

Хмельницький національний університет  
Факультет інформаційних технологій  
Кафедра кібербезпеки

**КВАЛІФІКАЦІЙНА РОБОТА**

Гасюка Євгенія Ігоровича

на здобуття ступеня вищої освіти Бакалавра


ІоТ–мережа для системи  
“Розумний замиський будинок”

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп’ютерна інженерія

Освітня програма Кібербезпека

Шифр КРБКІ.101003.21.01.03 ПЗ

Виконав студент 3 курсу група КІс-21-1  Євгеній ГАСЮК

Керівник старший викладач  Сергій МОСТОВИЙ

Нормоконтролер старший викладач  Сергій МОСТОВИЙ

До захисту допускаю:  
Завідувач кафедри кібербезпеки  Юрій КЛЮЧ

12 06 2024 р.

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій  
Кафедра Кібербезпеки  
Рівень вищої освіти Бакалавр  
Галузь знань 12 – Інформаційні технології  
Спеціальність 123 – Комп'ютерна інженерія  
Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ 

15 лютого 2024 р.

**ЗАВДАННЯ  
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Гасюку Євгенію Ігоровичу

1 Тема роботи IoT–мережа для системи “Розумний заміський будинок”

Керівник роботи Мостовий Сергій

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 12.06.2024

3 Вихідні дані до роботи Логічна топологія мережі, план заміського будинку, симуляція роботи мережі, завдання на кваліфікаційну роботу

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Дослідження предметної області та постановка задачі

Проектування та конфігурація мережі

Створення сценаріїв IoT та підключення мережі до інтернету

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)


Логічна топологія мережі

Розміщення пристроїв згідно плану будинку

Алгоритм роботи сценаріїв мережі

Симуляція роботи додатку Cisco Asset Vision

6 Консультанти розділів кваліфікаційної роботи

| Розділ        | Прізвище, ініціали та посада консультанта               | Підпис, дата   |   |
|---------------|---|----------------|---|
|               |   | завдання видав | завдання прийняв  |
| Нормоконтроль | Мостовий С.В.,<br>старший викладач кафедри кібербезпеки |                |  |

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

| Назва етапів (розділів) кваліфікаційної роботи   | Строк виконання етапів роботи | Примітка |
|--|-------------------------------|----------|
| Вибір і затвердження теми кваліфікаційної роботи | Січень                        |          |
| Ознайомлення з предметною областю                | Лютий                         |          |
| Дослідження існуючих рішень                      | Лютий                         |          |
| Постановка задачі                                | Березень                      |          |
| Визначення загальних принципів рішення задачі    | Березень                      |          |
| Деталізація принципів рішення задачі             | Квітень                       |          |
| Розробка проектних рішень                        | Квітень                       |          |
| Апробація проектних рішень                       | Травень                       |          |
| Оформлення пояснювальної записки згідно вимог    | Травень                       |          |
| Оформлення графічної частини                     | Травень                       |          |
| Захист КР  | Червень                       |          |

Студент



Євгеній ГАСЮК

Керівник кваліфікаційної роботи



Сергій МОСТОВИЙ



## АНОТАЦІЯ

Тема кваліфікаційної роботи: «IoT–мережа для системи “Розумний замський будинок”».

Автор роботи: Гасюк Євгеній Ігорович.

Керівник роботи: Мостовий Сергій.

Пояснювальна записка: 72 с., 50 рис., 21 табл., 1 дод., 41 джерело.

Графічна частина: 4 креслення.

ІОТ, КІБЕРФІЗИЧНА СИСТЕМА, Мережа, МОНІТОРИНГ, РОЗУМНИЙ БУДИНОК.

Метою кваліфікаційної роботи є планування та проєктування IoT–мережі, а також її конфігурація для забезпечення достатньої ефективності, автоматизованості та зручності роботи з нею.

Об'єктом дослідження є інтегрована мережа Інтернету речей.

Предметом дослідження є оцінка технологій, протоколів IoT–мереж, використовуваних для системи "Розумний замський будинок" та їх впливу на функціонування системи.

Під час проведення даного дослідження був використаний метод систематичного огляду літератури для вивчення і аналізу предметної області даного дослідження з текстових джерел інформації.

10.06.24



## ЗМІСТ

|   |    |
|---|----|
| Скорочення та умовні позначки .....   | 4  |
| Вступ.....  | 4  |
| 1 Дослідження предметної області та постановка задачі.....                        | 5  |
| 1.1 Аналіз предметної області та теоретичні основи роботи систем IoT.....         | 5  |
| 1.2 Огляд наявних видів IoT пристроїв та їх використання .....                    | 8  |
| 1.3 Аналіз існуючих варіантів підключення IoT пристроїв до мережі .....           | 13 |
| 1.4 Формування вимог для розробки IoT-мережі для системи "Розумний будинок" ..... | 19 |
| 1.5 Постановка задачі.....  | 20 |
| 1.6 Висновки .....  | 21 |
| 2 Аналіз існуючих рішень та вибір підходу для вирішення поставленої задачі ....   | 22 |
| 2.1 Огляд існуючих рішень для створення системи "Розумний будинок" .....          | 22 |
| 2.2 Порівняльний аналіз переваг та недоліків існуючих рішень .....                | 28 |
| 2.3 Вибір пристроїв для мережі з врахуванням плану території будинку .....        | 31 |
| 2.4 Висновки .....  | 46 |
| 3 Проектування та налаштування мережі "Розумний замський будинок" .....           | 48 |
| 3.1 Проектування мережі та розташування пристроїв згідно плану будинку ..         | 48 |
| 3.2 Сценарії. Їх розробка та впровадження .....                                   | 57 |
| 3.3 Підключення мережі до інтернету .....   | 61 |
| 3.4 Розрахунок вартості системи "Розумний замський будинок".....                  | 62 |
| 3.5 Напрямки вдосконалення.....   | 64 |
| 3.6 Висновки .....  | 65 |
| Висновки .....  | 67 |
| Література .....  | 69 |
| Додаток А Копія графічної частини.....  | 73 |

|                          |      |               |        |          |   |                |       |         |
|--------------------------|------|---------------|--------|----------|---|----------------|-------|---------|
| КвРКІ.101003.21.01.03 ПЗ |      |               |        |          |   |                |       |         |
| Зм.                      | Арк. | №докум.       | Підпис | Дата     | IoT-мережа для системи<br>"Розумний замський будинок"<br>Пояснювальна записка | Літера         | Арквш | Арквшів |
| Виконав                  |      | Гасюк Є.І.    |        | 10.08.24 |   |                | 2     | 72      |
| Перевір.                 |      | Мостовий С.В. |        | 12.01.24 |   |                |       |         |
| Н.контр.                 |      | Мостовий С.В. |        | 07.06.24 |   |                |       |         |
| Затвер.                  |      | Кльощ Ю.П.    |        | 12.06.24 |   |                |       |         |
|                          |      |               |        |          |   | ХНУ, КІІс-21-1 |       |         |

## СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IoT – Internet of Things (інтернет речей)

WiFi – Wireless Fidelity (безпроводний зв'язок)

ПЗ – програмне–забезпечення

AP – Access Point (точка доступу)

ІЧ – інфрачервоне випромінювання

PIR – Pyroelectric InfraRed (піроелектричний інфрачервоний)

RBF – Radio Bearer Frame (кадр радіоносія)

MQTT – Message Queue Telemetry Transport (телеметрійна черга транспорту повідомлень)

PAN – Personal Area Network (персональна мережа)

BLE – Bluetooth Low Energy (Bluetooth з низьким енергоспоживанням)

LED – Light–Emitting Diode (світловипромінюючий діод)

UCS – Unified Computing System (уніфікована обчислювальна система)

CIMC – Cisco Integrated Management Controller (інтегрований контролер керування Cisco)

DHCP – Dynamic Host Configuration Protocol (протокол динамічної конфігурації вузла)

UDP – User Datagram Protocol (протокол датаграм користувача)

TFTP – Trivial File Transfer Protocol (тривіальний протокол передачі файлів)

SSID – Service Set Identifier (унікальне найменування бездротової мережі)

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 3    |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

## ВСТУП

Щодня кількість електроніки та гаджетів у людей по всьому світу стрімко збільшується, оскільки технології та людство розвиваються дуже швидко. Запити людей стають дедалі більш вимогливими. Тому сучасний ринок електроніки відзначається великим розмаїттям технологічних процесів, які прагнуть перевершити вже існуючі. Таким чином, електроніка оновлюється щоденно, намагаючись задовольнити поточні потреби людства у зручності та забезпечити ефективність його використання.

Інтернет речей — це потужна сила, що може спростити та модернізувати наше життя в багатьох аспектах. Від поліпшення зв'язку та автоматизації до сприяння прийняттю рішень на основі даних і розвитку стійких розумних міст, IoT відкриває нам перспективу майбутнього, де взаємодія з технологіями буде гладкою, персоналізованою, безперервною та ефективною. З подальшим розвитком екосистеми IoT, її вплив на наше повсякденне життя, ймовірно, зростатиме, створюючи більш зв'язаний, розумний і чуйний світ [15].

Основною цінністю таких мереж є те, що вони значно полегшують наше повсякденне життя, дозволяючи людям ефективніше використовувати свій час і не витрачати його на дрібниці, які можуть бути вирішені за допомогою даних IoT систем [29].

Існує безліч типів IoT мереж, і виробників цих мереж також чимало. Тому дуже важливо вибрати відповідний тип мережі, необхідні пристрої та їх виробника, щоб уникнути внутрішніх мережних конфліктів [32].

IoT – це доволі складна мережева конструкція, яка ні в якому разі не виключає людський фактор, який сам по собі часто призводить до виходу з ладу деяких компонентів такої мережі. Тому часто потрібне обслуговування такої мережі. Правильне налаштування, та підбір потрібних пристроїв дозволяють уникати різноманітних збоїв, та помилок такої системи [16].

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 4    |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

# 1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

## 1.1 Аналіз предметної області та теоретичні основи роботи систем IoT

Інтернет речей (IoT) займає передові позиції в технологічних інноваціях, готовий змінити світ, яким ми його знаємо. IoT об'єднує фізичні пристрої, датчики, виконавчі механізми та технології зв'язку, які працюють разом, створюючи бездоганно взаємопов'язану мережу «розумних» об'єктів. Такий взаємозв'язок відкриває безліч можливостей у різних галузях, включаючи медицину, радикально змінюючи способи взаємодії з технологіями, управління навколишнім середовищем і життя в цілому [15, 38].

Впровадження інтернету речей (IoT) стає справжньою еволюцією в сфері технологій та комунікацій. Це інноваційний підхід, який може змінити наше сприйняття реальності і зробити наше життя значно зручнішим та безпечнішим. Можливості запровадження IoT зображені на рисунку 1.1.

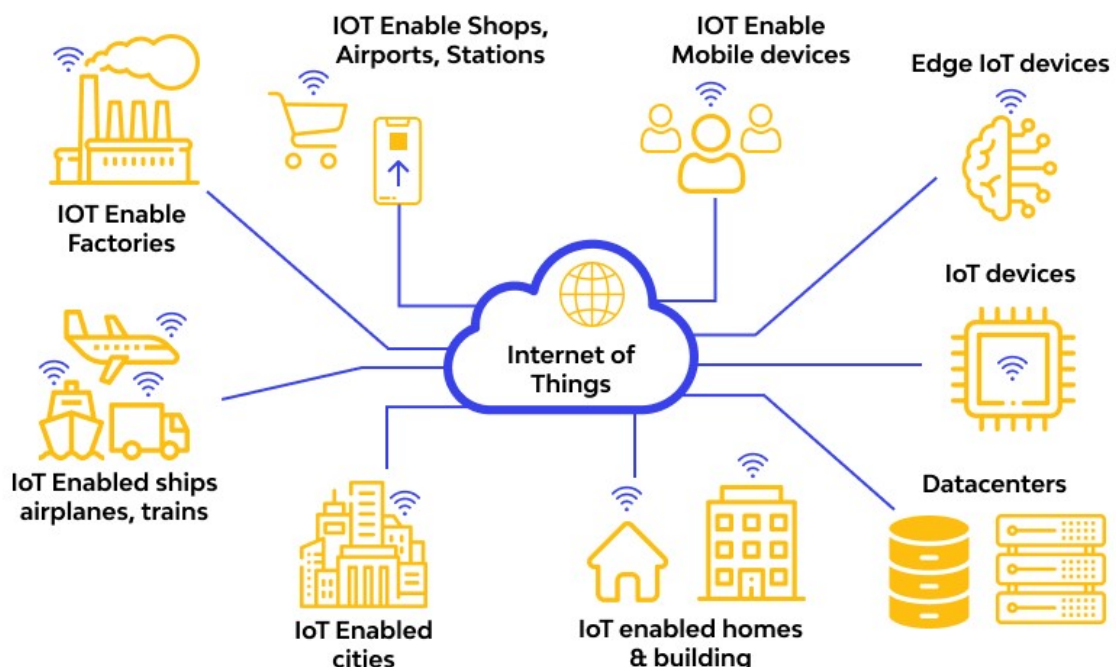


Рисунок 1.1 – Можливості запровадження IoT

Одним із найпереконливіших аспектів IoT є його здатність подолати розрив між цифровим і фізичним світами, створюючи симбіотичні відносини, які підвищують ефективність, зручність та продуктивність. Завдяки вбудованим датчикам і можливостям підключення в повсякденні об'єкти, IoT перетворює інертні пристрої на інтелектуальні, здатні збирати, аналізувати та передавати дані в режимі реального часу [21]. Цей підхід, що керується даними, відкриває безпрецедентне розуміння роботи нашого середовища, дозволяючи нам приймати більш обґрунтовані рішення, оптимізувати процеси та стимулювати інновації в різних сферах [17].

Як і інші пристрої, система розумного будинку має переваги, задля яких вона може бути встановлена [25]. Серед них:

- безпека;
- простота у використанні;
- гнучкість налаштувань;
- економія;
- автоматизація.

Безпека полягає у тому, що система має повний контроль над приміщеннями. Якщо буде здійснено незапланований доступ, вона надішле сповіщення. У разі виникнення надзвичайної ситуації «Розумний будинок» намагатиметься запобігти їм, в тому числі і виникненню пожеж.

Простота у використанні походить від того, що вся система управляється одним пристроєм. Найчастіше це мобільні телефони, або планшети.

Гнучкість системи дозволяє регулювати пристрої під себе, змінювати їх функції. Ви також можете додати до нього інші пристрої в будь-який час.

