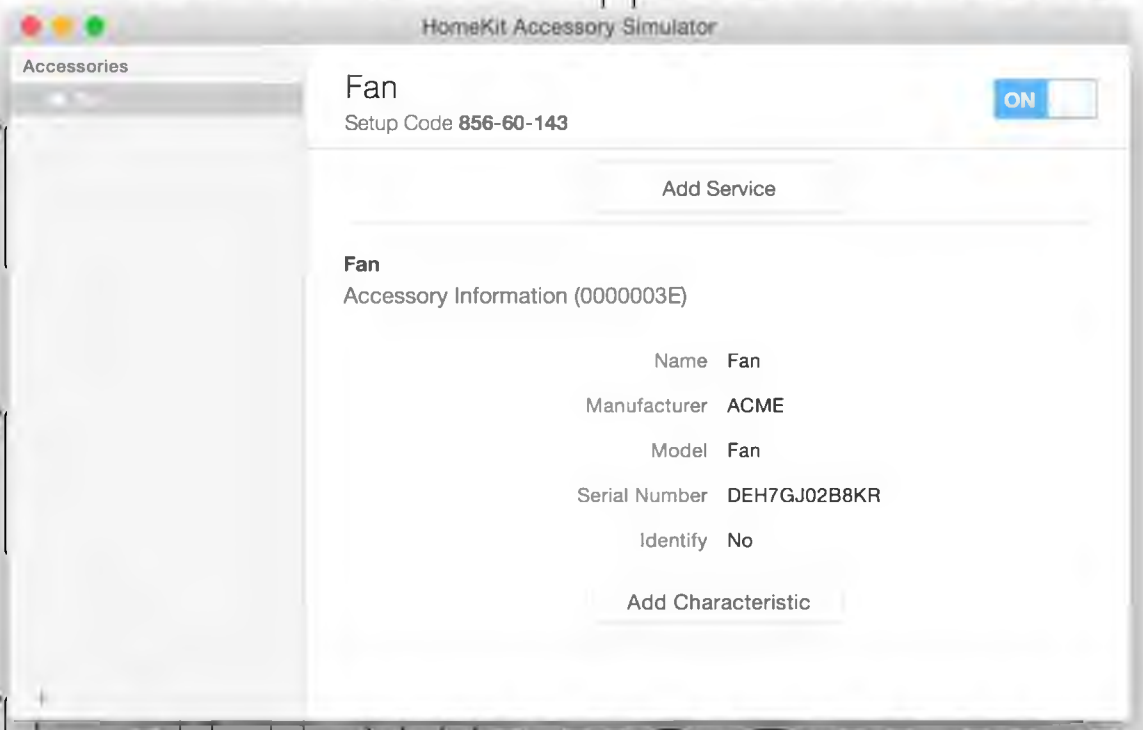


Рисунок 2.6 – Послуги для аксесуарів моделі на основі даних з IoT

Сформувати перехід до другої моделі управління на основі даних з IoT

```
- (void)viewWillDisappear:(BOOL)animated {
    [self.accessoryBrowser stopSearchingForNewAccessories];
}
```

Зупинити пошук аксесуарів моделі на основі даних з IoT.

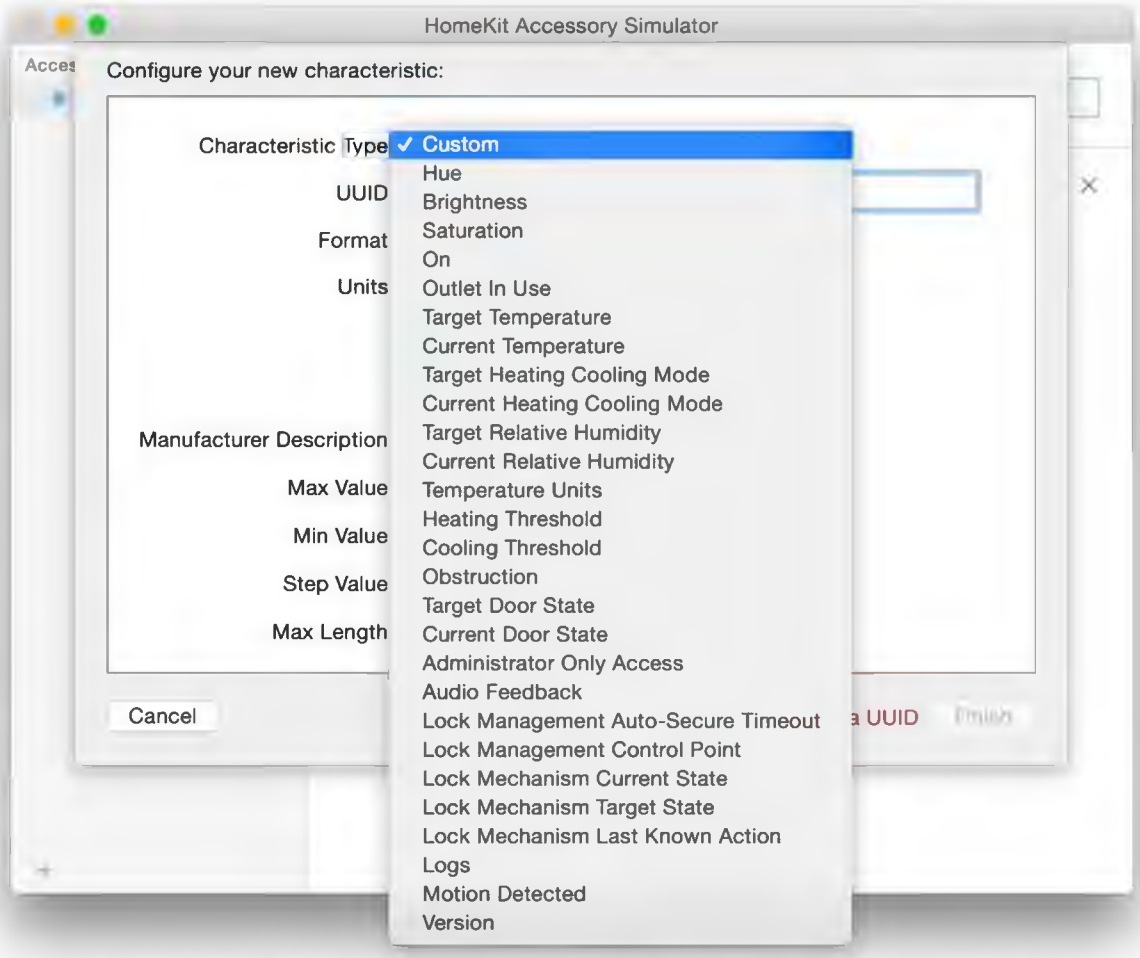


Рисунок 2.7 – Характеристики аксесуарів системи на основі даних з IoT

Переваги створеної системи на основі даних з IoT:

- дозволяє здійснити моніторинг всієї системи з урахуванням розташування датчиків моделі на основі даних з IoT;
- відкрита гетерогенна архітектура управління моделі на основі даних з IoT;
- об'єднана розподілена база даних управління моделі на основі даних з IoT;
- інтерфейси між процесами управління моделі на основі даних з IoT;
- масштабовані рішення управління моделі на основі даних з IoT;

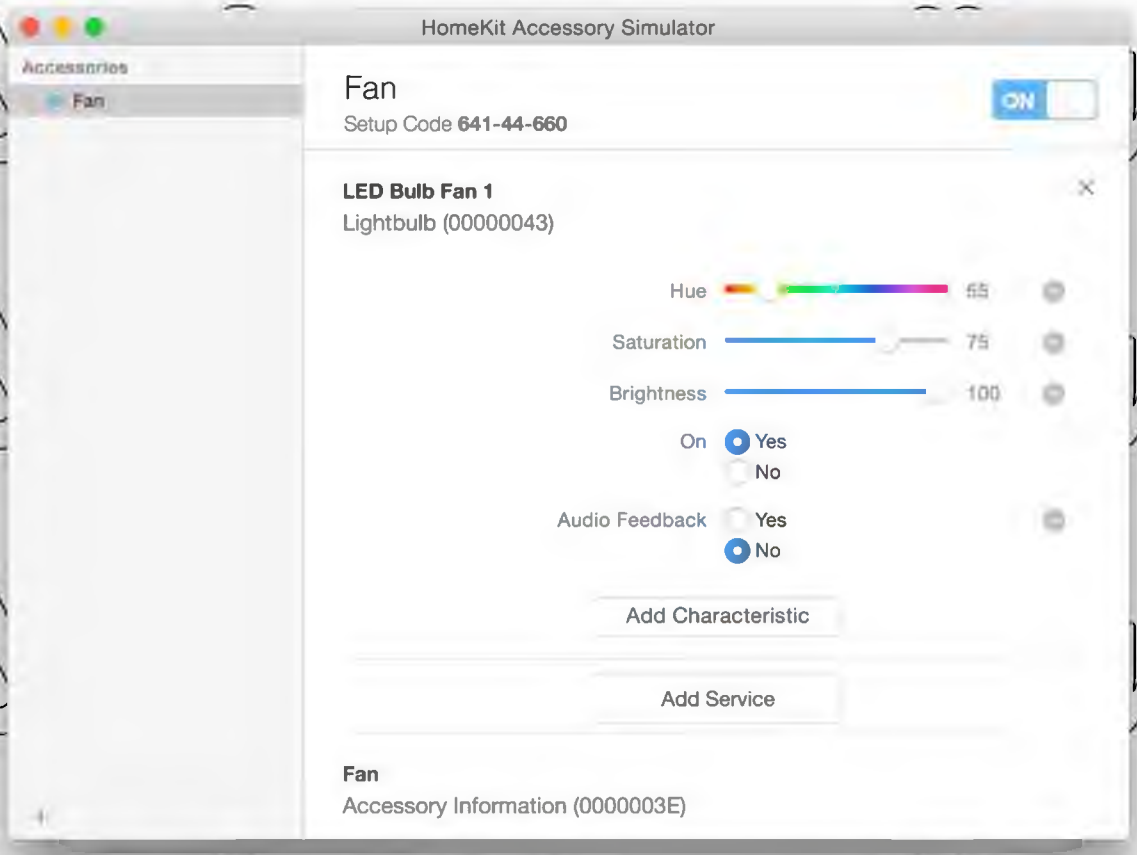


Рисунок 2.8 – Управління аксесуарами системи на основі даних з IoT

- модульна технологія, можливості для етапного впровадження моделі на основі даних з IoT;
- проста інтеграція існуючих і майбутніх систем і інтерфейсів управління моделі на основі даних з IoT;
- база управління, що настроюється моделі на основі даних з IoT;
- автоматизований аналіз подій управління моделі на основі даних з IoT;
- автоматичне управління аварійними ситуаціями управління моделі на основі даних з IoT.

2.3 Алгоритм управління елементами IoT

Модель на основі даних з IoT призначена для створення комфортних умов, захисту матеріальних цінностей, людей, що знаходяться на підприємстві / у будинку, що захищається, забезпечує виконання наступних функцій:

- аналіз сигналів тривог відкриття та злому;
- формування мікроклімату у всіх приміщеннях;
- подання сповіщення про наявність і місце виникнення тривожної / аварійних ситуацій на пульт сигналізації і зовнішній світлозвуковий оповіщувач;
- відключення кульових кранів подачі гарячої та холодної води;
- моніторинг стану елементів системи і її складових частин;
- формування сповіщення про не типову ситуацію в охоронні структури через термінал;
- формування сповіщення про не типову ситуацію, інших подій дзвоном і за допомогою SMS власнику і / або в охоронні структури [25].

Розглянемо приміщення двоповерхове, окремо стояче.

НУБіП України

НУБіП України

НУБіП України

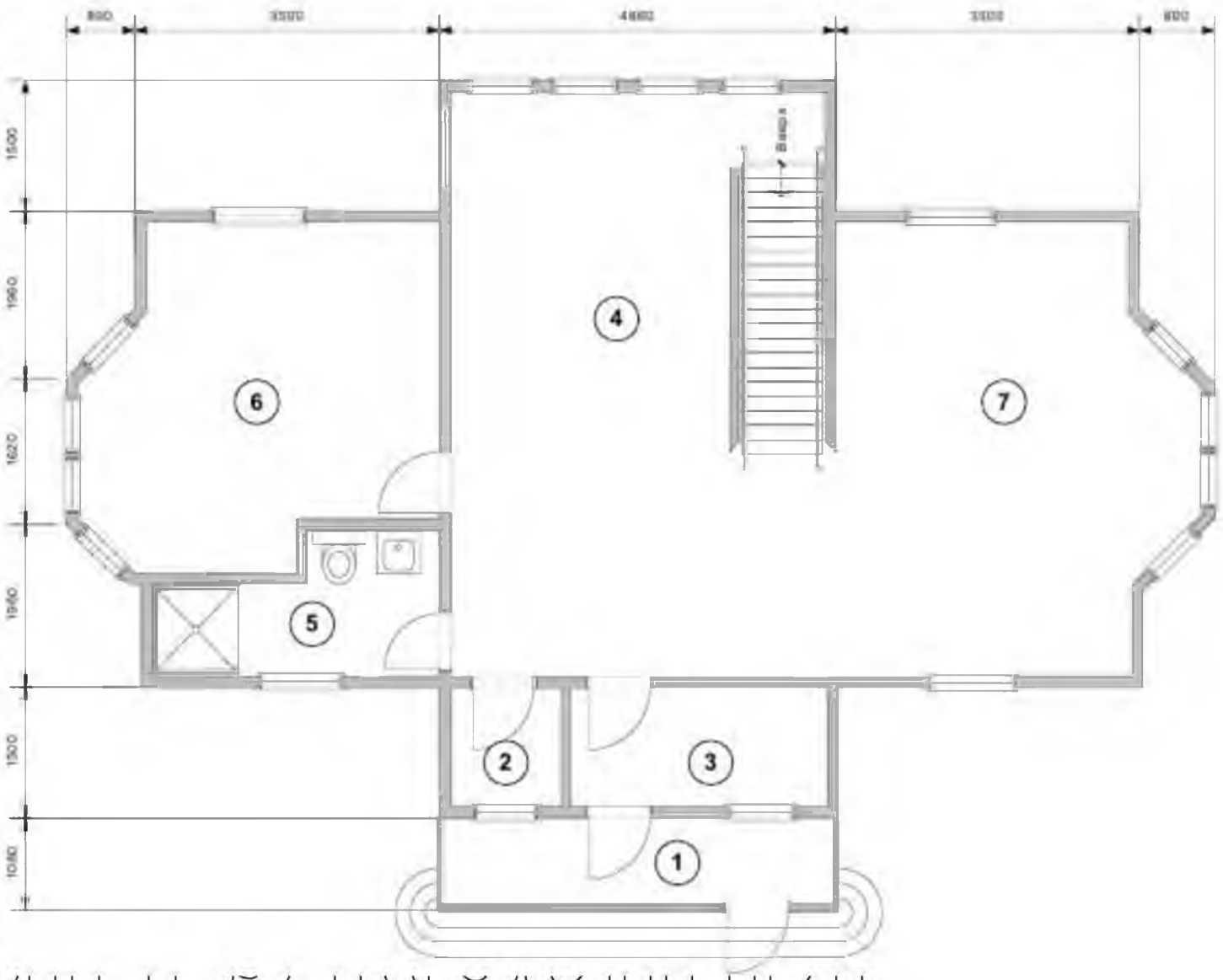
НУБіП України

НУЕ

НУЕ

НУЕ

НУЕ



План першого поверху

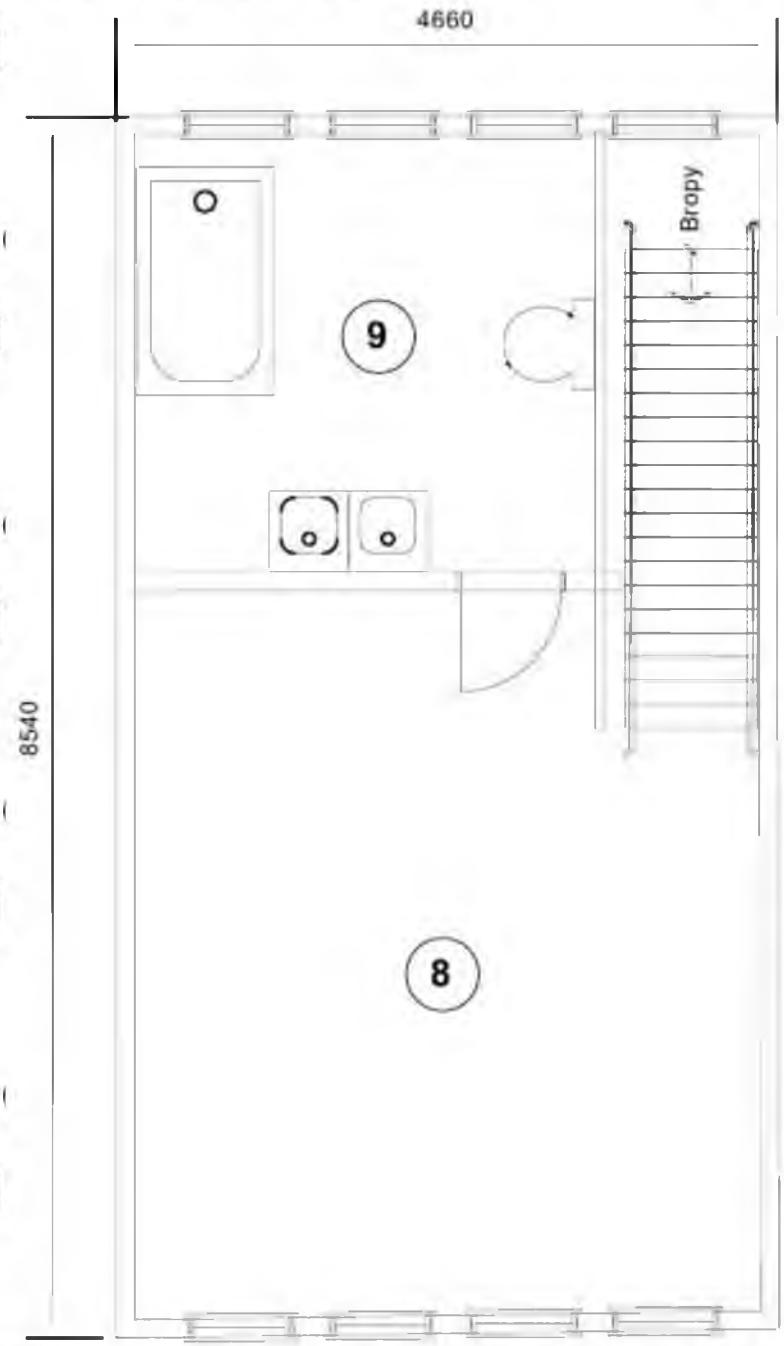
НУБіП України

НУБіП України

НУБіП України

НУБіП України

НУБіП України



План другого поверху

Рисунок 2.9 – План будівлі, яка підлягає встановленню системи на основі даних з IoT

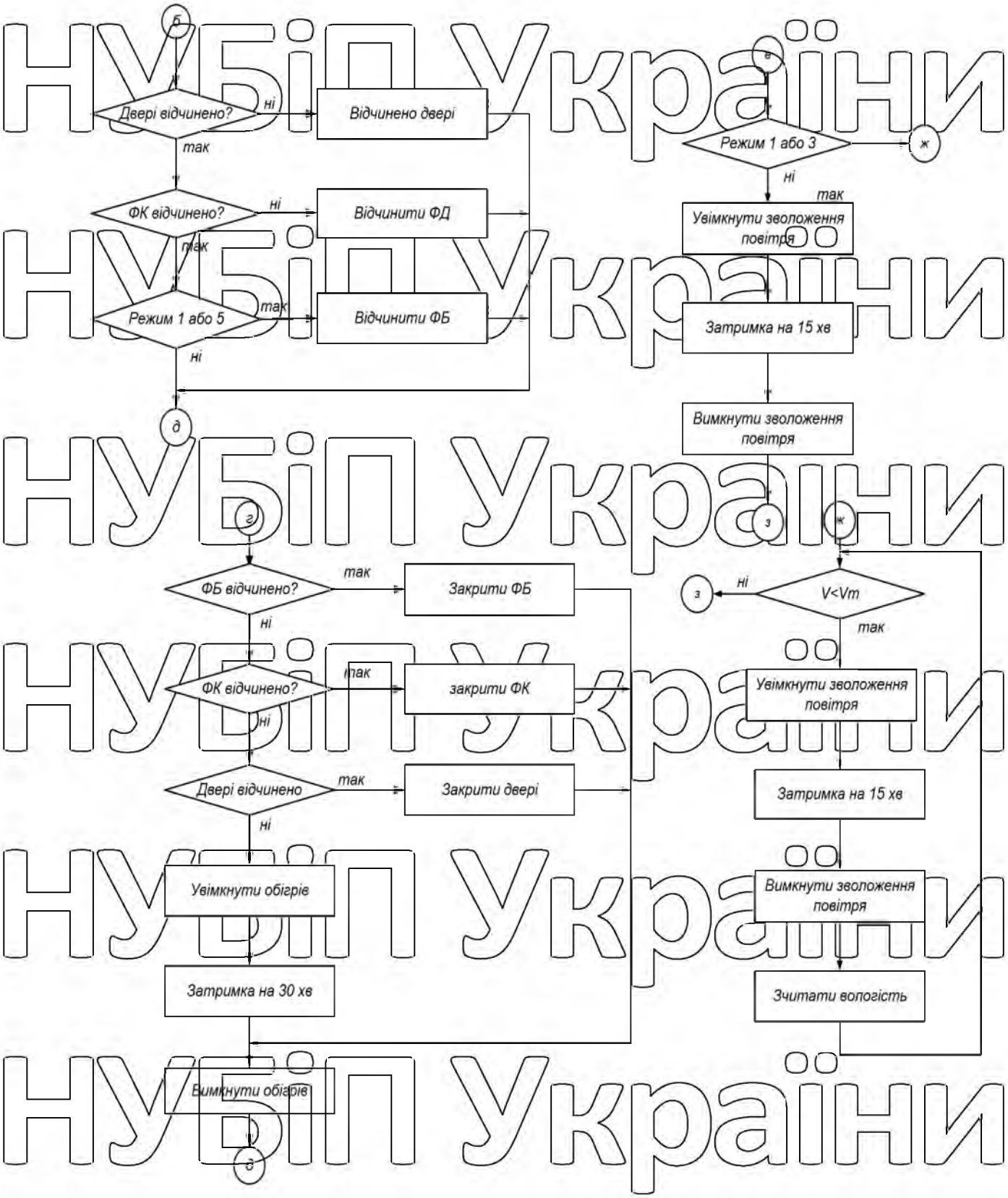
Таблиця 2.1 – Експлікація приміщень підприємства

№ п.п	Найменування	Площа, м^2

	Перший поверх підприємства	
1	Тераса відкрита підприємства	4,37
2	Господарське приміщення для інвентарю притирального підприємства	1,72
3	Тамбур закритий підприємства	4,36
4	Приймальня підприємства	25,25
5	Санвузол	4,66
6	Склад	14,44
7	Виробниче приміщення підприємства	19,21
	Другий поверх підприємства	
8	Бухгалтерія	20,09
9	Санвузол	9,52

Алгоритм роботи моделі на основі даних з IoT предетавлений на рисунку 2.10.