Економія ж виходить з того, що система розумного будинку зменшує комунальні платежі. Це тому, що система вимикає пристрої, які наразі не використовуються. Відповідно, знижується навантаження на мережу, а разом з нею і споживання електроенергії. Самі ж розумні пристрої споживають надзвичайно мало електроенергії. Економія на освітленні може досягати 40%, а на опаленні 30%.

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 6    |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

Автоматизація являється основною перевагою розумного будинку. Більшість предметів побуту можливо підключити до Розумного дому. Відповідно, це дає можливість контролювати їх автоматично, що економить багато часу [18].

Приклад застосування IoT у будинку зображено на рисунку 1.2.

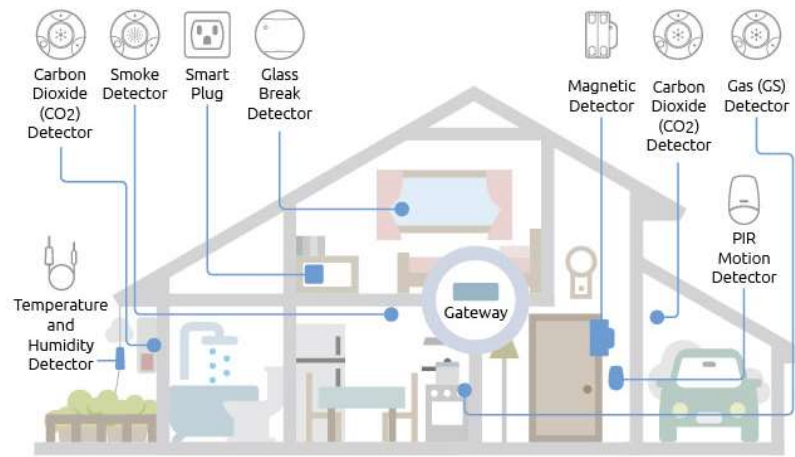


Figure: Smart Home Application

Рисунок 1.2 – Застосування IoT у будинку

Частіше усього, усі розумні девайси контролює “Gateway” або ж по-іншому – шлюз (Який також часто називають центральним контролером).

Шлюз IoT є ключовим вузлом, який з'єднує всі пристрої в мережі та з хмарою. Його робота включає кілька етапів, таких як збір, передача та обробка даних. Під час цього процесу шлюз IoT повинен взаємодіяти з різними гаджетами, щоб завантажити зібрані дані в хмару. Крім того, для цього необхідне надійне обладнання та програмне забезпечення [5].

Наприклад, він може забезпечувати дистанційне керування та контроль обладнання для забезпечення нормальної його роботи. У той же час він може фільтрувати та зберігати дані, покращувати їх якість і надавати підтримку для подальшого аналізу. Саме завдяки цим можливостям шлюз IoT став ключовим компонентом у сферах різноманітних галузей промисловості та розумних будинків (рисунок 1.3).

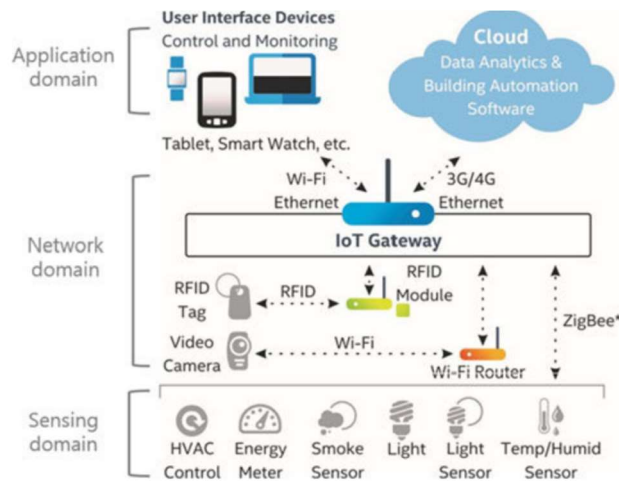


Рисунок 1.3 – Принцип роботи IoT контролера

Під час вибору найкращого шляху IoT необхідно враховувати численні критерії, включаючи сценарії застосування, кількість пристроїв, протоколи відповідного зв'язку, тощо [5].

## 1.2 Огляд наявних видів IoT пристроїв та їх використання

У мережах IoT використовуються різноманітні пристрої. Оскільки ця галузь постійно розвивається, щорічно з'являється все більше нових пристроїв, які претендують на впровадження новаторських та унікальних функцій у роботу системи. Давайте розглянемо найпопулярніші види таких пристроїв.

Сенсори та датчики – є невід'ємною складовою частиною Інтернету речей, які забезпечують збір інформації з навколишнього середовища та передають її для подальшого аналізу. Вони можуть бути встановлені на різних пристроях, починаючи від побутових, таких як холодильники та пральні машини, і закінчуючи промисловими об'єктами, наприклад, на фабриках та виробництвах [6].

Вони забезпечують збір інформації про різні параметри, такі як температура, вологість, освітленість, рух, звук та багато інших. Ця інформація передається через мережу інтернету до центральної системи, де проводиться аналіз та обробка даних. Прогноз популярності ринку таких датчиків зображено на рисунку 1.4.

|      |      |         |        |      |                          |           |
|------|------|---------|--------|------|--------------------------|-----------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>8 |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |           |

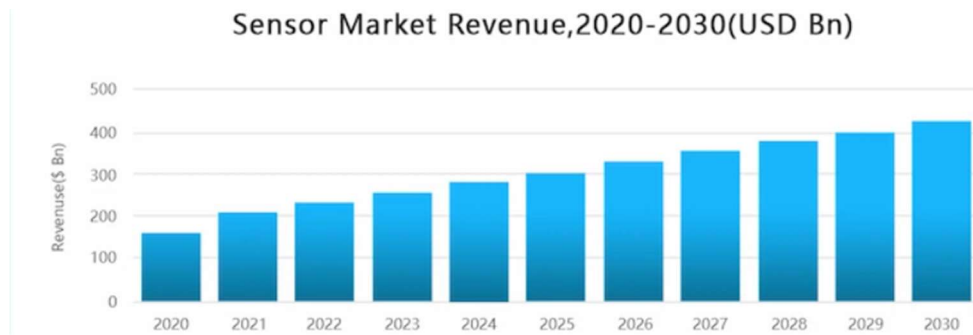


Рисунок 1.4 – Прогноз популярності ринку датчиків для IoT систем

PIR (пасивний інфрачервоний) датчик руху – є електронним пристроєм, який виявляє рух шляхом реагування на зміни в інфрачервоному випромінюванні, яке виділяються тілами з температурою, подібною до температури людини. Вони реагують на теплове випромінювання, що видають об'єкти при їхньому переміщенні у полі зору датчика. PIR датчики руху широко застосовуються в системах безпеки, освітленні та автоматизації будівель, а також в електронних системах безпеки автомобілів. Наприклад, PIR датчик може бути використаний для автоматичного увімкнення світла при вході людини до приміщення [8]. Для цього йому зовсім не обов'язково бути з'єднаним з джерелом світла за допомогою проводів, частіше усього такий тип взаємодії створений за допомогою сценарію IoT (рисунок 1.5).

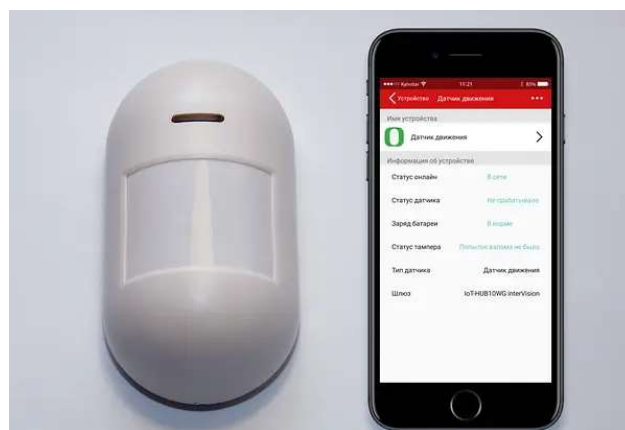


Рисунок 1.5 – PIR Датчик руху для “Розумного будинку”

Дверні магнітні датчики – це пристрої, які використовуються для виявлення відкриття або закриття дверей, вікон або інших механізмів. Вони складаються з

двох основних компонентів: магнітного контакту та магнітного датчика. Коли двері або вікно зачинені, магнітний контакт знаходиться вблизьку від магнітного датчика і замикання між ними встановлює замкнене становище. Якщо двері або вікно відкриваються, магнітний контакт віддаляється від датчика, що призводить до відкритого стану. Цей процес викликає зміну в сигналі датчика, яку можна використовувати для активації систем безпеки, освітлення або інших автоматизованих пристроїв (рисунок 1.6).



Рисунок 1.6 – Дверні магнітні датчики

(IoT) вимикач – це електричний вимикач, який може бути віддалено керований. Цей вимикач може бути підключений до мережі Wi-Fi або іншої мережі зв'язку, що дозволяє користувачам віддалено вмикати або вимикати електричні пристрої чи системи.

Зазвичай вони працюють в парі з мобільним додатком або веб-панеллю, де користувач може керувати станом вимикача, навіть якщо він знаходиться на відстані від пристрою. Це дозволяє зручно керувати освітленням, побутовими приладами, системами опалення та кондиціонування повітря та іншими пристроями, навіть коли ви поза домом. Такий вимикач зображено на рисунку 1.7.

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 10   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

Aqara РОЗУМНИЙ ВИМИКАЧ D1



Рисунок 1.7 – Розумний вимикач

Головним компонентом системи «розумний дім», який об'єднує всі розумні прилади в єдину мережу є центральний контролер.

Центральний контролер розумного будинку – це центральний пристрій або система, яка координує роботу різних розумних пристроїв у вашому будинку. Він служить як мозок системи, забезпечуючи взаємодію між різними пристроями та їхнє керування. Основні функції центрального контролера зображено у таблиці 1.1, а приклад зовнішнього вигляду такого контролера показано на рисунку 1.9.

Таблиця 1.1 – Функції центрального контролера

| Функції              | Опис  |
|----------------------|---|
| 1                    | 2   |
| Керування пристроями | Дозволяє вам взаємодіяти з різними розумними пристроями у вашому будинку, такими як розумні розетки, термостати, датчики руху тощо. |
| Автоматизація        | Можливість програмувати різні сценарії та розклади для автоматизації роботи розумних пристроїв                                      |

Кінець таблиці 1.1

| 1   | 2   |
|---|---|
| Моніторинг і управління енергоспоживанням | Надає інформацію про споживання енергії різними пристроями і допомагає вам ефективно керувати енергоефективністю вашого будинку                                     |
| Інтеграція з іншими системами             | Інтеграція з іншими розумними системами, такими як системи безпеки, освітлення, аудіо- та відеосистеми, що дозволяє створювати повноцінну систему розумного будинку |
| Віддалений доступ                         | Дозволяє керувати розумним будинком віддалено через мобільний додаток чи веб-інтерфейс.   |

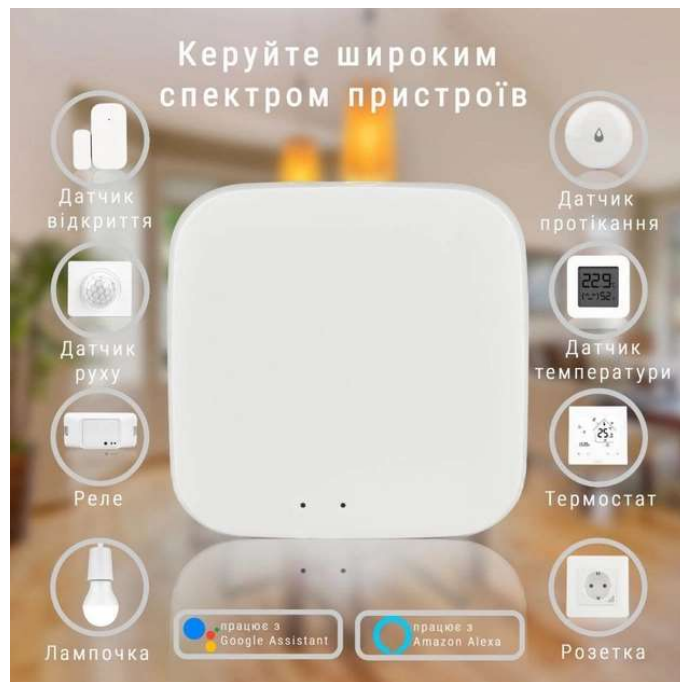


Рисунок 1.9 – Центральний контролер для розумного будинку

### 1.3 Аналіз існуючих варіантів підключення IoT пристроїв до мережі

За типом підключення існує дротове та бездротове підключення. Бездротове та дротове підключення пристроїв до мережі Інтернету речей (IoT) мають свої власні переваги та недоліки, які варто враховувати при виборі методу підключення. Переваги і недоліки такого підключення зображено у таблиці 1.2.

Таблиця 1.2 – Переваги і недоліки бездротового підключення

| Бездротове підключення     |                              |
|----------------------------|------------------------------|
| Переваги                   | Недоліки                     |
| Гнучкість в установці      | Обмежена зона покриття       |
| Простота розширення мережі | Збільшене споживання енергії |
| Мобільність                | Менша безпека                |

Перевагами бездротового підключення є:

- гнучкість в установці;
- простота розширення мережі;
- мобільність.

Гнучкість в установці полягає у тому, що бездротові пристрої можуть бути розміщені в будь-якому місці без необхідності проведення дротів, що забезпечує більшу гнучкість в розташуванні пристроїв.

Через те що усі девайси підключені безпроводним шляхом, додавання нових бездротових пристроїв до мережі може бути здійснене швидко та без необхідності проведення додаткових кабелів.

Також перевагою є і мобільність, оскільки бездротові пристрої можуть легко переміщатися з місця на місце, що дозволяє їх використання в різних локаціях без прив'язки до кабельної інфраструктури.

Але при цьому, воно має і свої недоліки:

- обмежене покриття;
- збільшене споживання енергії;

– менша безпека.

Сигнал бездротової мережі може бути обмеженим стінами або іншими перешкодами, що може призвести до обмежень у покритті мережі.

Збільшення споживання енергії полягає у тому, що бездротові пристрої зазвичай споживають більше енергії, оскільки потребують постійного підтримання бездротового зв'язку.

Також, бездротові мережі можуть бути вразливими до кібератак і перехоплення даних порівняно з дротовими мережами, що є дуже небезпечним [40]. Переваги і недоліки дротового підключення зображено у таблиці 1.3.

Таблиця 1.3 – Переваги і недоліки дротового підключення

| Дротове підключення           |                                    |
|-------------------------------|------------------------------------|
| Переваги                      | Недоліки                           |
| Стабільність зв'язку          | Складність установки та розширення |
| Вища швидкість передачі даних | Обмежена гнучкість                 |
| Більша безпека                | Вищі витрати                       |

Дротове підключення в свою чергу має наступні переваги:

- стабільність зв'язку;
- вища швидкість передачі даних;
- більша безпека.

Дротові мережі забезпечують більш стабільний та надійний зв'язок, оскільки вони не піддаються впливу перешкод або інтерференції.

Також, дротові з'єднання зазвичай мають вищу швидкість передачі даних порівняно з бездротовими з'єднаннями.

Безпековий аспект полягає у тому, що дротові з'єднання зазвичай більш захищені від кібератак та перехоплення даних порівняно з бездротовими системами та мережами.

Але при цьому має такі недоліки:

- складність установки та розширення;
- обмежена гнучкість;
- вищі витрати.

Установка та розширення дротової інфраструктури може бути більш складною та витратною через необхідність проведення кабелів.

Обмежена гнучкість полягає у тому, що дротові пристрої мають обмежену мобільність та можуть бути обмежені фізичними межами кабельної інфраструктури.

Також варто зазначити що вартість проводки яка необхідна для встановлення таких пристроїв є надзвичайно великою, в порівнянні з звичайним бездротовим з'єднанням.

Враховуючи усі плюси і мінуси обидвох варіантів, можна зробити висновок, що бездротове підключення є кращим за дротове, у питанні мережі розумного будинку [11, 40]. А використання комбінованого підключення – буде найбільш оптимальним варіантом. Порівняння обох видів підключення зображено у таблиці 1.4.

Таблиця 1.4 – Порівняння бездротового та дротового з'єднання

|                            | Бездротове  | Дротове   |
|----------------------------|---|---|
| Стабільність зв'язку       | Стабільність залежить від відстані пристрою до контролера | Зв'язок однаково стабільний на будь-якій відстані |
| Гнучкість                  | +   | –   |
| Простота розширення мережі | +   | –   |
| Мобільність                | +   | –   |
| Площа покриття             | Відносно мала (до 100м)                                   | Велика(від 100м)                                  |
| Витрати                    | Достатньо малі  | Великі(ціна проводки)                             |

Бездротові технології підключення IoT пристроїв також суттєво відрізняються. Відрізняють такі технології (протоколи) бездротового підключення для IoT пристроїв [14]:

- Zigbee;
- Z-Wave;
- BLE Bluetooth Low Energy;
- RBF (протокол під 1 ГГц);
- MQTT (Використовується IoT пристроями Cisco);

Розглянемо кожен з них більш детально:

Протокол Zigbee – це протокол, який використовується для бездротового зв'язку між розумними пристроями. Це описано в стандарті IEEE 802.15.4 і працює в неліцензійних смугах 868 МГц, 902–928 МГц і 2,4 ГГц. Він належить до PAN (Personal Area Network), подібно до відомої технології Bluetooth. До основних переваг Zigbee можна віднести його надійність, невибагливість і дуже низьке споживання енергії. Оскільки протокол орієнтований на дуже низьке енергоспоживання, відстань передачі обмежена приблизно 10–100 метрами, залежно від навколишнього середовища. Мережа Zigbee захищена 128-бітним симетричним ключем шифрування, тому вам не доведеться турбуватися про безпеку. Мінусом Zigbee є те, що неможливо з'єднати пристрої на більшій відстані ніж 100 метрів. Це проблема, яку вирішують маршрутизатори. Таким чином, сигнал поступово проходить через декілька пристроїв на більшу відстань [4]. Приклад Zigbee Mesh-мережі зображено на рисунку 1.10.

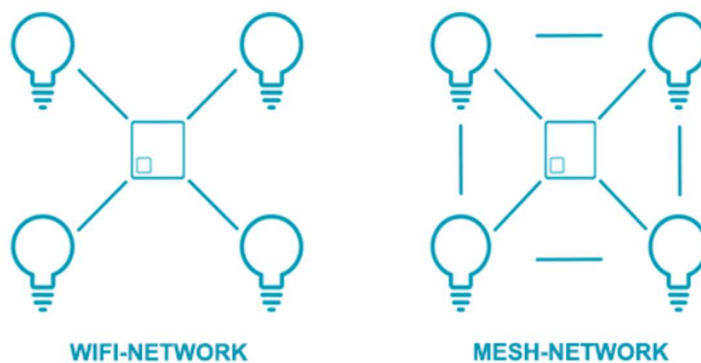


Рисунок 1.10 – Mesh-мережа

Чим більше таких вузлів у мережі Zigbee, тим вона стабільніша. Ця технологія також відрізняється високою масштабованістю, надійністю зв'язку та можливістю створювати різноманітні топології мереж. Вона підтримує різні типи мереж, такі як мережі "зірка", "маршрутизовані мережі" та "мега-зірка", що дозволяє адаптувати її для різних потреб та сценаріїв застосування.

Протокол Z-Wave – це радіо протокол, який спочатку замислювався для використання у домашній автоматизації. В Україні працює на частоті 869 МГц, що дає хорошу перешкодозахищеність від Wi-Fi мереж 2.4 ГГц і сигналізацій 433 МГц. Чіпи для Z-Wave пристроїв виготовляє компанія Silicon Labs, а протокол є суворо стандартизованим від фізичного рівня передачі даних до прикладного рівня. Всі пристрої Z-Wave проходять обов'язкову сертифікацію, яку контролює Z-Wave Alliance. Сертифікація гарантує сумісність усіх пристроїв Z-Wave всіх виробників у світі. На даний момент (2024 р.) до Z-Wave Alliance входить понад 730 компаній, що виробляють понад 5000 сумісних між собою пристроїв. Завдяки протоколу "mesh", Z-Wave може створювати динамічні мережі, які легко адаптуються до змін у середовищі. Одним з важливих плюсів є його відкритість та сумісність з різноманітними пристроями від різних виробників, що робить його досить універсальним вибором для систем розумного будинку. Z-Wave чудово справляється з керуванням десятками освітлювальних приладів, (плавно димувати світильник, налаштовувати колір LED стрічки, керувати світлом у коридорі з різних місць) але не призначений для керування освітленням на стадіоні з потужним навантаженням та на великій відстані [20].

Технологія BLE (Bluetooth Low Energy) – Основна особливість BLE полягає в здатності забезпечувати довготривалу роботу пристроїв з низьким споживанням енергії. Крім того, BLE забезпечує широкий радіус дії та може працювати в режимі "сон" до виникнення події, що дозволяє зберігати заряд батареї. Завдяки своїй низькій енергоспоживаності, BLE може використовуватися в різних сферах IoT. Хоча технологія BLE має багато переваг, вона також має деякі недоліки. Наприклад, обмежена швидкість передачі даних може ускладнити використання для деяких застосувань, особливо тих, що потребують великого

|      |      |         |        |      |                          |            |
|------|------|---------|--------|------|--------------------------|------------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>17 |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |            |

обсягу даних. Також, радіус дії BLE може бути обмеженим порівняно з іншими технологіями, такими як Wi-Fi, що може створити проблеми для деяких сценаріїв IoT. Також важливо враховувати, що низька споживання енергії та довга тривалість роботи можуть мати свою ціну в обмеженій пропускній здатності та можливостях взаємодії з іншими пристроями [34].

Протокол RBF (Radio Bearer Frame) – є одним із протоколів, призначених для бездротового зв'язку на частотах нижчих, ніж 1 ГГц. Ця технологія може використовуватися в різних бездротових мережах, таких як мережі IoT або бездротові мережі сенсорів. Основною особливістю протоколу RBF є його здатність працювати на низьких частотах, що може забезпечити більший радіус дії та кращу проникність через перешкоди порівняно з вищими частотами. Такий протокол може бути корисним для сценаріїв, де потрібно забезпечити зв'язок на великих відстанях або через товсті стіни. Однак, варто враховувати, що низькі частоти можуть мати обмежену пропускну здатність та меншу швидкість передачі даних порівняно з вищими частотами.

MQTT (Message Queuing Telemetry Transport) – це легковаговий протокол повідомлень, розроблений для передачі повідомлень між пристроями через мережі з низькою пропускну здатністю та/або ненадійним зв'язком. Основна ідея MQTT полягає в тому, щоб дозволити пристроям ефективно обмінюватися невеликими обсягами даних, зменшуючи навантаження на мережу та споживання енергії. Протокол MQTT працює на основі моделі "публікація–підписка", де пристрої підписуються на певні теми та отримують повідомлення, які опубліковані в цих темах. Цей протокол широко використовується в різних сферах, включаючи Інтернет речей (IoT), де ефективний обмін даними між пристроями відіграє ключову роль. MQTT підтримує різні механізми безпеки, включаючи шифрування TLS (Transport Layer Security) для безпечного обміну даними по мережі. Це гарантує, що повідомлення, якими обмінюються пристрої, зашифровані, запобігаючи несанкціонованому доступу або підробці даних, що робить його надійним протоколом [22, 31].

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>18 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |

## 1.4 Формування вимог для розробки IoT–мережі для системи “Розумний заміський будинок”

Оскільки метою цієї роботи є створення IoT–мережі для розумного будинку, необхідно сформулювати вимоги для її розробки. Такі вимоги можна сформулювати після опрацювання теоретичних та практичних відомостей стосовно мереж для розумних будинків. Давайте виділимо основні вимоги до мережі.

Однією з вимог є надійність підключення. Усі пристрої у мережі повинні надійно підключатись один до одного, з забезпеченням хорошого рівня сигналу, якщо це бездротове підключення, або за допомогою якісної проводки, якщо це звичайне дротове підключення.

Також, зручність використання. Усі кінцеві розумні пристрої мають легко налаштовуватись, тобто у мережі має забезпечуватись легкий доступ користувача до їх налаштувань та сценаріїв.

Обов’язкова також і наявність збереження даних. IoT система повинна мати можливість зберігати дані, або локально, або за допомогою хмарних технологій. Це необхідно як для аналізу мережі, так і для збереження налаштувань пристроїв, та розроблених користувачем сценаріїв.

Потрібно мати і віддалений доступ. Користувач має мати можливість підключення до мережі віддалено, будучи на роботі, або у будь–якому другому місці. Таке підключення має відбуватися через інтернет, і реалізовуватися як підключення або до хмари, або як підключення до серверу IoT напряду.

Система має підтримувати розробку сценаріїв. Сценарії є невід’ємною частиною будь–якої IoT мережі. Власник мережі має мати можливість створення кастомних сценаріїв для своєї системи, для задоволення своїх потреб.

Також, система повинна ефективно використовувати енергію. Дана система повинна ефективно використовувати електроенергію, особливо якщо деякі кінцеві пристрої встановлюються в важкодоступних місцях. Це може включати в себе як розробку енергозберігаючих сценаріїв, так і використання більш енерго–економлячих протоколів бездротового зв’язку.

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 19   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

Інтеграція з іншими пристроями також є дуже важливою. IoT мережа має підтримувати якомога більше пристроїв від різних виробників, для забезпечення її гнучкості використання.

Усе апаратне забезпечення у мережі має бути замінне. Усі пристрої у мережі мають бути легко замінними на інші. Таким чином мережа стає надзвичайно гнучкою, через підтримку широкого спектру пристроїв.

Система має легко масштабуватись, наприклад за допомогою підключення до неї нових пристроїв. Ці підключення мають відбуватися легко та без перешкод.

### 1.5 Постановка задачі

Постановка задачі вміщує в себе наступні етапи проектування та конфігурації IoT мережі:

- аналітичний огляд існуючих сучасних рішень;
- проектування мережі відповідно до плану заміського будинку;
- підбір необхідних пристроїв, для більш надійної/бюджетної мережі;
- конфігурація та підключення пристроїв;
- розробка сценаріїв поведінки пристроїв;
- розрахунок матеріальних витрат для обох версій мережі;
- тестування мережі та перевірка її ефективності;
- оформлення звіту за результатами дослідження.

Виконання усіх перерахованих етапів розробки мережі дозволяє досягти мети роботи – спроектувати та сконфігурувати IoT мережу для системи “Розумний заміський будинок” та виконати її експериментальну перевірку.

### 1.6 Висновки

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 20   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

Було проаналізовано предметну область, та визначено переваги та можливості встановлення системи IoT, серед яких: Автоматизація, простота у використанні, та економія.

Були проаналізовані різноманітні IoT пристрої, їх сфера використання, та їх різновиди. Після детального аналізу даних пристроїв, було визначено такі обов'язкові IoT девайси, як центральний IoT контролер та модуль реле, який дозволяє котролювати електричне навантаження. Інші кінцеві пристрої будуть обрані відповідно до плану будинку та вимог користувача.

Проаналізовано переваги та недоліки дротового та бездротового підключення пристроїв до IoT мережі. Тому, враховуючи усі їх особливості, було вирішено використовувати комбіновану систему підключень, для забезпечення найоптимальнішого рівня сигналу.

Виявлено що існує велика кількість протоколів для обміну даними між бездротовими розумними пристроями. Цими протоколами є протоколи Zigbee, Z-Wave, технологія BLE (Bluetooth Low Energy), протокол RBF (Radio Bearer Frame), MQTT (Message Queuing Telemetry Transport). Серед них, Zigbee являється більш вузько-спеціалізованим ніж Z-Wave, але це не робить його гіршим. Протокол MQTT виявлено як один з найпростіших та найшвидших протоколів.

Мета кваліфікаційної роботи – проектування та конфігурація IoT мережі для системи “Розумний заміський будинок”.

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 21   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

## 2 АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ТА ВИБІР ПІДХОДУ ДЛЯ ВИРІШЕННЯ ПОСТАВЛЕНОЇ ЗАДАЧІ

### 2.1 Огляд існуючих рішень для створення системи "Розумний будинок"

На сьогоднішній день існує багато рішень для створення систем "Розумний будинок", які забезпечують автоматизацію та контроль над різними аспектами домашнього середовища. Системи "Розумний будинок" включають в себе різноманітні компоненти, такі як розумні термостати, освітлення, безпека, енергозбереження та багато інших, що працюють на певних технологіях.