Рисунок 2.10 – Алгоритм роботи системи на основі даних з IoT



Продовження рисунку 2.10

Висновки до розділу

Другим розділом розкрито методологічні аспекти дослідження засобів моніторингу та управління елементами IoT. Визначено принципи моніторингу за елементами та представлено алгоритм управління.

Завдання системи управління та моніторингу за елементами IoT полягає у комплексному моніторингу за життєзабезпеченням підприємства чи окремого житлового будинку. Управління окремими елементами та всією системою загалом здійснюється за допомогою хмари. Всі пристрої IoT, використані в проекті, мають відносно середні характеристики і недорогі в ціні.

Переваги створеної системи на основі даних з IoT, дозволяє здійснити моніторинг всієї системи з урахуванням розташування датчиків моделі на основі даних з IoT; відкрита гетерогенна архітектура управління моделі на основі даних з IoT; об'єднана розподілена база даних управління моделі на основі даних з IoT; інтерфейси між процесами управління моделі на основі даних з IoT; масштабовані рішення управління моделі на основі даних з IoT; модульна технологія, можливості для етапного впровадження моделі на основі даних з IoT; проста інтеграція існуючих і майбутніх систем і інтерфейсів управління моделі на основі даних з IoT; база управління, що настроюється моделі на основі даних з IoT; автоматизований аналіз подій управління моделі на основі даних з IoT; автоматичне управління аварійними ситуаціями управління моделі на основі даних з IoT.

РОЗДІЛ 3 ПРАКТИЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ЗАСОБІВ МОНІТОРИНГУ ТА УПРАВЛІННЯ ЕЛЕМЕНТАМИ IOT

3.1 Архітектура IoT

Інформаційно-аналітична модель моніторингу та управління елементами IoT, що розробляється є багаторівневою. Інтерфейс RS–485 використано як інтерфейс зв'язку. Інтерфейс RS–485 широко використовується в промисловій автоматиці, а так само мережа Ethernet. Загальна структурна схема інформаційно-аналітичної моделі моніторингу та управління елементами IoT, що розробляється показана у додатку А на рис. А.1.

Електрична принципова схема управління комплексом моніторингу та управління елементами IoT наведена у додатку Б на рис. Б.1.

Впровадження системи моніторингу та управління елементами IoT передбачає:

- інтеграцію інженерних систем у інформаційно-аналітичу модель моніторингу та управління елементами IoT;
- створення системи управління інформаційно-аналітичної моделі моніторингу та управління елементами IoT;
- інтеграцію системи управління інженерним обладнанням у систему управління інформаційно-аналітичної моделі моніторингу та управління елементами IoT.

3.2 Система моніторингу та управління елементами IoT

Рішення VMware володіють найбільш досконалими функціями гібридних хмар, вони сумісні з різними типами навантажень і підтримують міграцію між приватними і публічними хмарами разом із синхронізацією каталогів і шаблонів цих хмар. Крім того, рішення VMware забезпечують побудову скоординованих фреймворків високої доступності та безпеки для приватної і публічної хмари.

Віртуалізація дата-центру

У VMware найпотужніші функції віртуалізації і досвід їх використання в корпоративному секторі з початку минулого десятиліття. Хоча Microsoft в останні роки розширює можливості своєї платформи віртуалізації, Hyper-V як і раніше сильно поступається vSphere за популярністю в корпоративному секторі і застосування бізнес-критичних систем. В середині 2014 року Hyper-V підтримував близько 35 гостьових ОС, в той час як у vSphere це значення становить майже сотню. В останні релізи Windows Server 2012 було додано кілька важливих нових функцій Hyper-V (наприклад, Extensible Virtual Switch і Replica), але головним недоліком архітектури Hyper-V як і раніше залишається використання батьківської ОС, що знижує безпеку і доступність гіпервизора при установці патчів і обслуговуванні материнської Windows Server. Крім того, залежність від Windows Server означає, що реалізація в Hyper-V нових функцій віртуалізації відбувається тільки при виході нових версій цієї ОС.

RHEV використовує гіпервізор KVM, на якому працює переважна більшість хмар OpenStack. Зараз RHEV дуже популярний у сервіс-провайдерів і розробників додатків для вбудованих систем. Як і Hyper-V, RHEL є ОСцентричним гіпервізором (його материнської ОС є Red Hat Enterprise Linux (RHEL)), що погіршує безпеку і знижує доступність через необхідність установки патчів RHEL. Він підтримує тільки 15 гостьових ОС, значно поступаючись за цим показником vSphere і Hyper-V. У Red Hat останніх релізів додали ряд нових функцій, але в ньому як і раніше немає віртуального розподіленого комутатора, пулів ресурсів зберігання, балансування навантаження і засобів контролю введення / виводу зберігання і мережі.

Корпоративні замовники рідко використовують хмари OpenStack на базі RHEV. vSphere здатний масштабуватися на кілька кластерів хостів і розширюватися на нові кластери і віртуальні машини в міру зростання потреб. Як показали тести Taneja Group, архітектура vSphere підтримує більше число віртуальних машин на хост, причому ці ВМ обробляли різні комбінації бізнескритичних додатків.

Засоби управління vcenter Server і vcenter Operations Manager можуть масштабуватися до декількох тисяч і навіть десятків тисяч ВМ.

Через обмеження архітектури Hyper-V не може масштабуватися так само ефективно, як vSphere – наприклад, цей гіпервизор не вміє керувати логічними пулами ресурсів (процесорів, пам'яті, мережевих ресурсів і ресурсів зберігання), тому для гарантії стабільної продуктивності віртуальних машин потрібно використовувати виділений кластер хостів. RHEV також не підтримує пули ресурсів процесорів і пам'яті, які масштабуються на кілька хостів кластера і не забезпечує ізоляцію ресурсів або їх спільне використання пулами.

Пакет VMware vCloud Suite Enterprise забезпечує функції високої доступності, відмовостійкості і відновлення після аварій за допомогою функцій vSphere HA, vMotion, Storage vMotion, Fault Tolerance і vCenter Site Recovery Manager. Для зменшення планових зупинок для обслуговування серверів або СГД функції vMotion і Storage vMotion переносять в онлайновому режимі віртуальні машини і їх диски без зупинки роботи додатків і користувачів. Функція vSphere Replication підтримує різні варіанти реплікації для vCenter Site Recovery Manager (SRM) для захисту від великих аварій. SRM забезпечує централізоване планування післяаварійного відновлення, автоматичні failover і failback з резервного сайту або з хмари vCloud, а також тестування післяаварійного відновлення без переривання роботи додатків.

У Microsoft Windows Server 2012 R2 з Hyper-V досить потужні функції HA, реалізовані за допомогою Failover clustering, в тому числі виявлення збоїв і онлайнова міграція ВМ і віртуальних машин. Однак Failover clustering не оптимізовані для захисту ВМ.

Red Hat RHEV здатний виявляти збої ОС хоста або гостьової ОС і підтримує онлайнову міграцію ВМ і віртуальних машин, але в ньому немає вбудованих функцій резервного копіювання та реплікації для швидкого відновлення після аварій.

Дослідження Taneja Group вийшло в середині 2014 року. За минулий рік на ринок вийшли спочатку vSphere 5.5, потім шоста версія vSphere, і рішення для віртуалізації дата-центрів інших вендорів, але значний технологічний відрив VMware від конкурентів зберігається.

Компанія SAFEDATA використовує VMware vSphere і інші продукти VMware як платформу віртуалізації в своєму рішенні « Віртуальний дата-центр» (Virtual Data Center, VDC), на базі якого замовник може самостійно створювати IT-інфраструктуру будь-якої складності, повністю аналогічну рішенням на фізичному обладнанні. В якості апаратної платформи рішення використовуються леза HP BladeSystem c-Class, а також системи зберігання NetApp FAS6220 і FAS8060.

Замовник VDC отримує обчислювальні ресурси для побудови віртуальної інфраструктури з хмари SFCLOUD, розміщеного в двох територіальнорозподілених дата-центрах. Стійкість до відмов вузлів vSphere в SFCLOUD реалізована на основі технології vSphere High Availability (HA). Замовник крім безпосереднього управління цієї віртуальної інфраструктурою за допомогою VMware vCloud Director може гнучко розподіляти виділені йому ресурси хмари між своїми додатками в залежності від зміни навантаження, наприклад, якщо в якийсь момент число запитів до одного з додатків істотно зросте, то можна тимчасово передати йому частину процесорів, виділених іншим додаткам. Крім того, в процесі використання хмарної послуги VDC замовник може збільшувати або зменшувати обсяг виділених йому ресурсів, а також застосовувати різні моделі тарифікації.

Всі дії, пов'язані з управлінням послугою, зміною її параметрів, моніторингом продуктивності, а також фінансовими документами, здійснюються через веб-інтерфейс «Особистого кабінету» замовника VDC.

У новій версії середовища віртуалізації VMware vSphere з'явилася можливість переносити віртуальні машини з приватної хмари в публічну, між

публічними хмарами Google, Amazon і Microsoft і, при бажанні, назад в приватну.

VMware вже давно працює з командою Amazon. Ще в vSphere 5.1 можна було розширити локальну інфраструктуру за рахунок публічної хмари AWS, переносити віртуальні машини в EC2 і управляти ними.

Технології VMware Cloud on AWS дозволяють використовувати всі ті ж надійні, перевірені часом рішення, які вже багато років працюють в ЦОДах наших замовників, але вже с можливістю безшовного розширення в публічне хмара Amazon. Причому це стосується не тільки базової технології віртуалізації обчислювальних ресурсів, але також і віртуалізації мережі (VMware NSX) і системи зберігання даних (VMware vSAN).

Таким чином, з одного боку, замовник може використовувати вже відомі йому технології VMware, а з іншого – розширювати за необхідності ємність свого Цода за рахунок публічного хмари Amazon. Перевага в тому, що можна використовувати ті ж інструменти і поняття, до яких звикли адміністратори, без необхідності переучуватися і занурюватися в ідеологію «Амазону». Крім іншого, це дозволяє забезпечити необхідний рівень SLA і сумісність додатків замовника як з приватною, так і з публічної інфраструктурою.