Серед популярних рішень можна виділити такі технології, як Zigbee, Z-Wave, Wi-Fi та Bluetooth Low Energy (BLE), які ми вже обговорювали у попередньому розділі. Кожна з яких має свої унікальні переваги та особливості. Деякі компанії пропонують інтегровані рішення, які поєднують в собі різні протоколи та забезпечують зручне управління за допомогою мобільних додатків або голосових помічників.

Оглянемо технологію Zigbee більш детально. На ринку існує багато компаній, які випускають пристрої з технологією Zigbee для систем розумного будинку. Деякі з найбільш відомих і найпопулярніших компаній в цій галузі включають Philips (з їх серією Philips Hue), Xiaomi (з їх серією Xiaomi Smart Home), Samsung (серія Samsung SmartThings), IKEA (з їх серією TRÅDFRI) та деякі інші. Кожна з цих компаній має свої унікальні пристрої та екосистеми, але серед них немає однозначного "найкращого" виробника. Вибір найкращого пристрою залежить від конкретних потреб та вимог користувача.

Основна відмінність між протоколами Z-Wave і Zigbee полягає в їх технічних характеристиках та характеристиках мережі. Зокрема, Z-Wave використовує частоту 900 МГц, що забезпечує кращу проникність через стіни та більший радіус дії порівняно з Zigbee, який працює на частоті 2,4 ГГц.

Особливості пристроїв Z-Wave включають високу стандартизацію, що забезпечує сумісність між пристроями різних виробників, та низьке споживання

|      |      |         |        |      |                          |            |
|------|------|---------|--------|------|--------------------------|------------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>22 |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |            |

енергії. Крім того, мережі Z-Wave можуть автоматично налаштовуватися та оптимізуватися для кращої працездатності.

Bluetooth Low Energy (BLE) – Основна відмінність між технологіями Bluetooth Low Energy (BLE), Z-Wave і Zigbee полягає у тому, що BLE відрізняється низьким споживанням енергії та широкою підтримкою мобільних пристроїв. Проте, в порівнянні з Z-Wave та Zigbee, BLE має обмежений радіус дії та меншу пропускну здатність, що робить його менш підходящим для великих систем розумного будинку.

MQTT (Message Queuing Telemetry Transport) – Виробниками пристроїв які підтримують цей протокол є Cisco, Philips, Samsung, Xiaomi, Bosch, Honeywell, та інші. Основна відмінність між протоколом MQTT та Zigbee або Z-Wave полягає в їх архітектурі та принципах роботи. MQTT – це протокол повідомлень, який дозволяє пристроям обмінюватися даними через мережу Інтернет. Він базується на моделі "публікація-підписка", що дозволяє пристроям підписуватися на певні теми та отримувати повідомлення, які опубліковані в цих темах. MQTT не був спеціально розроблений для використання в мережах Інтернету речей, але зазвичай використовується саме в таких системах.

Тепер розглянемо особливості усіх протоколів, які можуть відіграти дуже важливу роль при побудові IoT-мережі.

Те, що пристрої використовують протокол Zigbee, далеко не означає що вони всі будуть добре і злагоджено працювати між собою. Хоча протокол Zigbee й забезпечує стандартизовану специфікацію, яка дозволяє пристроям різних виробників працювати разом, на практиці існують деякі обмеження.

Сумісність між пристроями Zigbee залежить від того, чи вони використовують однакові профілі та версії стандарту Zigbee. Протокол включає в себе різні профілі, такі як Zigbee Home Automation, Zigbee Light Link, Zigbee Smart Energy, тощо. Якщо пристрої підтримують однаковий профіль та версію, вони зазвичай будуть сумісні між собою. Однак, якщо пристрої використовують різні профілі або версії, їх сумісність може бути обмеженою або відсутньою.

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 23   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

І навіть при однакових версіях Zigbee, пристрої всеодно можуть не розпізнаватися додатком, або центральним контролером, адже їх сумісність також залежить від виробника, та того факту, чи підтримуються вони додатком. Те ж саме стосується і пристроїв Z-Wave.

Це саме стосується й BLE. Те, що пристрої використовують технологію Bluetooth Low Energy (BLE), не гарантує автоматичну сумісність та можливість взаємодії між собою. Різні виробники впроваджують різні профілі та характеристики, що може призвести до несумісності між пристроями. Крім того, можливі різні рівні підтримки функцій та версій специфікації BLE.

Отже, пристрої на основі технології Zigbee можуть бути хорошим бюджетним варіантом для систем розумного будинку. Zigbee забезпечує надійний та ефективний бездротовий зв'язок за доступну ціну, що робить його привабливим варіантом для більшості користувачів. Одною з переваг цього протоколу є “меш” зв'язок, який дозволяє посилювати сигнал без наявності точок підсилення, адже кожен з пристроїв буквально виступає однією з них (рисунок 2.1).

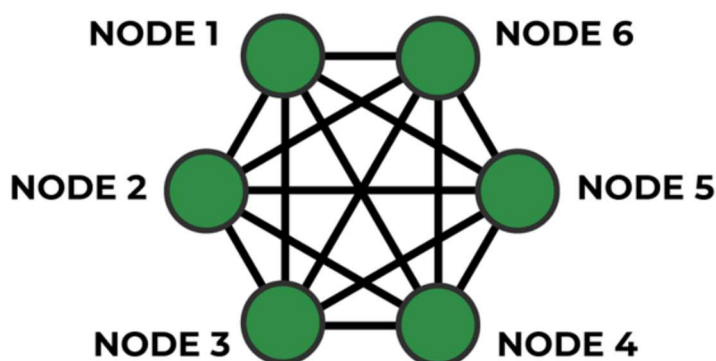


Рисунок 2.1 – Візуальна репрезентація роботи Mesh мережі

Натомість, пристрої з використанням протоколу MQTT можуть бути дуже надійними, але вони зазвичай є дорогими, так як MQTT – це високопродуктивний протокол повідомлень, який часто використовується в промислових системах, а основний виробник пристроїв з підтримкою цього протоколу – компанія Cisco. Він забезпечує надійну передачу даних та високий рівень безпеки, але його використання може бути витратним (рисунок 2.2).

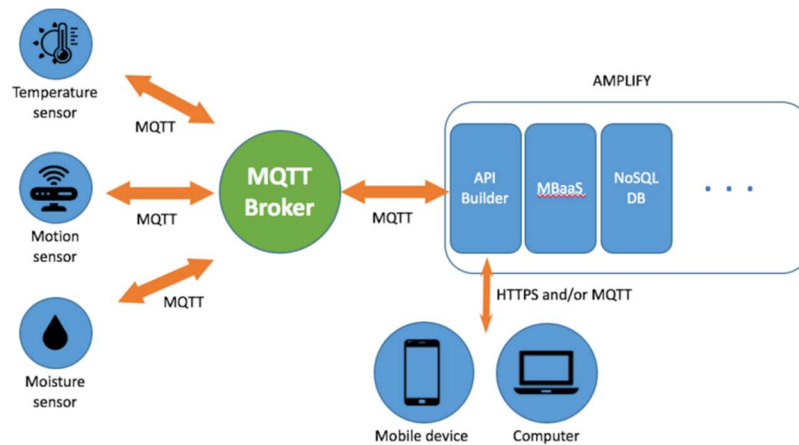


Рисунок 2.2 – Візуальна репрезентація принципу роботи MQTT мережі

Основними платформами для керування IoT-девайсами, які підтримують пристрої з протоколом Zigbee є Tuuya Inc, Xiaomi, та Samsung. Розберемося в них більш детально:

Tuuya Smart Home – це платформа для розумного будинку, яка надає рішення з підключення, управління та автоматизації пристроїв у вашому домі через Інтернет.

Платформа Tuuya дозволяє виробникам створювати різноманітні пристрої, такі як розумні розетки, лампи, датчики, камери безпеки та інші, які можна легко підключити до системи розумного будинку.

Платформа Tuuya Smart Home стала популярною завдяки своїй простоті використання, широкому спектру сумісних пристроїв і доступності для виробників та споживачів.

Користувач може підключитися до своїх пристроїв, крім локальних Bluetooth, з будь-якої точки світу або отримувати миттєві Push-сповіщення на телефон. Швидкодія відгуку в додатку цілком непогана, та й повідомлення надходять миттєво. Якщо порівнювати з Mi Home від Xiaomi – Tuuya має явну перевагу у цьому питанні. Але все залежить від Інтернету, до якого підключається пристрій та до якого підключений смартфон, та й на магістралі бувають затримки [3]. Можливості додатку Tuuya Smart Home зображено на рисунку 2.3.

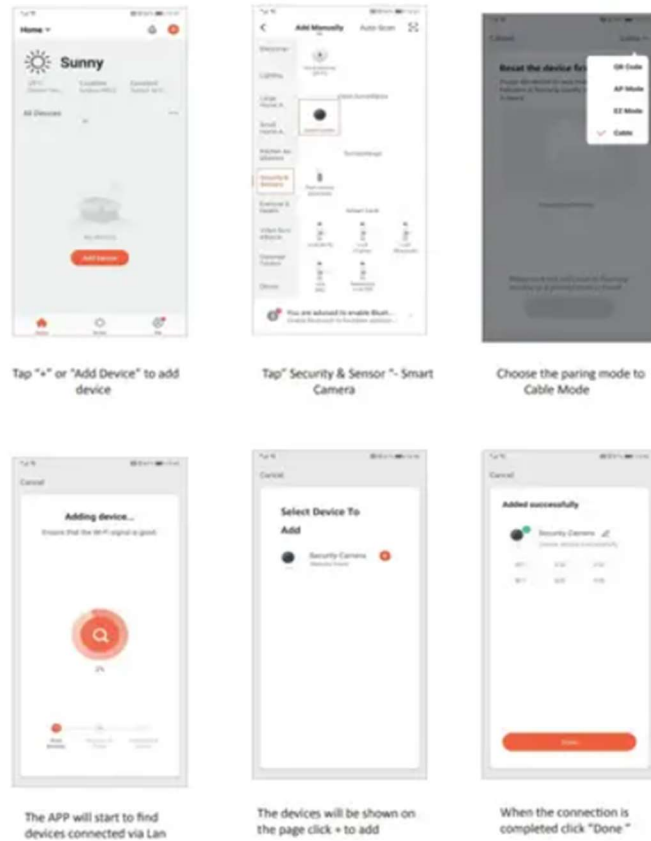


Рисунок 2.3 – Можливості додатку TuYa Smart Home

Тепер давайте розглянемо Mi Home від Xiaomi. Mi Home – це така ж система, завдяки якій можна з'єднати між собою різні пристрої квартири чи будинку, а також автоматизувати та контролювати їхню роботу. Сам функціонал не сильно відрізняється від TuYa Smart Home, але все ж має свої недоліки, які роблять Mi Home не дуже хорошим вибором. Не дивлячись на те, що розумні пристрої Xiaomi підтримують інтеграції з іншими системами розумних будинків, вони не завжди коректно працюють, а інколи й зовсім не відображаються у контрольній панелі. Воно й зрозуміло – в першу чергу, Mi Home створено для управління пристроями Xiaomi, а інтеграція з іншими пристроями, звичайно ж, відходить на другий план, і не гарантує коректної роботи даних пристроїв [39]. Можливості додатку Mi Home зображено на рисунку 2.4.

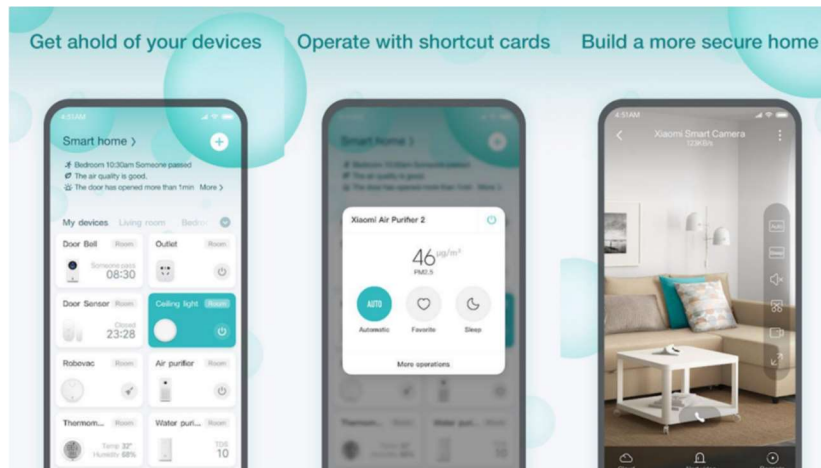


Рисунок 2.4 – Можливості додатку Mi Home

Тепер розглянемо платформу, для управління пристроями які працюють використовуючи MQTT протокол – Cisco Asset Vision.

Cisco Asset Vision – це інноваційна платформа для моніторингу, управління та аналізу пристроїв у мережі в реальному часі. Ця система розроблена компанією Cisco для підприємств та людей, які бажають оптимізувати управління своїми пристроями, забезпечити ефективність їхньої роботи, та відслідковувати їх стан.

Зберігає усю інформацію про пристрої у хмарі або локально, що превентує втрату інформації після того як пристрій вийде з ладу. Можливості платформи зображено на рисунку 2.5.

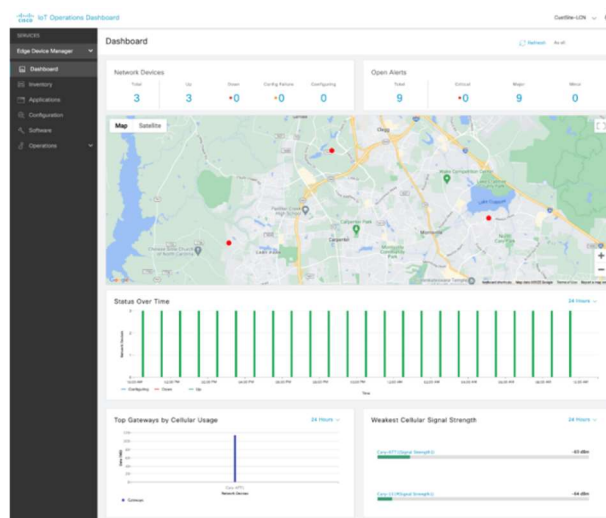


Рисунок 2.5 – Можливості платформи Cisco Asset Vision

## 2.2 Порівняльний аналіз переваг та недоліків існуючих рішень

|      |      |         |        |      |
|------|------|---------|--------|------|
|      |      |         |        |      |
| Зм.. | Арк. | №докум. | Підпис | Дата |

Обираючи лише одну платформу для створення системи розумного будинку, користувач отримує декілька переваг, які зроблять його систему набагато надійнішою та ефективнішою.

По–перше, використання лише однієї платформи спрощує процес управління та підтримки системи. Користувачам не потрібно переключатися між різними додатками та сервісами, щоб керувати своїми пристроями.

По–друге, використання однієї платформи забезпечує більшу сумісність та стабільність системи. Проблеми з несумісністю та конфліктами між пристроями можуть виникнути, якщо використовуються пристрої з різних платформ.

Нарешті, обираючи лише одну платформу, користувач може отримати більше функцій та можливостей для автоматизації свого будинку, оскільки виробники пристроїв часто пропонують розширені функції для власних платформ. Тому у результаті порівняння буде обрано лише одну платформу.

Давайте порівняємо платформи Mi Home, TuYa Smart Home та Cisco Assset Vision (таблиця 2.1).

Таблиця 2.1 – Переваги і недоліки платформи TuYa Smart Home

| Переваги                         | Недоліки                          |
|----------------------------------|-----------------------------------|
| Широкий вибір сумісних пристроїв | Обмежені можливості автоматизації |
| Простота використання            | Приватність даних під сумнівом    |
| Віддалений доступ                | Залежність від хмарних сервісів   |
| Низька вартість                  | –                                 |

TuYa Smart Home має значну кількість переваг, серед яких можна виділити широкий вибір сумісних пристроїв, так як платформа підтримує велику кількість пристроїв інших виробників, простоту використання – адже інтерфейс у додатку є інтуїтивним, та одразу зрозумілим користувачу, а також одна з основних переваг – це низька вартість пристроїв, що робить їх доступними для будь–кого.

Тепер відокремимо переваги і недоліки платформи Mi Home. Недоліки і переваги цієї платформи зображено у таблиці 2.2.

Таблиця 2.2– Переваги і недоліки платформи Mi Home

| Переваги                           | Недоліки                              |
|------------------------------------|---------------------------------------|
| Широкий вибір сумісних пристроїв   | Обмеженість функцій в деяких регіонах |
| Інтеграція з екосистемою Xiaomi    | Приватність даних під сумнівом        |
| Розширені можливості автоматизації | Залежність від екосистеми Xiaomi      |
| Низька вартість                    | Не інтуїтивність використання         |

Mi Home в аспекті переваг майже не відрізняється від TuYa Smart Home, але має набагато більше недоліків, серед яких варто виділити залежність від екосистеми Xiaomi, та обмеженість функцій в деяких регіонах. Залежність від екосистеми Xiaomi є мінусом, оскільки сам додаток підтримує тільки пристрої з цієї екосистеми, в цей ж час дозволяючи іншим платформам розпізнавати свої пристрої. Тобто, більш оптимальним варіантом буде використовувати іншу платформу, як ось наприклад TuYa Smart Home, та під'єднувати до неї пристрої компанії Xiaomi.

Повернемося до Cisco Asset Vision. Переваги та недоліки даної платформи зображено у таблиці 2.3

Таблиця 2.3 – Переваги і недоліки платформи Cisco Asset Vision

| Переваги                           | Недоліки                    |
|------------------------------------|-----------------------------|
| Інтеграція з екосистемою Cisco     | Високі витрати              |
| Розширені можливості безпеки       | Складність в налаштуванні   |
| Розширені можливості автоматизації | Залежність від мережі Cisco |
| Гнучкість та масштабованість       | –                           |

Хоча й Cisco Asset Vision не є бюджетним варіантом для більшості людей, надійність самих пристроїв Cisco, розширені можливості автоматизації, та гнучкість самої системи робить її варіантом який варто розглянути. Користувач буде мати повний контроль над усією екосистемою розумного будинку, та може

не хвилюватися про її безпеку та надійність. Усі пристрої від компанії Cisco надзвичайно надійні, адже зроблені з якісних матеріалів, що гарантує довготривалість служби та відсутність зносу. Враховуючи те, що Cisco являється провідним виробником мережевих пристроїв, це робить інтеграцію IoT девайсів у дану екосистему надзвичайно простою. Cisco Asset Vision підтримує складні сценарії, та віддалене керування та контроль, а також відстеження докладної статистики виникнення збоїв, та сили сигналу девайсів. Наприклад, тут навіть є можливість відстеження сили мобільного сигналу, якщо система IoT під'єднана до мобільного інтернету, замість звичайного постачальника інтернет послуг (рисунок 2.6).

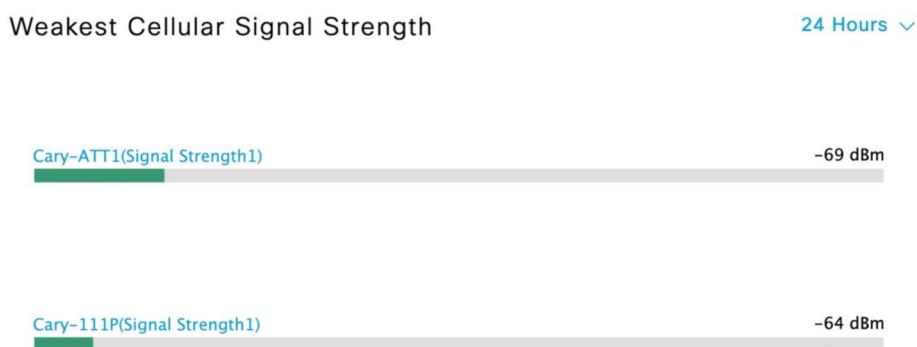


Рисунок 2.6 – Відображення сили мобільного сигналу у Cisco Asset Vision

Користувач має доступ до великої кількості різних графіків і статистик, що дозволяє одразу виявити проблему при виникненні якогось збою. Так як Cisco Asset Vision в основному розрахований на використання бізнесменами, у яких є свій бізнес, Cisco Asset Vision дозволяє контролювати пристрої не тільки у своєму будинку, але й, наприклад, у своєму офісі, що робить дану платформу надзвичайно гнучкою та з можливістю легкого масштабування (рисунок 2.7).

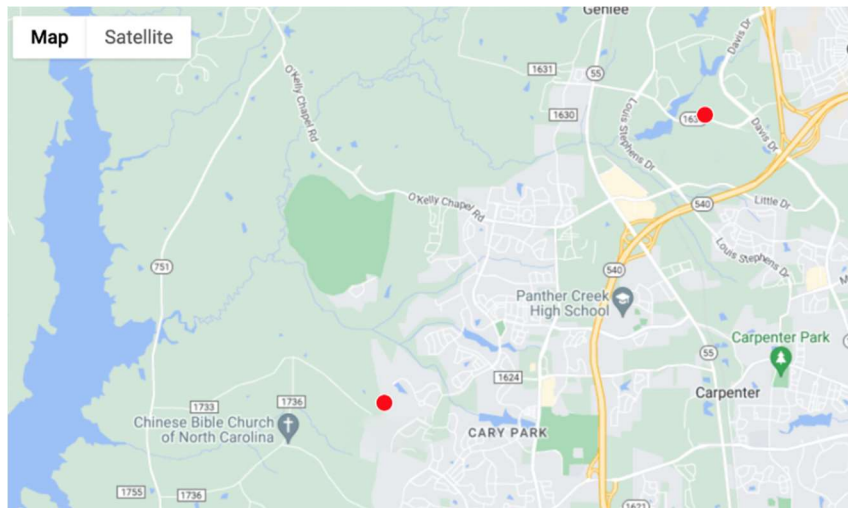


Рисунок 2.7 – Можливість відстеження пристроїв у будь-якій точці світу

Так як усі IoT пристрої чудово інтегруються з іншим обладнанням Cisco, використання Cisco IoT серверу замість хабу є найкращим варіантом, оскільки такий сервер може виступати як у ролі центрального хабу, так і у ролі DHCP серверу, який забезпечує динамічну IP-адресацію для всіх пристроїв, включаючи й пристрої які не входять до IoT екосистеми. Даний сервер може тримати дані як локально, так і вивантажити їх у хмару, що робить його надзвичайно надійним варіантом, який ми і будемо використовувати у цьому проекті.

### 2.3 Вибір пристроїв для мережі з врахуванням плану території будинку

Врахування території будинку є важливим аспектом при підборі пристроїв для мережі IoT. По-перше, розташування пристроїв потрібно ретельно розглянути, щоб забезпечити оптимальний зв'язок між ними. Залежно від розміру будинку та його архітектурних особливостей, може виникнути необхідність встановлення підсилювачів сигналу або додаткових точок доступу, використання більшої кількості датчиків, та інших IoT девайсів.

Планування дозволяє визначити оптимальне розташування датчиків, та інших пристроїв, щоб забезпечити максимальний охоплення всієї території будинку [13]. План будинку зображений на рисунку 2.8.



Перед вибором кінцевих девайсів для мережі, необхідно визначити основні потреби користувача: тобто врахувати усю територію будинку, та спростити користувачу нагляд за нею.

Наприклад, оскільки власник території має малий город неподалік від будинку, можна забезпечити автоматизацію його поливу. Враховуючи те що власник має декілька транспортних засобів, необхідно встановити датчик диму у гаражі, для превентування виникнення надзвичайних та небезпечних ситуацій, а також забезпечити автоматичне відкривання та закривання гаражних дверей.

Також необхідно встановити певну кількість базових датчиків, для контролю температури у приміщенні, кондиціонер, розумні замки на двері, тощо.

Для початку, необхідно обрати ядро нашої мережі, – IoT сервер. Зваживши усі наші потреби, було обрано Сервер Cisco UCS C220 M3 LFF (рисунок 2.9).



Рисунок 2.9 – Сервер Cisco UCS C220 M3 LFF

Причиною вибору саме цього серверу є в першу чергу, його надійність, а також його ціна порівняно з іншими Cisco серверами.

Сервер оснащено двома процесорами Intel Xeon E5–2650L v2, з діапазоном частот 1.70–2.10 GHz, 10–Core, на 25MB, та 70W, оперативною пам'яттю на 8 GB серії DDR3 (2 плашки по 4 GB), та RAID–контролером Cisco UCS RAID SAS 2008M–8i і блоком живлення 2 x 650 W.

Мережевий контролер має 2 порти 1 Gb Ethernet з можливістю віддаленого доступу через Cisco Integrated Management Controller (CIMC).

Цей стічний сервер, висотою в одну стандартну одиницю (1RU) підтримує продуктивність і щільність, достатні для надійної роботи широкого кола бізнес–додатків, веб–сервісів і розподілених баз даних. Даний 2–процесорний сервер високої щільності загального призначення оптимізований для високої продуктивності, та для широкого спектру робочих навантажень, в тому числі і для:

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 33   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

розподілених кластерів баз даних, Middleware, віртуальних робочих столів, IT і веб-інфраструктури. Система Cisco Unified Computing System (UCS) Manager забезпечує уніфіковане, вбудоване управління всіма програмними і апаратними компонентами Cisco UCS [36]. Характеристики даного серверу зображено у таблиці 2.5.

Таблиця 2.5 – Характеристики серверу Cisco UCS C220 M3 LFF

| Характеристика  | Значення                         |
|---|----------------------------------|
| Форм-фактор дисків                                      | 3.5"                             |
| Кількість слотів під накопичувачі                       | 4x 3.5"                          |
| Тип оперативної пам'яті                                 | DDR3                             |
| Форм-фактор корпусу                                     | 1U Rackmount                     |
| Кількість сокетів під процесори                         | 2                                |
| Тип процесорів  | Intel Xeon E5-26xx V1/V2 (S2011) |
| Інтерфейс накопичувачів                                 | SATA, SAS                        |
| Контролери SAS/SATA                                     | Cisco UCS RAID SAS 2008M-8i      |
| Кількість LAN (RJ-45)                                   | 2x порта 1Gb Ethernet            |
| Габарити (Ш (з вухами) x Г (з блоком живлення) x В), мм | 429 (482) x 760 (775) x 44       |

Так як територія будинку доволі велика, необхідно встановити декілька точок підсилення, для забезпечення хорошого та стабільного рівню сигналу у будь-якій точці будинку. Для ролі ретранслятора було обрано Cisco Aironet 3600i (рисунок 2.10).



Рисунок 2.10 – Cisco Aironet 3600i

Причиною вибору Cisco Aironet 3600i є в першу чергу його ціна, а також функціонал, який йому доступний.

Точка доступу Cisco Aironet 3600i забезпечує кращу в галузі продуктивність бездротового зв'язку з підтримкою новітнього стандарту Wi-Fi, IEEE 802.11ac Wave 2. Він також відповідає зростаючим вимогам гнучкості бездротових мереж за рахунок використання комірчастої технології, забезпечуючи при цьому простоту взаємодії з користувачем [35].

Точка доступу 140AC розширює зону покриття і ємність для клієнтів Wi-Fi, таких як смартфони, планшети і високопродуктивні ноутбуки, які мають інтегровану підтримку 802.11ac Wave 1 або Wave 2. Характеристики цієї точки доступу зображено у таблиці 2.6.

Таблиця 2.6 – Характеристики Cisco Aironet 3600i

| Характеристика           | Значення                      |
|--------------------------|-------------------------------|
| 1                        | 2                             |
| Режими роботи            | Wifi-точка підсилення сигналу |
| Стандарти мереж          | ac (до 867 Мбіт/с)            |
| Робоча частота           | 2.4 / 5 ГГц                   |
| Безпека інформації       | WPA2, AES , WPA3              |
| Моніторинг та управління | Web-інтерфейс                 |



Таблиця 2.7 – Характеристики Cisco Catalyst 2960

| Характеристика              | Значення              |
|-----------------------------|-----------------------|
| Число портів 10/100         | 24                    |
| Число портів 10/100/1000    | 2                     |
| Максимум VLAN               | 64                    |
| Пропускна здатність, Гбіт/с | 8,8                   |
| Максимум MAC-адрес          | 8000                  |
| Розміри (ВхШхГ) см.         | 4,4 x 44, 5 x 23,6 1U |

Для підключення мережі для інтернету будемо використовувати роутер Cisco 886VA-K9 VDSL Router (рисунок 2.12). Він є чудовим і надійним варіантом для нашої мережі [33].



Рисунок 2.12 – Роутер Cisco ISR4331 VDSL Router

Причиною вибору саме цього роутеру є його ціна, компактність, та стійкість до ударів [19]. Характеристики цього роутера зображено у таблиці 2.8.