Якщо спуститися на рівень нижче, то для такого спільного проекту в рамках інфраструктури Amazon використовується виділене обладнання, яке допомагає запускати оптимізовані продукти віртуалізації VMware поверх технологій Amazon: VMware vSphere і Amazon EC2 (обчислювальні ресурси), VMware NSX і Amazon VPC (мережеві ресурси), VMware vSAN і Amazon EBS (ресурси для зберігання). З боку технологій VMware все управляється через єдине вікно – vCenter, з боку Amazon можна використовувати всі можливості AWS. Ці технології дають найкраще з двох світів приватних і публічних хмар: можливість перенесення додатків, готову інфраструктуру безпеки, необхідну продуктивність, еластичність сервісів, можливості використання DR, мікросегментацію, запуск контейнерів,ефективне управління вартістю ресурсів і

багато іншого – і все це за моделлю «як сервіс». Причому всі сервіси надаються, керуються, підтримуються і продаються через єдиного постачальника – VMware.

Нове в vSphere 6.5

У жовтні на конференції VMworld 2016 компанія VMware оголосила про прийдешнє оновлення платформи віртуалізації vSphere до версії 6.5. Заявлено, що в ньому з'являться нові засоби автоматизації і менеджменту. Ось кілька ключових новинок в vSphere 6.5:

vCenter – засіб, який спрощує доставку патчів, апгрейд, бекапи і відновлення, стане ключовим елементом vSphere; vSphere Client – новий клієнтський засіб адміністрування засновано на HTML5 і спрощує адміністрування;

VM Encryption – засіб шифрування рівня віртуальних машин, покликане захистити від несанкціонованого доступу до даних і віртуальним машинам, які проходять міграцію за допомогою vMotion;

Secure Boot – нововведення, яке забезпечить захист від втручання в образи і від завантаження неавторизованих компонентів;

Integrated Containers (інтегровані контейнери) – інтерфейс, сумісний з Docker, який дозволить клієнтам завантажувати контейнери, не порушуючи інфраструктуру.

Окремо варто відзначити появу RESTful API, які спрощують автоматизацію і полегшують життя програмістам і адміністраторам. Ну і звичайно, нова версія зазнала ряд оптимізацій, які повинні помітно збільшити продуктивність. Міграція між приватною і публічною хмарою

1. Вибираємо місце розташування

При використанні даної технології є можливість вибрати один з регіонів для розміщення ресурсів замовника, зокрема один з регіонів, доступних в AWS. Для розміщення ресурсів використовується виділена апаратна інфраструктура Amazon нового покоління, на якій забезпечується робота справжнього гіпервізора VMware ESX.

Рисунок 3.1 – Орієнтування

2/ Вибираємо розмір

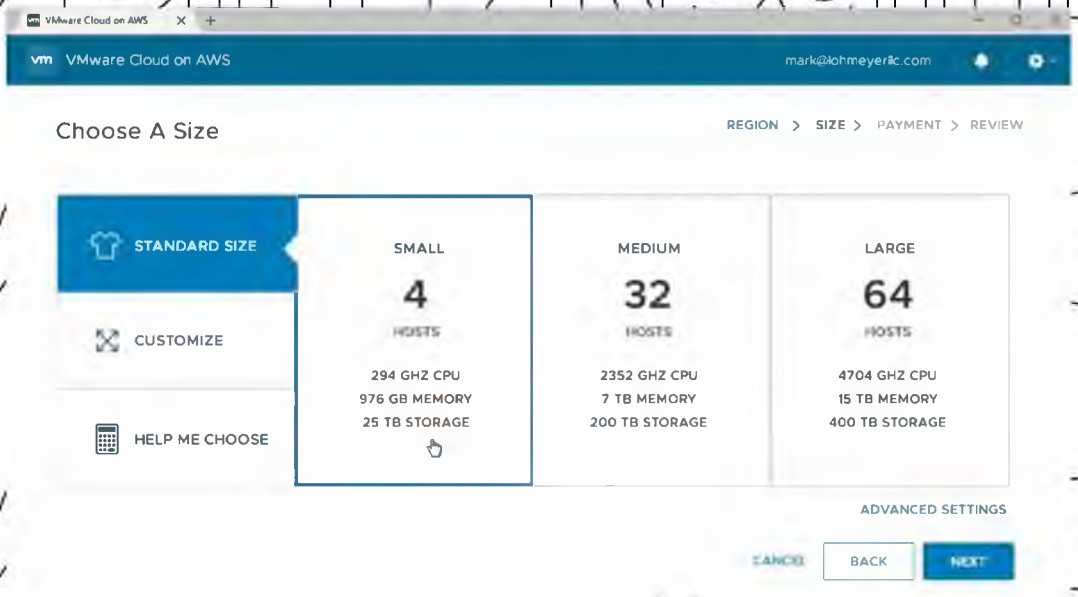


Рисунок 3.2 – Розмір

Для оренди публічних обчислювальних ресурсів Amazon можна вибрати кілька варіантів: від декількох хостів до потужного кластера в 64 Ноди. Все

залежить від потреб замовника. Оренда ресурсів в Amazon відбувається з єдиного акаунту VMware через стандартний особистий кабінет, звідки можна управляти всіма ліцензіями VMware. Якщо необхідно, можливе використовувати REST API для виділення ресурсів, розширення публічного ЦОДа, білінгу та іншого.

3. Оплата

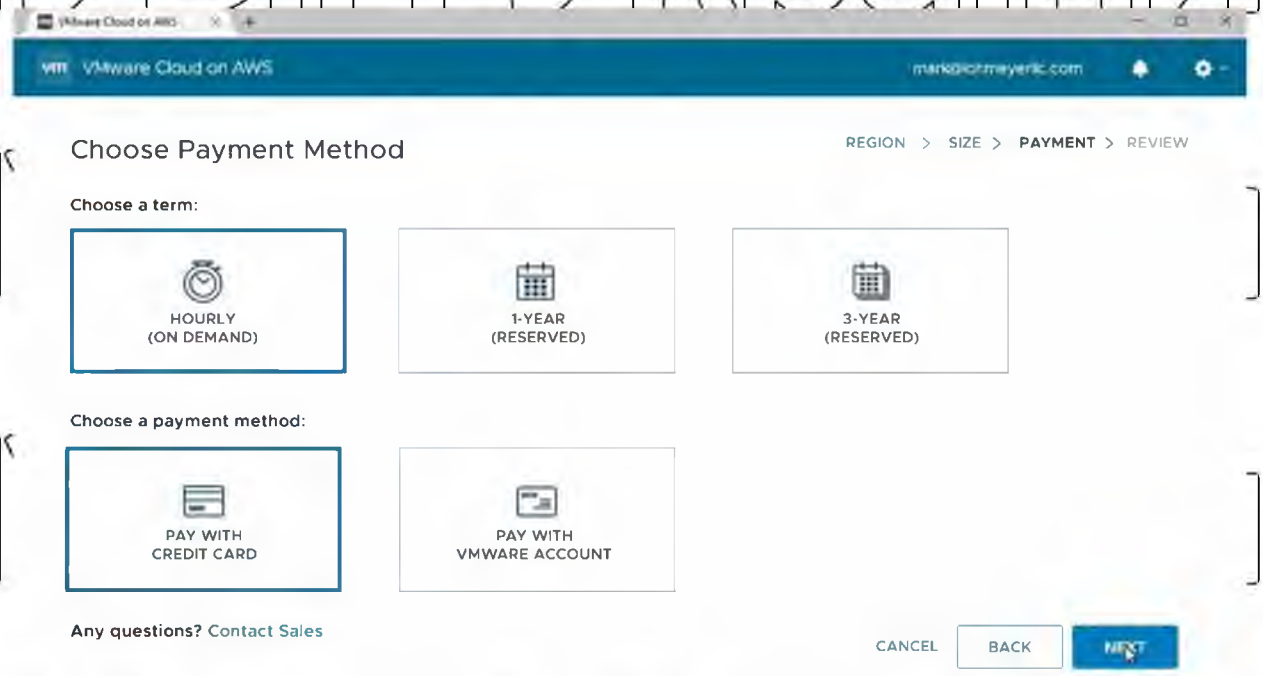


Рисунок 3.3 – Оплата

Вибір моделі резервування та обліку ресурсів: погодинна оплата (Pay-AsYou-Go) або резерв ресурсів на один або три роки. Оплатити можна кредитною або з балансу особистого кабінету VMware.

4. Оточення VMware SDDC

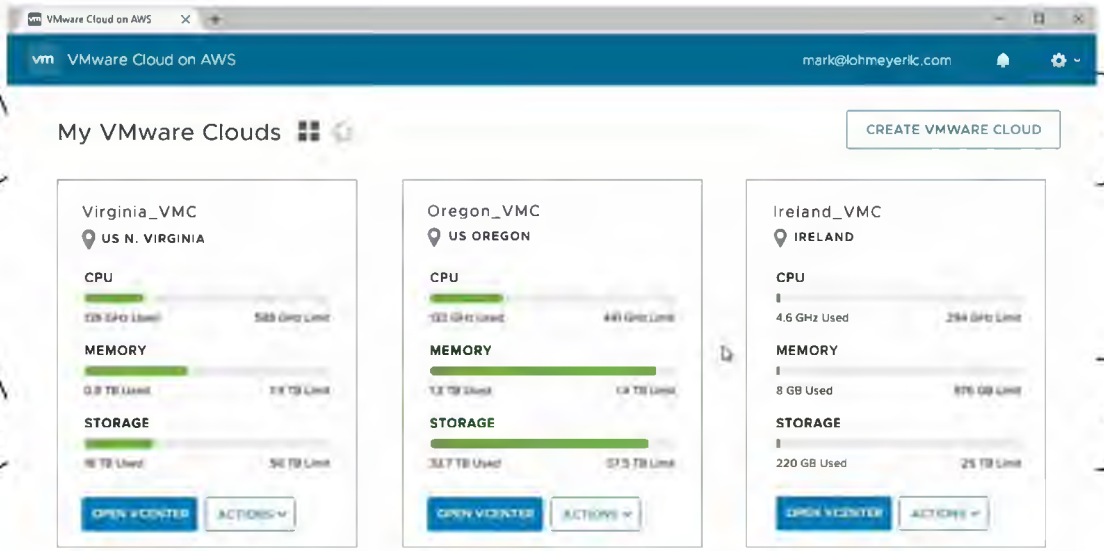


Рисунок 3.4 – Оточення

Панель моніторингу та управління публічними ресурсами: ресурси в публічній хмарі Amazon орендуються в декількох регіонах, відображається їх завантаження.