Таблиця 2.8 – Характеристики Cisco ISR4331 VDSL Router

| Характеристика           | Значення |
|--------------------------|----------|
| Число серійних портів    | 2        |
| Число портів 10/100/1000 | 3        |
| Вага                     | 1,5 kg   |

Тепер перейдемо до кінцевих IoT пристроїв. Обирати можна будь-які моделі, які підтримують або Wifi або MQTT протоколи. В такому разі пристрої будуть працювати та відображатись коректно та без перебоїв.

Для коректної роботи не IoT девайсів, таких як кухонна витяжка, витяжні вентилятори, та водяний насос, будуть використовуватись розумні розетки. Такий підхід дозволяє використовувати будь-які моделі пристроїв, незважаючи на їх сумісність з мережею чи наявністю безпроводного підключення як такого.

Для даного проекту було обрано модель розумної розетки TP-LINK міні Таро P110 (рисунок 2.13).



Рисунок 2.13 – Розумна розетка TP-LINK міні Таро P110

Основною перевагою цієї моделі є просте налаштування та використання — не потрібен окремий центр керування, розетку можна дуже просто під'єднати до Wifi мережі, а IoT додаток сам розпізнає її функції. Якщо додаток не є рідним, наприклад Cisco Asset Vision, самі тригери розетки всеодно буде видно у дашборді, але без розширених функцій [24]. Характеристики цієї розумної розетки зображено у таблиці 2.9.

Для забезпечення безпеки та захисту будинку встановимо декілька розумних замків NaviCat X8 з підтримкою програми TUYA Black (рисунок 2.14).

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 38   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

Таблиця 2.9 – Характеристики TP-LINK міні Таро P110

| Характеристика                       | Значення          |
|--------------------------------------|-------------------|
| Бездротовий стандарт                 | Wifi, MQTT        |
| Керування                            | Віддалений доступ |
| Кількість гнізд                      | 1                 |
| Гранична потужність навантаження, Вт | 3680              |
| Розміри                              | 72 x 51 x 77 мм   |



Рисунок 2.14 – Розумний дверний замок NaviCat X8

NaviCat X8 – врізний замок на двері з гібридною ідентифікацією користувача: відбиток пальців або пароль, також підтримується карта доступу. Замок відмінно підійде як сучасна система контролю доступу для офісу та будинку. Замок універсальний і простий як у монтажі, так і у використанні. Для встановлення потрібні лише дріль та викрутка. Його можна встановити як на лівосторонні, так і на правосторонні двері та на двері, що відчиняються як ззовні, так і всередину приміщення. Замок відмінно підійде як для дерев'яних та металевих, так і пластикових дверей з вузьким профілем [26]. Характеристики NaviCat X8 зображено у таблиці 2.10.

Таблиця 2.10 – Характеристики NaviCat X8

| Характеристика       | Значення  |
|----------------------|---|
| Бездротовий стандарт | Wifi, MQTT  |
| Керування            | Віддалений доступ, початкове налаштування за допомогою TUYA Black |
| Спосіб установки     | Виразний  |

Для контролю над гаражними воротами, необхідно встановити на них необхідний контролер. Будемо використовувати контролер WG-088, через його доступність і ціну (рисунок 2.15).



Рисунок 2.15 – Wi-Fi контролер для керування гаражними воротами,  
WG-088

Контролер WG-088 дозволяє керувати секційними воротами за допомогою програми на смартфоні. Все що для цього потрібно: завантажити та встановити на смартфон програму з AppStore або PlayMarket під назвою Tuya Smart / Smart Life (QR-код в інструкції) для початкового налаштування, та підключити пристрій до приводу воріт [41]. Характеристики цього контролера зображено у таблиці 2.11

Таблиця 2.11 – Характеристики WG-088

|      |      |         |        |      |                          |            |
|------|------|---------|--------|------|--------------------------|------------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>40 |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |            |

| Характеристика       | Значення  |
|----------------------|---|
| Бездротовий стандарт | Wifi, MQTT  |
| Керування            | Віддалений доступ, налаштування за допомогою TUYA Smart |
| Розміри              | 9 x 3.9 x 2.4 см  |

Для автоматичного провітрювання будинку на вікна будуть встановлені пристрої для їх автоматичного відкривання. Сама технологія є новою, але дуже корисною. Єдине що необхідно знати, це те що такі пристрої в основному працюють тільки з мансардними вікнами.

Для даного проекту було обрано модель автоматичного відкривача вікон TuYa Huurized JOActuator, так як це самий надійний з бюджетних варіантів (рисунок 2.16).



Рисунок 2.16 – Автоматичний відкривач вікон TuYa Huurized JOActuator

Ланцюг такого девайсу може згинатися в одному напрямку. Він розтягується при відкритті вікна і втягується в механізм відчинення після закриття вікна. Ланцюг є двошаровим, тому він міцний і його нелегко зламати.

Цей пристрій оснащений захистом від перевантаження і може відкриватися та закриватися 20000 разів. Зусилля блокування досягає 2000 Н, а зусилля, що штовхає/тягне, 400 Н, при робочій температурі 20–75 °С [2]. Підходить для кількох типів вікон. Перелік усіх характеристик TuYa Huurized JOActuator зображено у таблиці 2.12.

Таблиця 2.12 – Характеристики TuYa Huurized JOActuator

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>41 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |

| Характеристика       | Значення  |
|----------------------|---|
| Бездротовий стандарт | Wifi, MQTT  |
| Керування            | Віддалений доступ, початкове налаштування за допомогою TUYA Smart |
| Тип ланцюга          | Двошарова   |
| Зусилля блокування   | $\leq 2000$ Н   |
| Розміри              | 200 мм  |

Для віддаленого керування кондиціонером буде використовуватись розумний інфрачервоний пульт TuYa IF Smart (рисунок 2.17). Даний пульт може запросто імітувати сигнали для кондиціонеру (тільки для тих які отримують сигнали через інфрачервоне випромінювання), перетворюючи будь-який кондиціонер на “розумний”.



Рисунок 2.17 – Розумний інфрачервоний пульт TuYa IF Smart

Використовуючи універсальний пульт дистанційного керування WIFI від TuYa, ми можемо керувати будь-якими домашніми пристроями за допомогою одного застосунку. Пульт дистанційного керування підтримує 99% побутової техніки, робота якої здійснюється за допомогою інфрачервоних пультів дистанційного керування, наприклад, потрібним нам кондиціонером [27]. Усі його характеристики зображені у таблиці 2.13.

Таблиця 2.13 – Характеристики TuYa IF Smart

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>42 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |

| Характеристика                  | Значення  |
|---------------------------------|---|
| Бездротовий стандарт            | Wifi, MQTT  |
| Керування                       | Віддалений доступ, початкове налаштування за допомогою TUYA Smart |
| Тип з'єднання                   | Wi-Fi 2.4 Гц 802.11b/g/n  |
| Вбудовані ІЧ-світлодіоди        | 6 шт.   |
| Робоча відстань ІЧ-світлодіодів | До 9 метрів   |
| Розміри                         | 67 x 67 x 19.5 мм   |

Для запобігання для правильному поведженню з надзвичайними ситуаціями, у гараж та на кухню буде встановлено розумні датчики диму TuYa smart house 902565 (рисунок 2.18).

Основною особливістю цього пристрою є виявлення як диму, так і підвищеної температури.



Рисунок 2.18 – Датчик диму TuYa smart house 902565

Інтелектуальний Wi-Fi датчик для виявлення диму та забезпечення пожежної безпеки від TuYa. Працює як автономний пристрій або в складі екосистеми. Датчик диму можна встановити на будь-якій поверхні, чи то стіна, чи стеля. Пристрій виявляє дим або підвищену температуру (пожежа). Цей пристрій можна інтегрувати з датчиком відкриття дверей чи іншими датчиками для

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>43 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |

створення сценарію, в якому при спрацюванні датчика відкриття дверей датчик диму буде використовуватися як сирена [7]. Перелік його характеристик зображено у таблиці 2.14.

Таблиця 2.14 – Характеристики датчику диму Tuuya smart house 902565

| Характеристика       | Значення  |
|----------------------|---|
| Бездротовий стандарт | Wifi, MQTT  |
| Керування            | Віддалений доступ, початкове налаштування за допомогою TUYA Smart |
| Тип з'єднання        | 802.11b/g/n 2.4GHz  |
| Розміри              | 90 x 90 x 40 мм   |
| Робоча температура   | -10°C – 50°C  |
| Розміри              | 90 x 90 x 40 мм   |

Для увімкнення вуличних ліхтарів та поливу городу при заході сонця, буде використовуватись датчик руху та освітленості VIDEX VL-SPC24W (рисунок 2.19).

Даний датчик не потребує підключення до екосистеми розумного будинку, і буде працювати автономно, вмикаючи вуличне освітлення та полив при заході сонця, і вимикати його вночі.



Рисунок 2.19 – Датчик руху та освітленості VIDEX VL-SPC24W

VIDEX VL–SPC24W 220V 1200W дозволяє керувати системою освітлення та фіксує переміщення об'єктів. Датчик автоматично вмикає та вимикає освітлення у приміщенні в залежності від виявлення руху у своєму полі дії. Широко використовується для освітлення промислових, складських, паркових, прибудинкових територій, зон відпочинку, доріг. Рекомендована висота встановлення–2,2–4м. Дозволяє регулювати світловий поріг спрацювання в діапазоні від 10Лк до 2000Лк. Усі його характеристики перераховані у таблиці 2.15.

Таблиця 2.15 – Характеристики датчику освітленості VIDEX VL–SPC24W

| Характеристика              | Значення           |
|-----------------------------|--------------------|
| Бездротовий стандарт        | Немає              |
| Керування                   | Автономне          |
| Тип з'єднання               | Дротове            |
| Дистанція виявлення         | від 2м до 8м       |
| Світловий поріг спрацювання | від 10Лк до 2000Лк |
| Розміри                     | 103 x 58 мм        |

Для контролю температури у будинку буде встановлено датчик температури та вологості РТ–ТУ800S (рисунок 2.20).



Рисунок 2.20 – Датчик температури та вологості РТ–ТУ800S

|     |      |         |        |      |                          |      |
|-----|------|---------|--------|------|--------------------------|------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|     |      |         |        |      |                          | 45   |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |      |

Цей датчик має швидкий та точний моніторинг – Визначає температуру та вологість за допомогою високоточного датчика швейцарського виробництва. Отримання та оновлення даних кожні 2 секунди. (Точність:  $\pm 0,3$  °C,  $\pm 3\%$  відносної вологості) [9].

Включає можливість домашньої автоматизації – автоматично вмикає/вимикає домашню електроніку, коли параметри виходять за межі встановлених діапазонів. Характеристики цього датчику зображені у таблиці 2.16.

Таблиця 2.16 – Характеристики датчику RT-TY800S

| Характеристика       | Значення   |
|----------------------|--|
| Бездротовий стандарт | Wifi, MQTT   |
| Керування            | Віддалений доступ, початкове налаштування за допомогою Smart Life/Tuya Smart |
| Тип з'єднання        | 802.11b/g/n 2.4GHz   |
| Робоча температура   | -10°C – 55°C   |
| Розміри              | 70*25*20 мм  |

## 2.4 Висновки

У другому розділі нашого дослідження було виконано аналіз існуючих рішень для створення мережі розумного будинку.

Насамперед було проаналізовано типи можливих підключень пристроїв до мережі, та обрано найбільш оптимальний варіант їх застосування, а саме використання змішаного підключення девайсів до мережі.

Після цього було детально проаналізовано усі існуючі протоколи роботи розумних пристроїв, та обрано найбільш оптимальний з них для даного проекту протокол – MQTT, після чого були визначені його переваги в порівнянні з іншими

протоколами, зокрема його простота, надійність, та підтримка більшою кількістю пристроїв.

Наступним кроком також було проаналізовано усі доступні додатки для управління розумними пристроями, серед яких Xiaomi Smart Home, Tuya Smart, та Cisco Asset vision, та порівняно їх переваги та недоліки між собою.

На основі отриманої інформації було обрано додаток Cisco Asset Vision, через його гнучкість у налаштуванні, та можливість підняття веб-дашборду на власному сервері.

Після цього було обрано ядро системи, а саме власний сервер, який буде виступати у ролі IoT хабу, замість уже доступних хабів китайського виробництва, оскільки такий варіант є найнадійнішим, та чудово працює як з пристроями IoT, так і з пристроями які не входять до цієї екосистеми. Було проведено повний аналіз характеристик серверу, його можливостей, переваг та недоліків.

Після обрання серверу було обрано кінцеві IoT пристрої з врахуванням потреб користувача та плану будинку, проведено повний аналіз їх характеристик та можливостей, та детальне обґрунтування причини обрання саме цих моделей.

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 47   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

### 3 ПРОЄКТУВАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖІ "РОЗУМНИЙ ЗАМІСЬКИЙ БУДИНОК"

#### 3.1 Проектування мережі та розташування пристроїв згідно плану будинку

Перед початком встановлення кінцевих пристроїв, необхідно спланувати їх оптимальне розташування та їх оптимальну кількість [23]. При цьому необхідно врахувати розміри будинку, а також відстані між кімнатами (рисунок 3.1).



Рисунок 3.1 – Розміри будинку

Для початку необхідно вибрати підходяще місце для розташування IoT серверу, маршрутизатора та комутатора.

Оптимальним місцем для такої апаратури буде пуста, або майже пуста кімната, з ускладненим доступом для дітей. У ролі такої кімнати була вибрана кімната, зображена на рисунку 3.2.



Рисунок 3.2 – Серверна кімната

Ця кімната являється оптимальною для розташування серверу з наступних причин:

- затруднений доступ для дітей;
- можливість легкого виводу проводки на вулицю при необхідності;
- достатньо великі розміри кімнати;
- можливість нагляду за роботою пристроїв ззовні;
- легкість пожежогасіння у разі виникнення пожежі;

Основним елементом такої мережі являється точка доступу, оскільки усі кінцеві розумні пристрої будуть підключатись саме до неї. Зважаючи на розміри самого будинку, необхідно вибрати оптимальну кількість точок доступу, для рівномірного поширення сигналу по території будинку.

Враховуючи те, що сила сигналу втрачається по мірі віддалення пристрою від точки доступу, та максимальну дальність поширення сигналу у 100 метрів, було вирішено встановити 3 точки доступу, для забезпечення сильного сигналу по усій території будинку [1].

Так як у будинку присутня достатня кількість стін, номінальний максимальний показник дальності поширення сигналу значно знижується, що може привести до непередбачуваних проблем поширення сигналу та його перешкод. Розташування корінних пристроїв системи зображено на рисунку 3.3.

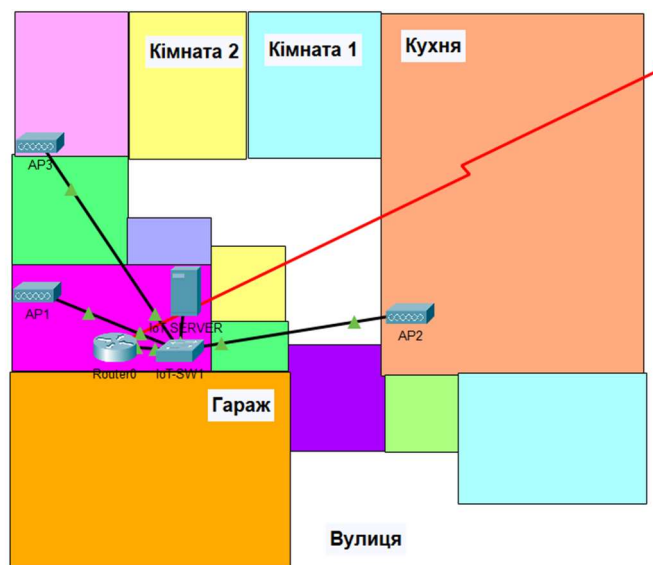


Рисунок 3.3 – Розташування корінних пристроїв системи

Єдиними пристроями що будуть з'єднані за допомогою дротового з'єднання являються IoT сервер, маршрутизатор, комутатор, та точки доступу.

Так як у комутатора будуть використовуватись рівно п'ять портів, необхідно їх перевести у стан "увімкнено". Для цього достатньо перейти у вкладку config комутатора, та увімкнути порти FastEthernet з першого по п'ятий.

Для з'єднання комутатора з точками доступу, необхідно просто з'єднати один з FastEthernet портів комутатора з портами Port0 точок доступу. Роутер ж підключаємо використовуючи інтерфейс GigabitEthernet 0/0/0, попередньо перевівши його у стан "увімкнено". Підключення серверу до комутатора відбувається через порт FastEthernet0, який також потрібно увімкнути.

Для компактного та впорядкованого з'єднання усі дроти ховаються за плінтус, а для підключення найкоротшим шляхом робляться отвори у стінах, для простого пересування проводки між кімнатами. Усі інші пристрої будуть під'єднані до мережі через безпроводне з'єднання, використовуючи точки доступу.

Тепер давайте розташуємо усі кінцеві пристрої, які ми обрали у другому розділі проекту враховуючи розміри кімнат (рисунок 3.4). Повна логічна топологія мережі зображена у додатку А.

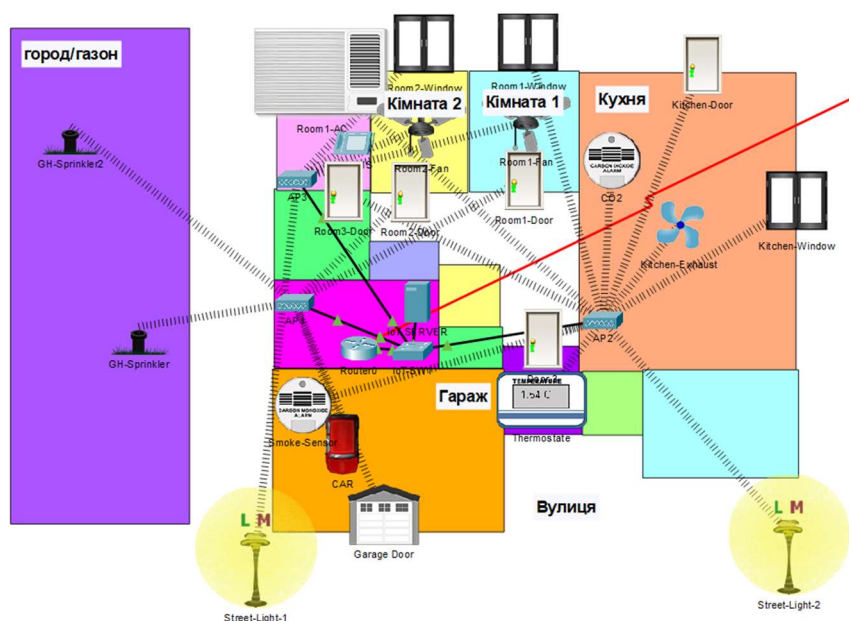


Рисунок 3.4 – Розташування кінцевих пристроїв

Давайте покроково розберемо усі пристрої та причину подібного їх розташування у приміщенні.

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 50   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

Контролер гаражних воріт було підключено до приводу воріт, для можливості віддаленого керування ними.

До вуличних ліхтарів було під'єднано датчики освітленості, для автоматичного вмикання і вимикання ліхтарів у нічну пору, з метою економії електроенергії та автоматизації.

У гараж також було встановлено датчик диму, оскільки у власника будинку є дві машини. Даний датчик буде вимірювати кількість диму у приміщенні, та вмикати сирену при його надлишку.

На вхідних дверях будинку, а також на дверях кімнат були встановлені розумні замки, для віддаленого керування ними у цілях безпеки.

Такі пристрої як кондиціонер, стельові вентилятори, кухонна витяжка, та водяний насос були підключені до мережі через розумні розетки, Для гнучкого їх використання та з цілями економії як електроенергії, так і коштів. Це дозволяє використовувати будь-які моделі пристроїв, що сильно розширює усі наявні варіанти, та дозволяє людині не заціклюватись на пошуку “розумних” моделей, та використовувати якісні та надійні девайси.

На кухонні та кімнатні вікна було встановлено автоматичні відкривачі, для збільшення комфорту та зручності використання у повсякденному житті. Це також дає змогу провітрювати будинок свіжим повітрям при відсутності у ньому власника, або при певній температурі повітря.

В коридорі також був встановлений датчик температури, який дозволяє контролювати температуру у будинку навіть коли його власник не вдома, та виконувати потрібні йому сценарії. Саме цей датчик і дозволяє автоматизувати такі дії як автоматичне відкриття вікон при певній темпаратурі, увімкнення поливу, закриття вікон, вмикання кондиціонерів чи стельових вентиляторів у кімнатах, тощо.

Після розташування усіх пристроїв, необхідно правильно їх сконфігурувати, та підключити до мережі. Спочатку налаштуємо наш IoT-сервер.

Для початку необхідно підняти IoT дашборд на нашому сервері. Для цього встановлюємо будь-яку серверну версію Windows на сервер, та завантажуюмо на

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 51   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |



Для цього переходимо у вкладку DHCP, та піднімаємо сервіс. Тепер необхідно додати сервірний пул адрес, які сервер зможе призначати кінцевим пристроям.

Виставимо початкову адресу 192.168.10.11 та виставимо максимальне число клієнтів: 240. Це значення є надзвичайно великим, в порівнянні з хабами китайського виробництва, які підтримують не більше 100 одночасних підключень пристроїв, що є ще одним плюсом встановлення власного надійного серверу.

Після додавання пулу адрес, будь-який пристрій який буде підключено до мережі, буде автоматично отримувати IP адресу [37].

Тепер необхідно підняти TFTP сервіс, це дозволить нашому серверу використовувати UDP протокол, який не має перевірки помилок як TCP. Саме через те що він не потребує автентифікації, він використовується для передачі невеликих файлів, та прискорює роботу серверу (рисунок 3.7).

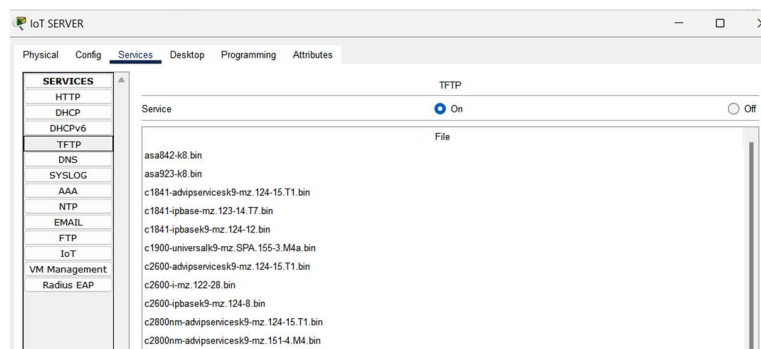


Рисунок 3.7 – Увімкнення TFTP сервісу

Після цього наш сервер є повністю налаштованим. Наступним кроком нам необхідно налаштувати точки доступу та під'єднати усі кінцеві пристрої до мережі.

Для того щоб налаштувати точки доступу перейдемо до їх веб інтерфейсу, або у випадку Cisco Packet Tracer, буде достатньо просто перейти у вкладку конфігурації (рисунок 3.8).

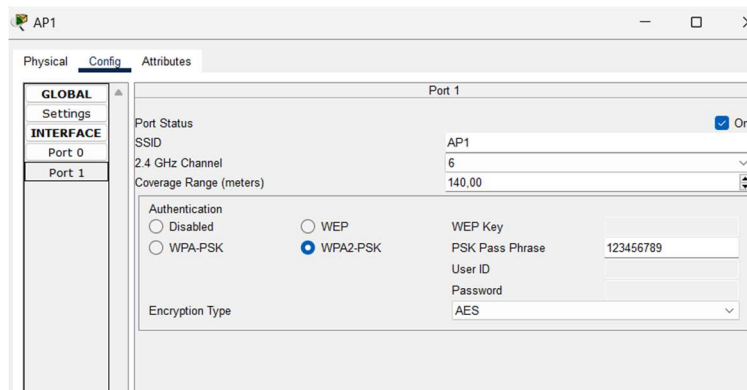


Рисунок 3.8 – Конфігурація точки доступу

Встановлюємо точці доступу будь-яке SSID – це ім'я мережі, яке буде відображатись при підключенні безпроводним шляхом. Наступним кроком буде встановлення паролю мережі, та типу шифрування. Обираємо протокол WPA2-PSK. Він дозволяє обмінюватись даними з пристроями за допомогою способу шифрування AES. Після цього встановлюємо пароль мережі. Пароль має бути надійним, та включати в себе як великі так і малі літери, хоча б один спеціальний символ та як мінімум одну цифру, та бути не коротше 8 символів. Решту точок доступу налаштовуємо так само [12].

Кінцеві пристрої підключаються до мережі Wi-fi двома способами: за допомогою сторонніх програм, такі як Tuuya Smart або Smart Life, або за допомогою власних веб-інтерфейсів, схожих до тих що використовують роутери. Процес підключення кінцевого пристрою до мережі Wi-Fi зображено на рисунку 3.9.

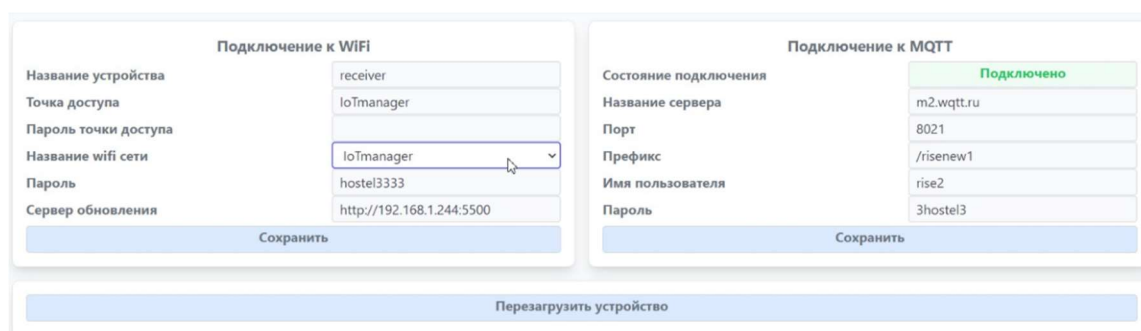


Рисунок 3.9 – Підключення кінцевого пристрою до мережі Wi-fi

Для підключення через Tuuya Smart достатньо зайти у додаток, зажати кнопку увімкнення на кінцевому пристрої, і додаток автоматично його розпізнає, після

чого йому можна задати назву мережі до якої необхідно підключитися, та пароль до неї. Якщо ж пристрій не підтримує TuYa Smart чи Smart Life, необхідно зажати кнопку увімкнення пристрою, після чого він перейде у режим точки доступу. Далі необхідно до нього під'єднатися, відкрити його веб-інтерфейс та вписати назву мережі та пароль до неї вручну. Після цього необхідно перезапустити пристрій, для того щоб він перейшов в нормальний режим роботи. Підключення пристрою вручну було продемонстровано на рисунку 3.10.

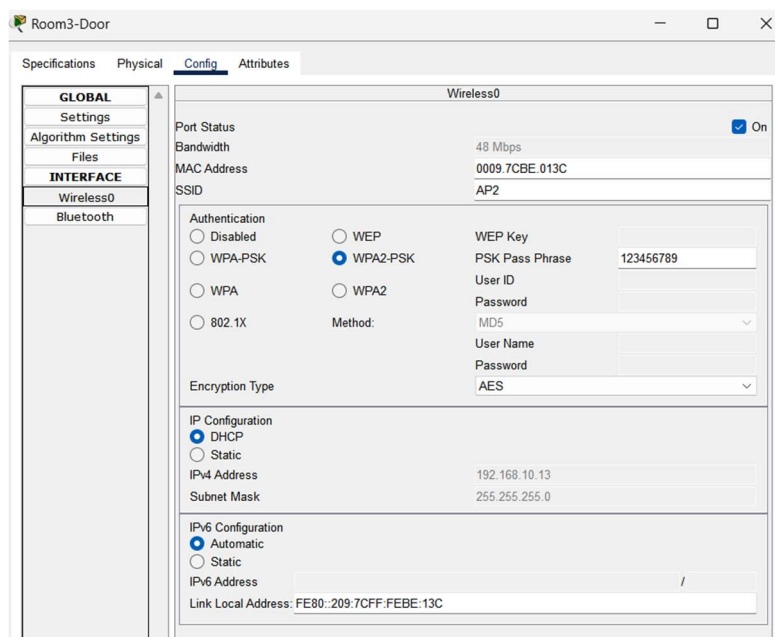


Рисунок 3.10 – Підключення кінцевого пристрою до мережі Wi-fi вручну

Для того щоб підключити кінцевий пристрій до мережі у Cisco Packet Tracer, використовується наступний метод: Необхідно зайти у налаштування пристрою, перейти у вкладку “Wireless0”, ввести SSID мережі до якої потрібно під'єднатись, тип протоколу безпеки цієї мережі, та пароль до неї. Після цього вимкнути статичну IP адресу, та увімкнути DHCP. Тепер цей пристрій отримає власну адресу після підключення до мережі, отримає власну тему для розсилки, і зможе спілкуватися з сервером.