5. vCenter, full environment

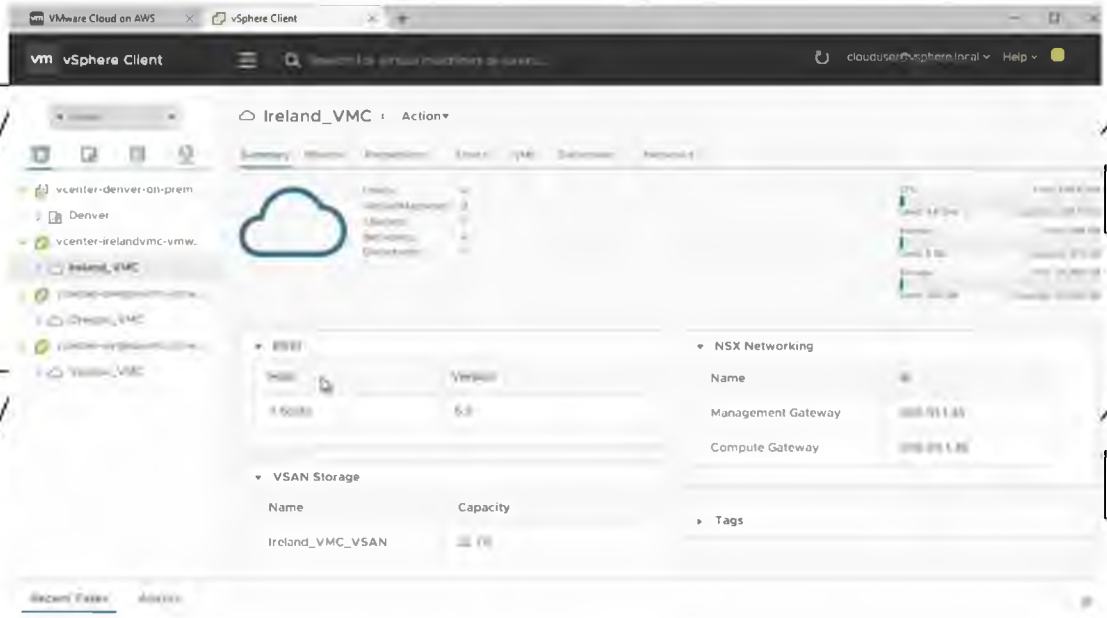


Рисунок 3.5 – vCenter, full environment

Можливість мати єдиний засіб управління прямо з консолі vCenter. Не треба переключатися між різними інтерфейсами, використовувати різні консолі

і так далі. У адміністратора всього одне вікно для управління як внутрішніми ресурсами, так і публічними Amazon, включаючи управління різними регіонами.

6. Переміщуємо сервіс з однієї хмари в іншу.

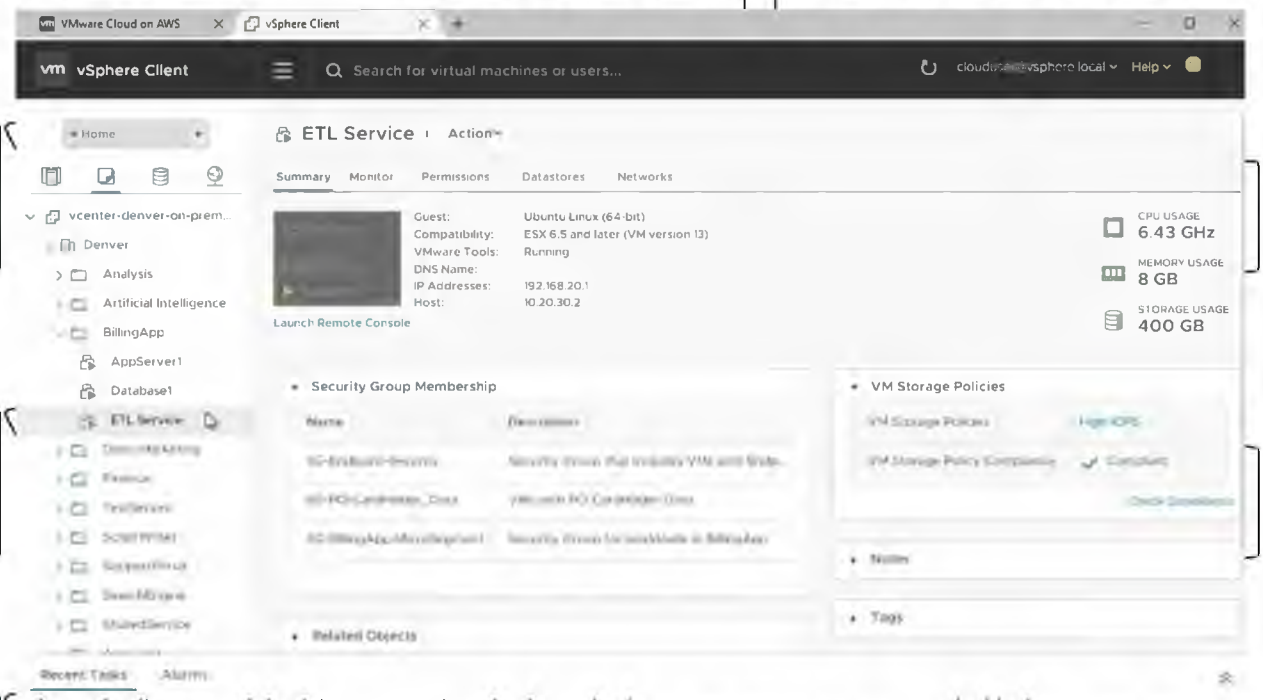


Рисунок 3.6 – Переміщуємо сервіс з однієї хмари

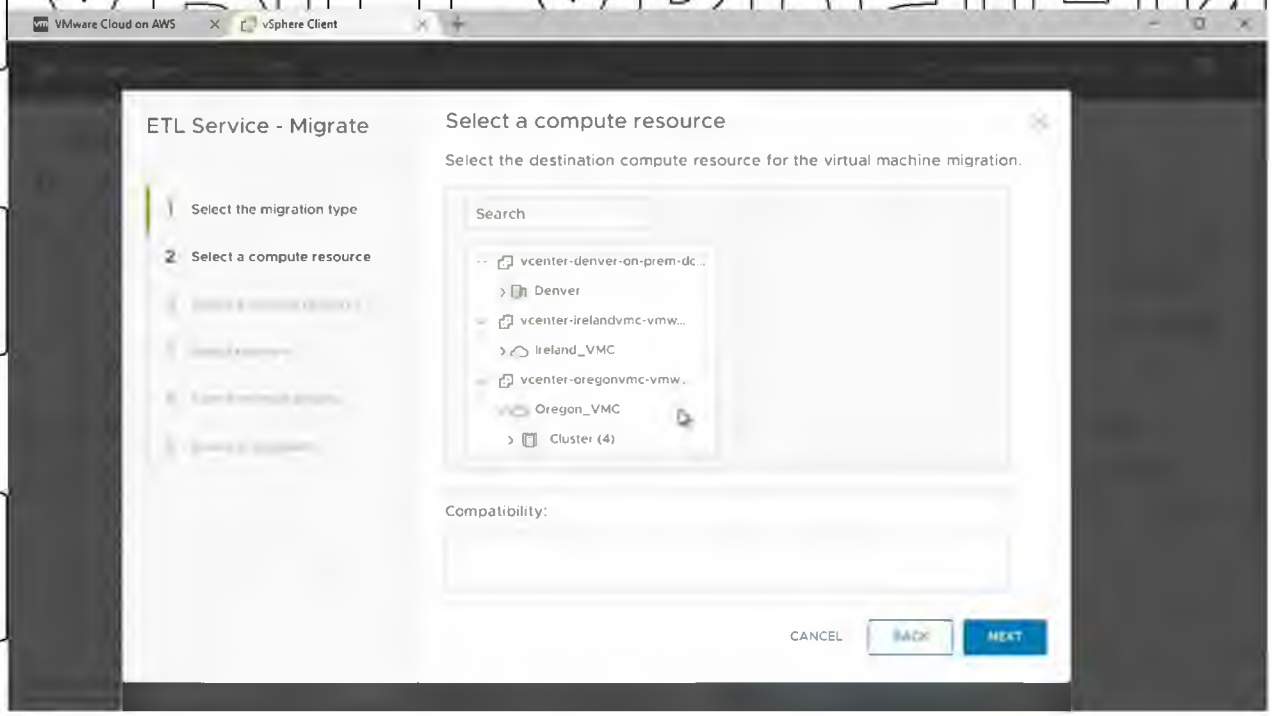


Рисунок 3.7 – Переміщуємо сервіс з однієї хмари

Можливість міграції віртуальної машини існує вже дуже давно. Можна переміщати ВМ як з локального ЦОДа в публічний (з внутрішньої хмари VMware в хмару Amazon), так і між різними регіонами публічної хмари Amazon.

7. Що буде, якщо перевищити обсяг кластера?

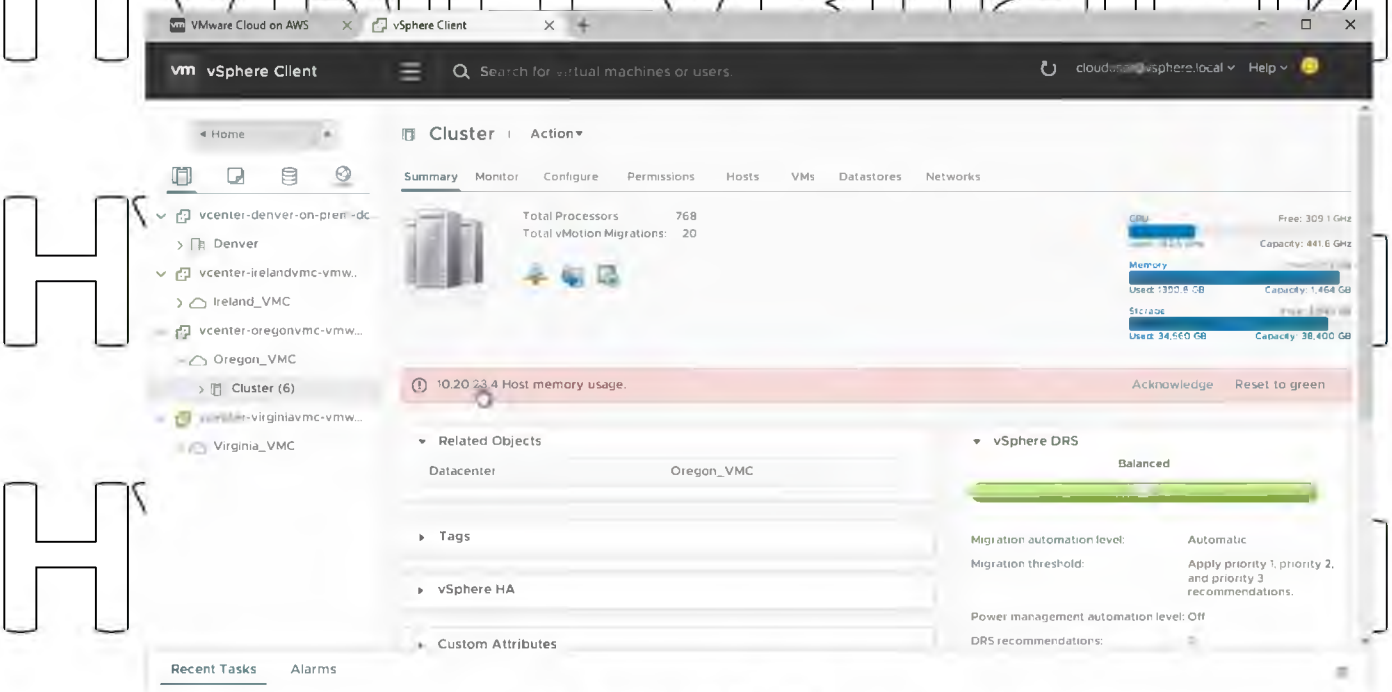


Рисунок 3.8 – Обсяг кластеру

Адміністратор організації має можливість активувати автоматичне масштабування обчислювальних ресурсів. Тобто в разі нестачі публічних ресурсів в автоматичному режимі будуть запитані і виділені нові. З одного боку, технологія побудована поверх AWS EC2 API, яка і забезпечує можливість виділення нових ресурсів, а з іншого – використовується ресурсна модель і аналіз використання ресурсів від VMware. Причому поряд з простим перерозподілом ресурсів реалізовані і технології обходу відмов, коли в разі падіння апаратного сервера для замовника тут же виділяється новий абсолютно безкоштовно. Ця технологія була б неможлива без спільного використання всіх наявних ноухау VMware і Amazon.

Технологія мережевого доступу на основі моделі Zero Trust Network Access (ZTNA): VMware Secure Access – це сервіс ZTNA, який об'єднує продукти VMware Workspace ONE і VMware SD-WAN в єдине хмарне рішення, яке забезпечує більш безпечний, оптимізований і зручний доступ для розподілених користувачів .

Інструменти хмарної і веб-безпеки: VMware співпрацює з провідними гравцями на ринку, щоб надати замовникам більш широкий вибір рішень відповідно до їх вимог до хмарних обчислень і веб-безпеки. Новий сервіс VMware Cloud Web Security дозволить інтегрувати Menlo Security – компонент Service Broker для доступу до хмарним сховищ і віддаленій ізоляції браузера - безпосередньо в рішення VMware SASE.

Інтегрований міжмережевий екран наступного покоління: VMware NSX Firewall – це міжмережевий екран сьомого рівня з контролем стану, який буде надаватися за моделлю SaaS і інтегруватися в платформу VMware SASE як при розрахованому на одного користувача, так і при багато користувальницькому використанні. Це доповнює можливості брандмауера існуючого рішення VMware SD-WAN. У своєму звіті Now Tech: Enterprise Firewalls, Q1 2020 аналітики з Forrester Research назвали VMware одним з п'яти провідних виробників міжмережевих екранів в світі.

Рішення VMware Workspace Security об'єднує провідну в галузі систему уніфікованого управління кінцевими точками і платформу забезпечення їх безпеки. Це дозволяє замовникам використовувати всі переваги роботи з великими даними для досягнення повної прозорості кінцевих точок, а також отримувати потенційно корисні дані і використовувати технологію предикативної аналітики на єдиної панелі управління. Сьогодні VMware оголошує про додаткові пропозиції для VMware Workspace ONE і Workspace Security, які застосовуються для організації ефективної і надійної захисту пристроїв.

VMware Workspace Security Remote – комбінація ведучої в галузі системи для уніфікованого управління кінцевими пристроями (UEM) і технології забезпечення безпеки кінцевих пристроїв і віддаленій IT-підтримки. Сьогодні, в той час як команда фахівців з інформаційної безпеки зосереджена на запобіганні, виявленні та реагуванні на загрози, IT-фахівці контролюють суворе відповідність нормативним вимогам і допомагають замовникам з розгортанням

систем безпеки. Workspace Security Remote об'єднує ці два напрямки, щоб підвищити працездатність пристроїв, забезпечити доступ на основі моделі Zero Trust і автоматизувати процеси реагування на загрози.

VMware Workspace Security VDI інтегрує технології VMware Horizon і VMware Carbon Black Cloud в єдине уніфіковане рішення, що дозволяє ІТспеціалістам і фахівцям з інформаційної безпеки створювати віртуальні робочі столи і додатки з високим ступенем захисту. Workspace Security VDI відрізняється від звичних рішень, оскільки інтегрує технологію Carbon Black особливим чином – безпосередньо в рішення VMware vSphere Hypervisor і VMtools. Це підвищує загальну захищеність системи від злому і відкриває можливості по виявленню програм-вимагачів.

3.3 Верифікація результатів дослідження

Головною метою впровадження сучасної системи моніторингу та управління елементами IoT є підвищення якості обслуговування клієнтів і поліпшення процесу управління. Основними показниками якості є час обслуговування і максимальне, безпомилкове виконання побажань клієнта.

Розрахунок середніх витрат часу на обслуговування клієнтів наведено в таблиці 3.1.

При автоматизованій системі управління річні витрати часу на обробку інформації складаються з витрат часу на обробку первинної інформації (перший етап) та витрат часу на збір і обробку інформації по кожному комплексу (другий етап). У підсумку загальна трудомісткість робіт при такому способі обробки:

$$(5 * 6500) + ((10 + 5 + 5 + 5) * 6500) = 19000/60 = 3500 \text{ год / рік.}$$

Таблиця 3.1 – Час обробки в даний час і в проектному варіанті

	Параметри у поточний час	Параметри у проектному варіанті

Кількість клієнтів, що обслуговуються за рік	6500	6500
Час на збір інформації з датчиків, хв..	5	5
Час оформлення первинної документації, хв.	10	3
Уточнення параметрів, хв.	5	1
Внесення даних про основні показники в базу, хв..	5	0
Передача інформації в інші відділи, хв..	5	0
Час на формування повного пакету з урахуванням усіх використаних послуг та показників датчиків, хв.	6	1

У проектному варіанті роботи зі збору та аналізу інформації виконуються швидше, так як програма працює он-лайн, вносячи зміни в режимі реального часу відразу в базу даних без проміжних вікон підтвердження.

Загальна трудомісткість робіт при впровадженні сучасної системи моніторингу та управління елементами IoT складе:

$$(5 * 6500) + ((3 + 1) * 6500) == 54000/60 = 950 \text{ год / рік}$$

Розрахунки показують, що при запровадженні нової сучасної системи моніторингу та управління елементами IoT загальна трудомісткість роботи знизиться, користувач витратить на 2100 годин на рік менше, ніж в даний час. З цього можна зробити висновок, що якість обслуговування, підвищиться за рахунок економії часу.

Загальний час, який йде на обробку та формування звітної документації по всіх відділеннях з діючої системи становить:

$$6 * 6500 = 36000 / 60 = 650 год / рік.$$

З використанням сучасної АСУ час, необхідний на виставлення остаточного рішення дорівнює:

$$1 * 6000 = 6000 / 60 = 100 год / рік,$$

що на 500 годин менше.

Таблиця 3.2 – Капітальні вкладення за проектом впровадження сучасної системи моніторингу та управління елементами IoT

Найменування	Ціна за од. тис. грн.	Кількість, шт..	Вартість, тис. грн.
Програмне забезпечення	600	1	600
2 робочих місця	1,2	4	4,8
Робоча станція (ПК Celeron G540 (2.5GHz)/2GB /Intel HD/320GB/DVDRW/Cam/WiFi/KB+M/DOS/Black)	14,7	2	2,94
Сенсорні монітори ZTE 11.6	6,4	46	243
Універсальне кріплення Holder DRS-3103	0,24	46	10,8
Кабель UTP кат.5е бухта 305м Telecom Ultra	0,99	1	0,99
Установка додаткових модулів	10,6	1	10,6
Послуги фахівців з впровадження	3	10	60
Навчання персоналу	-	-	80
Інфрачервоний датчик руху Ajax MotionProtect Outdoor	0,3	12	3,6
Всього			893,69

Перелік обладнання і витрат на реалізацію проекту впровадження сучасної системи моніторингу та управління елементами IoT наведено в таблиці 3.2.

Реалізація проекту буде здійснюватися поетапно протягом тижня.

Паралельно з впровадженням ПЗ буде проводитися установка сенсорних моніторів з «блоковим» інтерфейсом Metro.

В процесі впровадження і установки необхідно проводити навчання персоналу, на організацію семінарів виділено 80 тис. грн., консультанти компанії-підрядника проведуть 2 семінари та консультуватимуть користувачів з виникаючих питань в процесі навчання роботи на новій системі моніторингу та управління елементами IoT. Етапи впровадження представлені в таблиці 3.3.

Таблиця 3.3 – Реалізація проекту та терміни виконання

Найменування етапу	Строки виконання
Аналіз існуючої системи управління та моніторингу	Одна доба
Впровадження розумної системи моніторингу та управління елементами IoT	Упродовж тижня
Навчання персоналу і гарантійний супровід системи моніторингу та управління елементами IoT	Упродовж тижня
Установка сенсорних моніторів	Упродовж тижня

Для оцінки рівня ризику найкращим чином підійде метод експертних оцінок, який дозволяє визначати рівні фінансових ризиків в тому випадку, якщо на підприємстві відсутня необхідна інформація для здійснення розрахунків або порівнянь. Даний метод базується на опитуванні експертів (кваліфікованих фахівців страхових, податкових, фінансових органів, інвестиційних менеджерів, працівників відповідних спеціалізованих фірм) з подальшою статистичною обробкою результатів опитування. Комерційні ризики пов'язані з реалізацією послуг (зменшення розмірів і місткості ринку, зниження платоспроможного попиту, появу нових конкурентів).

Заходами щодо зниження ризиків будуть:

- систематичне вивчення кон'юнктури ринку послуг;

- відповідна цінова політика;
- створення системи комплексного обслуговування і додаткових послуг.

Фінансові ризики можуть бути викликані інформаційними процесами, загальними неплатежами, коливаннями валютних курсів і пересичення ринку пропозицій.

Підприємство враховує і ризики, пов'язані з форс-мажорними обставинами, - це ризики, обумовлені непередбаченими обставинами (від зміни політичного курсу країни до страйків і землетрусів). Для зниження загального впливу ризиків на ефективність роботи підприємство передбачає комерційне страхування по системах менеджменту страхування.

Ризик появи альтернативної послуги на ринку послуг досить великий. Для зниження рівня даного ризику можна застосувати систему знижок, що знизить ціни в порівнянні з конкурентами і приверне нових клієнтів. Щоб знизити ризик нестійкості попиту відсутності резервів, підприємству можна запропонувати акцентувати увагу на унікальних пропозиціях – тих продуктах, які ніколи раніше не пропонувалися.

Велику увагу варто приділяти ризику зниження цін конкурентами, так як більшість споживачів вибирають там де дешевше. Для зниження даного ризику організації можна запропонувати стежити за діяльністю конкурентів і своєчасно реагувати на зміни.

Таким чином, підбиваючи підсумки проведеного дослідження, можна зробити висновок, що впровадження сучасної системи моніторингу та управління елементами IoT дозволить:

1) підвищити відповідальність кожної категорії службовців, шляхом автоматизації їх діяльності;

2) скоротити час обслуговування, використовуючи сучасну систему управління;

3) знизити змінні витрати на електроенергію, шляхом підключення модуля енергозбереження з датчиками руху;

4) збільшити дохід підприємства, завдяки автоматизації бізнес-процесів, пов'язаних з плануванням і проведенням заходів, а також за рахунок використання розумного планування та моніторингу.

Сформована практика впровадження даної автоматизованої системи моніторингу та управління елементами IoT в бізнесі за кордоном, а також і на території України показує, що при впровадженні проекту більш ефективним стане зв'язок між функціональними підрозділами. Істотно скоротиться час на обробку інформації і прийняття рішень, підвищиться якість управлінської праці.

Використання сучасних технологій дозволяє досягти підвищення продажів, прихильності клієнтів і ефективності роботи працівників. Комплекс перетворюється в кероване підприємство, яке здатне гнучко реагувати на зміни в ринковій ситуації, що робить вкладення коштів в технології повністю такими, що окупаються.

Для успішної реалізації проекту необхідний обсяг капітальних вкладень становить 893590000 грн. Джерелом фінансування проекту виступають власні кошти підприємства в необхідному розмірі.

Звіт про фінансові результати підготовлений з урахуванням минулорічних фінансових звітів організації, поточної ринкової вартості на основні статті витрат. У таблиці 3.4 представлений прогноз виручки після реалізації проекту впровадження автоматизованої системи моніторингу та управління елементами IoT. У перший рік реалізації проекту відбудеться зростання виручки від експлуатації на 4%, у другий – на 3%, третій рік – 2,5%, 4 рік – 2%.

Вихідні дані для аналізу ефективності інвестиційних вкладень при розробці та реалізації заходів в таблиці 3.5.

Таблиця 3.4 – Прогноз виручки після впровадження системи моніторингу та управління елементами IoT, грн.

Показники	Роки				
	2022	2023	2024	2025	2026
Дохід від експлуатації системи	82882760	85368220	87502420	89252470	92037520
Прибуток (збиток) до оподаткування	22800320	23284330	23523940	23784220	24059900
Чистий прибуток (збиток)	8399040	8652022	8867286	9044632	9225525
Збільшення прибутку за рахунок впровадження системи моніторингу та управління елементами IoT	323040	757022	792286	968632	2249525

У перший рік реалізації проекту виручка організації збільшиться на 3 187760 грн. і складе 82 881760 грн., у другий рік – на 5 674210 грн. з паралельним збільшенням чистого прибутку за рахунок скорочення постійних і змінних витрат, шляхом використання енергозберігаючої системи з датчиками автоматичного включення освітлення в коридорах, а також знизяться витрати на семінари, конференції та комерційні витрати на рекламу і оплату комісійних служби супроводу.

Автоматизація робочих місць всіх категорій співробітників підвищує їх залученість в управлінський процес. Аналітична база нової системи моніторингу та управління елементами IoT дозволить створювати резерви для зниження податкового навантаження.

Запропоновані заходи передбачають вдосконалення процесу автоматизації на підставі впровадження сучасної автоматизованої системи моніторингу та управління елементами IoT.

Таблиця 3.5 – Розрахунок економічної ефективності проекту впровадження системи моніторингу та управління елементами IoT, грн.

Показники	Роки				
	2022	2023	2024	2025	2026
Програмне забезпечення	500000	-	-	-	-
Додаткове обладнання	233890	-	-	-	-
Послуги спеціалістів по впровадженню	80000	-	-	-	-
Навчання персоналу	60000	-	-	-	-
Усього витрат	893590	-	-	-	-
Збільшення рівня прибутку за рахунок впровадження автоматизованої системи моніторингу та управління елементами IoT	-	323040	575022	792286	968632
Економічний ефект	- 893590	323040	575022	792286	968632

В результаті впровадження автоматизованої системи моніторингу та управління елементами IoT в пропонованому проектному варіанті значно зменшилися витрати часу і кількість помилок. Це дозволило підвищити якість обслуговування на підприємстві. Зростання частки постійних клієнтів призведе до зростання виручки підприємства.

В результаті комплекс оснащений сучасною системою моніторингу та управління елементами IoT та одночасно механізмом розумного управління, де на високому рівні реалізовані функції контролю і статистики, управління заходами обліку, що покращує процес управління та документообігу.

Висновки до розділу

У третьому розділі здійснено реалізацію архітектури інформаційноаналітичної моделі системи моніторингу та управління елементами IoT, наведено алгоритм системи моніторингу та управління елементами IoT, здійснено обгрунтування вибору хмарних сервісів та їх налаштування.

Запропоновані заходи передбачають вдосконалення процесу моніторингу та управління елементами IoT на підприємстві на підставі впровадження сучасної автоматизованої системи моніторингу та управління елементами IoT.

В результаті впровадження автоматизованої системи моніторингу та управління елементами IoT в пропонованому проектному варіанті значно зменшилися витрати часу і кількість помилок. Це дозволило підвищити якість обслуговування на підприємстві. Зростання частки постійних клієнтів призведе до зростання виручки підприємства.

В результаті комплекс оснащений сучасною системою моніторингу та управління елементами IoT та одночасно механізмом розумного управління, де

на високому рівні реалізовані функції контролю і статистики, управління заходами обліку, що покращує процес управління та документообігу.

ВИСНОВКИ

У рамках даної кваліфікаційної роботи здійснено дослідження засобів моніторингу та управління елементами IoT. На основі вищевикладеного варто зробити наступний висновок:

Інтернет речей (англ. Internet of Things, IoT) – концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або із зовнішнім середовищем, що розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає із частини дій та операцій необхідність участі людини. Базові елементи поділяються на кілька типів: сенсори, актуатори та гейти.

Середовище роботи систем Інтернету речей часто таке, що зміни можна простежити лише на великих проміжках часу. У разі використання тих чи інших технологій симуляції, емуляції чи імітації варто звернути увагу на те, що потрібна побудова окремої тестової інфраструктури для вирішення цього завдання. Нерідко потрібна певна адаптація систем, що тестують і тестуються, для їх спільної роботи.

Основним завданням IoT є розробка та вибір правильної архітектури системи, оскільки від рішень на початкових етапах досліджень залежатиме весь подальший процес розробки. На даний момент не існує конкретної угоди з архітектури IoT, яка була б затверджена та використовувалася повсюдно.

Завдання системи управління та моніторингу за елементами IoT полягає у комплексному моніторингу за життєзабезпеченням підприємства чи окремого житлового будинку. Управління окремими елементами та всією системою загалом здійснюється за допомогою хмари. Всі пристрої IoT, використані в проекті, мають відносно середні характеристики і недорогі в ціні.

Переваги створеної системи на основі даних з IoT: дозволяє здійснити моніторинг всієї системи з урахуванням розташування датчиків моделі на основі даних з IoT; відкрита гетерогенна архітектура управління моделі на основі даних з IoT; об'єднана розподілена база даних управління моделі на основі даних з IoT; інтерфейси між процесами управління моделі на основі даних з IoT; масштабовані рішення управління моделі на основі даних з IoT; модульна технологія, можливості для етапного впровадження моделі на основі даних з IoT; проста інтеграція існуючих і майбутніх систем і інтерфейсів управління моделі на основі даних з IoT; база управління, що настроюється моделі на основі даних з IoT; автоматизований аналіз подій управління моделі на основі даних з IoT; автоматичне управління аварійними ситуаціями управління моделі на основі даних з IoT.

Запропоновані заходи передбачають вдосконалення процесу моніторингу та управління елементами IoT на підприємстві на підставі впровадження сучасної автоматизованої системи моніторингу та управління елементами IoT.

В результаті впровадження автоматизованої системи моніторингу та управління елементами IoT в пропонованому проектному варіанті значно зменшилися витрати часу і кількість помилок. Це дозволило підвищити якість обслуговування на підприємстві. Зростання частки постійних клієнтів призведе до зростання виручки підприємства.

В результаті комплекс оснащений сучасною системою моніторингу та управління елементами IoT та одночасно механізмом розумного управління, де на високому рівні реалізовані функції контролю і статистики, управління заходами обліку, що покращує процес управління та документообігу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. «Интернет вещей» в промышленности: обзор ключевых технологий и трендов // Ли Да Сюй (Li Da Xu), By Xe (Wu He) - whe@odu.edu, Сянчан Ли (Shancang Li) - shanchang.li@bristol.ac.uk, перевод Алексей Ссотов. – http://www.controlengrussia.com/internet-veshhej/klyuchevy-h-tehnologij/ (Станом на 20.09.2022)

2. 2020. 5G and the enablement of IoT edge processing. Retrieved Nov 2021 from https://hazelcast.com/resources/5g-and-the-enablement-of-iot-edge-processing/

3. A. Zanella, N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," IEEE Internet of Things Journal, vol. 1, pp. 22-32, 2014.

4. Ane Blázquez-García, Angel Conde, Usue Mori, and Jose A Lozano. 2021. A review on outlier/anomaly detection in time series data. Comput. Surveys 54, 3 (2021), 1–33.

5. Asif Iqbal Baba, Manfred Jaeger, Hua Lu, Torben Bach Pedersen, WeiShinn Ku, and Xike Xie. 2016. Learning-based cleansing for indoor RFID data. In SIGMOD. 925–936.

6. Chao Chen, Yan Ding, Xuefeng Xie, Shu Zhang, Zhu Wang, and Liang Feng. 2019. TrajCompressor: An online map-matching-based trajectory compression framework leveraging vehicle heading direction and change. IEEE Transactions on Intelligent Transportation Systems 21, 5 (2019), 2012–2028.

7. Chaoxiong Chen, Chao Chen, Chaocan Xiang, Songtao Guo, Zhu Wang, and Bin Guo. 2020. ToiletBuilder: A PU learning based model for selecting new public toilet locations. IEEE Internet of Things Journal (2020).

8. Elarbi Badidi and Muthucumaru Maheswaran. 2018. Towards a platform for urban data management, integration and processing. In IoTBDS. 299–306.

9. Eikhodr, Mahmoud. (2015). A Smart Home Application Based on the Internet of Things Management Platform. 10.1109/DSDIS.2015.23.

10. Fernandes Nicole Ann and Rupali Wagh. 2019. Quality assurance in big data analytics: An IoT perspective. Telfor Journal 11, 2 (2019), 114–118.

11. Frederike Dümbgen, Cynthia Oeschger, Mihailo Kolundžija, Adam Scholefield, Emmanuel Girardin, Johan Leuenberger, and Serge Ayer. 2019. Multimodal probabilistic indoor localization on a smartphone. In IPIN. 1–8.

12. Garvita Bajaj, Rachit Agarwal, Pushpendra Singh, Nikolaos Georgantas, and Valérie Issarny. 2018. 4W1H in IoT semantics. IEEE Access 6 (2018), 65488–65506.

13. Growing opportunities in the Internet of Things. Retrieved Nov 2021 from https://www.mckinsey.com/industries/ private-equity-and-principal-investors/ourinsights/growing-opportunities-in-the-internet-of-things

14. IDC forecasts connected IoT devices to generate 79.4ZB of data in 2025. Retrieved Nov 2021 from https //futureiot.tech/idc-forecasts-connected-iot-devicesto-generate-79-4zb-of-data-in-2025/

15. Isam Mashhour Al Jawarneh, Paolo Bellavista, Antonio Corradi, Luca Foschini, and Rebecca Montanari. 2020. Big spatial data management for the Internet of Things: A survey. Journal of Network and Systems Management 28, 4 (2020), 990–1035

16. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, pp. 1645-1660, 2013

17. Jian Chen, Gang Ou, Ao Peng, Lingxiang Zheng, and Jianghong Shi. 2018. An INS/WiFi indoor localization system based on the weighted least squares. Sensors 18, 5 (2018), 1458.

18. Li, Daming & Deng, Lianbing & Cai, Zhiming & Souri, Alireza. (2022). Blockchain as a service models in the Internet of Things management: Systematic review. Transactions on Emerging Telecommunications Technologies. 33. 1-14. 10.1002/ett.4139.

19. Li, Huan & Lu, Hua & Jensen, Christian & Tang, Bo & Cheema, Muhammad. (2022). Spatial Data Quality in the Internet of Things: Management, Exploitation, and Prospects. 10.1145/3498338.

20. Liang Chen, Sarang Thombre, Kimmo Järvinen, Elena Simona Lohan, Anette Alén-Savikko, Helena Leppäkoski, M Zahidul H Bhuiyan, Shakila Bu-Pasha, Giorgia Nunzia Ferrara, Salomon Honkala, et al. 2017. Robustness, security and privacy in location-based services for future IoT: A survey. IEEE Access 5 (2017), 8956–8977.

21. Ling Chen, Yaya Cai, Yifang Ding, Mingqi Lv, Cuili Yuan, and Gencai Chen. 2016. Spatially fine-grained urban air quality estimation using ensemble semisupervised learning and pruning. In UbiComp. 1076–1087.

22. M. Elkhodr, S. Shahrestani, and H. Cheung, "A Semantic Obfuscation Technique for the Internet of Things," presented at the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 2014

23. Mamta Agiwal, Navrati Saxena, and Abhishek Roy. 2019. Towards connected living: 5G enabled Internet of Things (IoT). IETE Technical Review 36, 2 (2019), 190–202.

24. Peng Dai, Yuan Yang, Manyi Wang, and Ruqiang Yan. 2019. Combination of DNN and improved KNN for indoor location fingerprinting. Wireless Communications and Mobile Computing 2019 (2019).

25. Qing Cheng, Huiqing Liu, Huanfeng Shen, Penghai Wu, and Liangpei Zhang. 2017. A spatial and temporal nonlocal filter-based data fusion method. IEEE Transactions on Geoscience and Remote Sensing 55, 8 (2017), 4476–4488.

26. Tanvi Banerjee and Amit Sheth. 2017. IoT quality control for data and application needs. IEEE Intelligent Systems 32, 2 (2017), 68–73.

27. Xiao Chen and Shenghan Zou. 2017. Improved Wi-Fi indoor positioning based on particle swarm optimization. IEEE Sensors Journal 17, 21 (2017), 7143–7148.

28. Xin Ding, Lu Chen, Yunjun Gao, Christian S. Jensen, and Hujun Bao. 2018. UlTraMan: A unified platform for big trajectory data management and analytics. Proceedings of the VLDB Endowment 11, 7 (2018), 787–799.

29. Xinyu Chen, Jiajie Xu, Rui Zhou, Wei Chen, Junhua Fang, and Chengfei Liu. 2021. TrajVAE: A Variational AutoEncoder model for trajectory generation.

Neurocomputing 428 (2021), 332–339.

30. Zhida Chen, Gao Cong, Zhenjie Zhang, Tom Z.J Fuz, and Lisi Chen. 2017. Distributed publish/subscribe query processing on the spatio-textual data stream. In ICDE. 1095–1106.

ДОДАТКИ

Додаток А Функціональна схема IoT-рішення

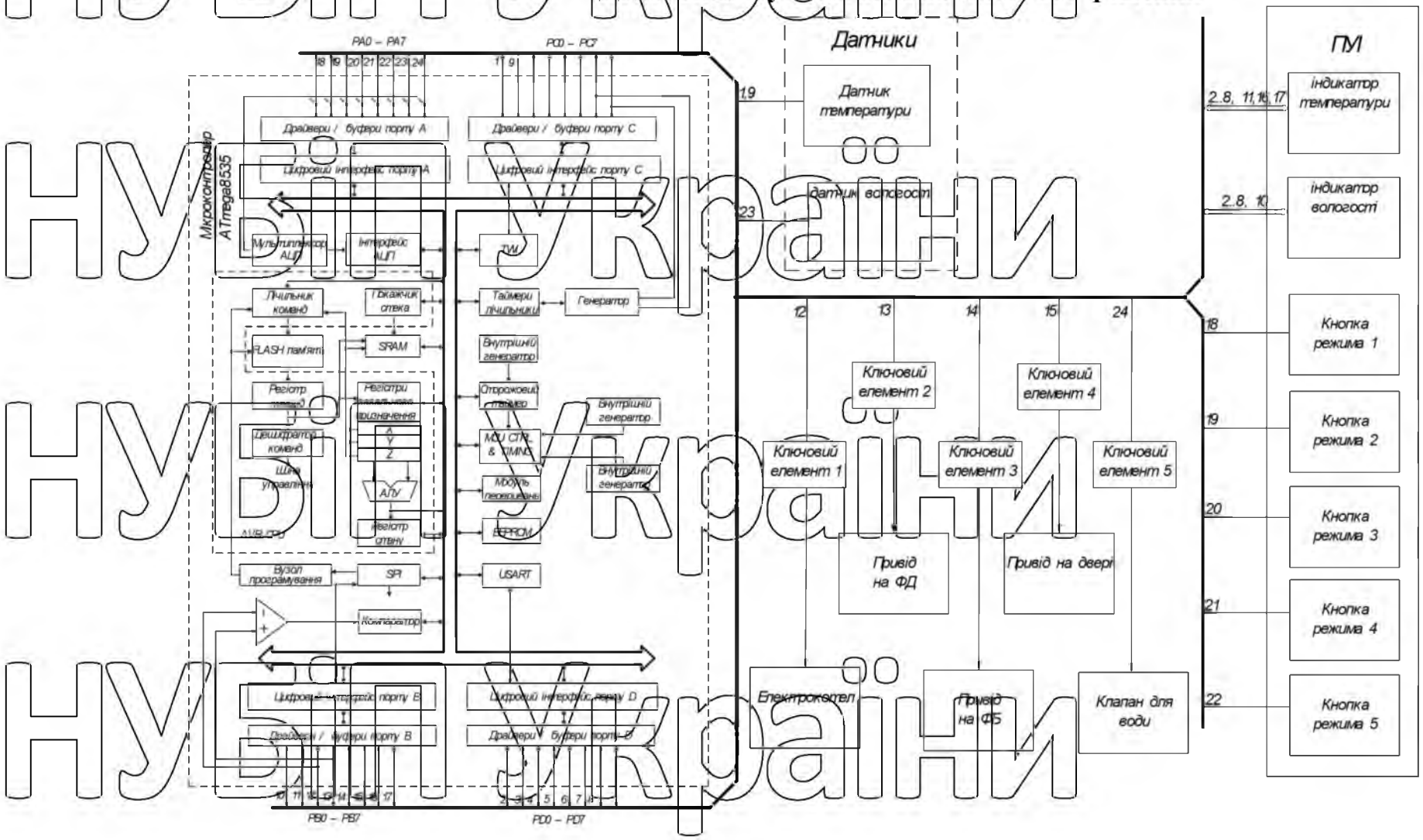


Рисунок А.1 – Функціональна схема системи моніторингу та управління елементами IoT

Додаток Б Електрична принципова схема IoT-рішення

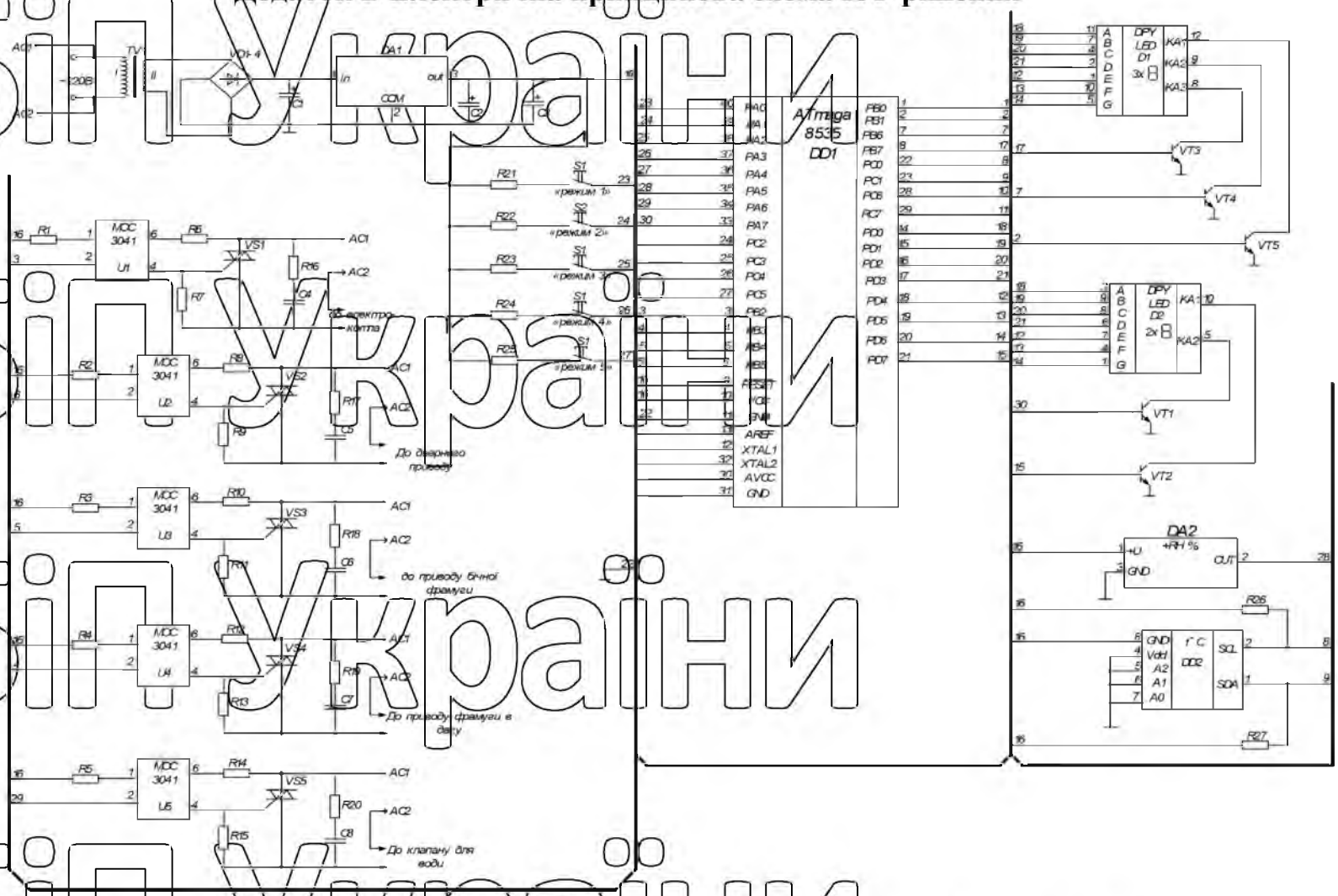


Рисунок Б.1 – Електрична принципова схема системи моніторингу та управління елементами IoT