Після підключення усіх пристроїв, необхідно перевірити чи вони правильно відображаються. Для цього у браузері переходимо по публічній IP адресі серверу, та потрапляємо на сторінку логіну до нашої IoT-системи. Вводимо користувача



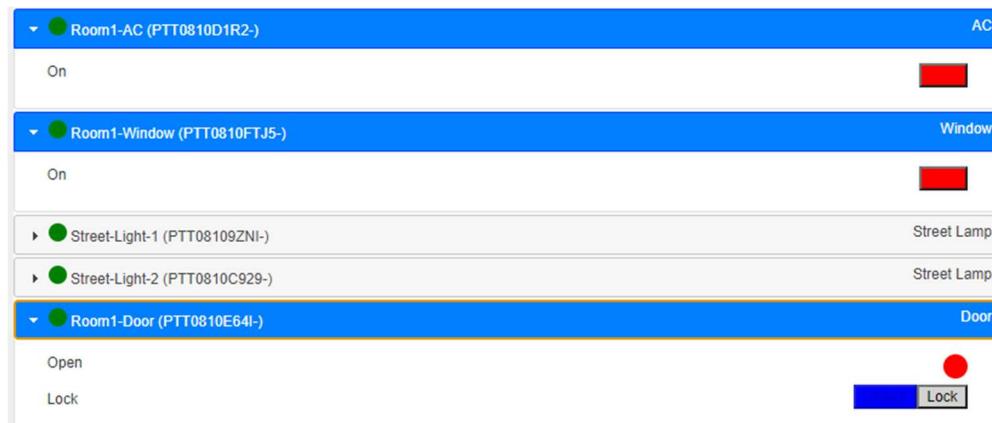


Рисунок 3.13 – Панель керування пристроями

### 3.2 Сценарії. Їх розробка та впровадження

Сценарії в Інтернеті речей є набором автоматизованих дій, які виконуються відповідно до заданих умов або подій. Вони грають важливу роль у покращенні зручності, ефективності та безпеки в розумних будинках та мережах.

Основна перевага сценаріїв полягає в їх здатності забезпечити автоматизоване, систематичне та уніфіковане керування різними пристроями та системами в мережі Інтернету речей. Вони дозволяють ефективно використовувати ресурси, забезпечуючи комфорт, безпеку та економію енергії. Крім того, сценарії можуть підвищити рівень автоматизації та реагування на зміни у оточенні, що робить їх незамінним інструментом для створення сучасного розумного будинку.

Для того щоб розробити на створити сценарій у Cisco Asset Vision, потрібно перейти до вкладки “Conditions” у нашому дашборді. Тут будуть відображатись усі колись створені сценарії поведінки пристроїв разом з їх тригерами. У кожного сценарію є своя назва, що дозволяє користувачу легко відрізнити їх один від одного (рисунок 3.14).



**Add Rule**

Name: Увімкнення кондиціонеру

Enabled:

If:

Match: All

Thermostate Temperature > 30 °C

Then set:

Room2-Fan Status to Low

Room1-Fan Status to Low

Room1-AC On to true

OK Cancel

Рисунок 3.16 – Створення нового сценарію

В випадяючому списку поряд вибираємо що саме будемо перевіряти. У нашому випадку це температура, яку показує термостат.

Після цього обираємо оператор, в даному випадку це оператор “>”(більше), та ставимо температуру при якій умова буде виконуватись.

У полі “Then set” вибирається дія, яка буде відбуватися при виконванні раніше заданої умови. У нашому випадку, будуть вмикатися стельові вентилятори та кондиціонер. Після чого натискаємо “ОК” для підтвердження створення сценарію.

Таким чином, ми створили сценарій, у якому при температурі більше 30 °C стельові вентилятори будуть вмикатися у режим “Low”, а кондиціонер у третій кімнаті у стан “On”.

Тепер створимо декілька важливих сценаріїв для нашої мережі. Створення сценарію для увімкнення кухонної витяжки було зображено на рисунку 3.17.

**Edit Rule**

Name: Kitchen-has-Smoke

Enabled:

If:

Match: Any

CO2 Level >= 0.14

Then set:

Kitchen-Exhaust Status to High

Kitchen-Window On to true

Рисунок 3.17 – Сценарій “На кухні є дим”

Створимо сценарій при якому буде запускатися кухонна витяжка та відкриватися вікно на кухні.

При умові, коли рівень CO<sub>2</sub> перевищує рівень в 0.14 ppm, буде вмикатися кухонна витяжка, а статус вікна буде замінено на “true”, що означає, що вікно буде відкрито як тільки ця умова буде виконана.

Таким чином, ми створили сценарій, який дозволяє моментально зреагувати на небезпеку, та запобігти виникненню надзвичайної ситуації. Таким ж чином створимо сценарій і для гаражного приміщення, при перевищенні рівню CO<sub>2</sub> в якому, будуть відкриватися гаражні ворота та вмикатися сигналізація (рисунок 3.18).

The screenshot shows the 'Edit Rule' window with the following configuration:

- Name: GarageDoorOpen
- Enabled:
- If: Match Any
  - Smoke-Sensor Level >= 0.04
  - Garage Door On is true
- Then set: Garage Door On to true

Рисунок 3.18 – Сценарій “Відкриття гаражних воріт”

Також, створимо сценарій при якому включається автоматичний полив городу. Для цього перевіряємо стан датчика освітленість в статусі “Dim”(тускле світло) то буде вмикатися автоматичний полив городу. І як тільки сонце сідає (освітленість менше 5 люкс), полив вимикається (рисунок 3.19).

The screenshot shows the 'Edit Rule' window with the following configuration:

- Name: GreenHouseWatering
- Enabled:
- If: Match All
  - SUN Status is Dim
- Then set: GH-Sprinkler Status to true, GH-Sprinkler2 Status to true

Рисунок 3.19 – Сценарій “полив городу”

Таким чином були створені базові сценарії, які значно автоматизують необхідні процеси, та полегшують життя.

### 3.3 Підключення мережі до інтернету

Для того щоб користувач міг віддалено керувати розумними пристроями, необхідно забезпечити доступ серверу до інтернету.

На даний момент, підключити будь-яку мережу до інтернету можна трьома способами:

- провідне підключення до провайдера інтернет послуг;
- використання супутникового інтернету;
- підключення за допомогою мобільного інтернету;

Провідне підключення завжди вважалося й вважається найнадійнішим типом підключення. Будучи надійним, воно також є й найшвидшим. 80% людей які мають інтернет, використовують саме провідне підключення [3, 10].

Не так давно в Україні з'явився й супутниковий інтернет. Його основним плюсом є можливість користувача бути підключеним до інтернету майже з будь-якої точки світу. Таке підключення також є надзвичайно швидким, але його остаточна доля в Україні ще не вирішена.

Підключення за допомогою мобільного інтернету також є непоганим варіантом, якщо користувачу не доступна ніяка з вище перелічених опцій.

У нашому випадку, для забезпечення ще більшої надійності й швидкості мережі, припустимо що користувачу доступне провідне підключення до інтернету.

Провайдером оберемо Kyivstar, оскільки у цього провайдера найбільша площа покриття [28, 30]. Провідне підключення мережі до провайдера інтернет послуг у Cisco Packet Tracer зображено на рисунку 3.20.

|     |      |         |        |      |                          |      |
|-----|------|---------|--------|------|--------------------------|------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|     |      |         |        |      |                          | 61   |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |      |

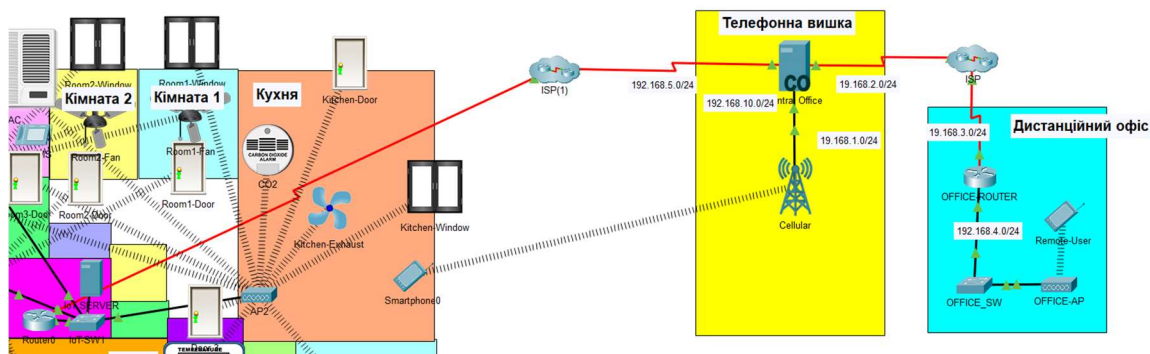


Рисунок 3.20 – Провідне підключення мережі до провайдера інтернет послуг

Провідним шляхом підключаємо наш роутер до центрального офісу Kyivstar через серійний порт Serial 0/1/0, попередньо його увімкнувши. Таким чином користувач буде мати доступ до мережі з будь-якої точки України.

При відсутності можливості підключення дротовим шляхом, наведена вище схема може дуже легко модифікуватися для підтримки мобільного інтернету. Для цього просто необхідно встановити замість звичайного роутера, роутер мобільного інтернету. Такі роутери використовують sim-картку для того щоб підключатися до інтернету. Тому потрібно буде просто замінити наявний роутер на мобільний роутер, та підключитися до телефонної вишки напряду.

Таким чином мережа буде мати доступ до інтернету у будь-якому випадку.

### 3.4 Розрахунок вартості системи "Розумний замський будинок"

Для оптимальної та надійної роботи IoT мережі були обрані такі елементи:

- сервер Cisco UCS C220 M3 LFF;
- точка доступу Cisco Aironet 3600i;
- комутатор CISCO CATALYST 2960;
- роутер Cisco ISR4331 VDSL Router;
- розумна розетка TP-LINK міні Таро P110;
- розумний дверний замок NaviCat X8;
- Wi-Fi контролер для керування гаражними воротами WG-088;

- автоматичний відкривач вікон TuYa Huurized JOActuator;
- розумний інфрачервоний пульт TuYa IF Smart;
- датчик диму TuYa smart house 902565;
- датчик руху та освітленості VIDEX VL–SPC24W;
- датчик температури та вологості PT–TY800S.

Вартість реалізованої мережі залежить від вартості елементів, що входять до складу системи.

У таблиці 3.1 наведено перелік компонентів і розрахунки витрат на них.

Таблиця 3.1 – Розрахунок витрат

| № | Найменування компонентів                                    | Ціна,<br>грн | Кількість,<br>шт. | Загальна<br>сума,<br>грн |
|---|---|--------------|-------------------|--------------------------|
| 1 | 2   | 3            | 4                 | 5                        |
| 1 | Сервер Cisco UCS C220 M3<br>LFF                             | 8428         | 1                 | 8428                     |
| 2 | Точка доступу Cisco Aironet<br>3600i                        | 1390         | 3                 | 4170                     |
| 3 | Комутатор CISCO<br>CATALYST 2960                            | 3100         | 1                 | 3100                     |
| 4 | Розумна розетка TP–LINK міні<br>Таро P110                   | 499          | 4                 | 1996                     |
| 5 | Розумний дверний замок<br>NaviCat X8                        | 3149         | 4                 | 12596                    |
| 6 | Wi–Fi контролер WG–088                                      | 780          | 1                 | 780                      |
| 7 | Автоматичний відкривач<br>вікон TuYa Huurized<br>JOActuator | 808          | 3                 | 2424                     |

Кінець таблиці 3.1

| 1              | 2   | 3    | 4 | 5     |
|----------------|---|------|---|-------|
| 8              | Розумний інфрачервоний пульт Tuuya IF Smart | 770  | 1 | 770   |
| 9              | Датчик диму Tuuya smart house 902565        | 559  | 2 | 1118  |
| 10             | Датчик руху та освітленості VIDEX VL-SPC24W | 444  | 3 | 1332  |
| 11             | Датчик температури та вологості PT-TY800S   | 280  | 1 | 280   |
| 12             | Роутер Cisco ISR4331 VDSL Router            | 2280 | 1 | 2280  |
| Загальна ціна: |   |      |   | 39274 |

Мережу можна удешевити при бажанні користувача. Для цього просто необхідно замінити наш сервер на контролер Nous E7 китайського виробника, забрати з мережі точки доступу, та замінити роутер від компанії Cisco на мобільний роутер Xiaomi F490 4G LTE. Таким чином, загальна вартість усієї мережі буде становити: 27894 грн., що є на 29% дешевше, але значно знизить надійність та гнучкість усієї мережі.

### 3.5 Напрямки вдосконалення

Спроектвану та сконфігуровану IoT-мережу можна використовувати не тільки для контролю та управління замським будинком, а також і для управління пристроями у офісі будь-якого розміру, або в будь-якій іншій бізнес установі. Функціональні можливості мережі можна розширити додавши зберігання даних у хмарі.

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 64   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

Після аналізу IoT–мережі для системи “Розумний замиський будинок” було намічено два основних напрямки вдосконалення.

Ними являються: збільшення швидкості доступу мережі до інтернету, та вдосконалення апаратної частини.

Збільшення швидкості доступу мережі до інтернету може відбуватися за допомогою використання більш новітнього способу підключення – супутникового.

Вдосконалення апаратної частини може відбуватися за рахунок заміни корінних пристроїв системи на більш нові, Використання потужнішого серверу, що дозволить підключення більше 1000 пристроїв одночасно, або за допомогою впровадження нових способів управління системою, наприклад за допомогою голосового помічника, чи жестів.

### 3.6 Висновки

Усю структуру та конфігурацію мережі було сплановано враховуючи план будинку, його території, а також потреб користувача. Серцем системи є сервер, який і здійснює управління усіма кінцевими розумними девайсами. Розташування пристроїв було вибрано з врахуванням зон покриття точок доступу.

Було налаштовано усі точки доступу, та встановлено на них надійний пароль у цілях безпеки.

Для реалізації сценаріїв були встановлені спеціальні умови та правила за допомогою програми Cisco Asset Vision, що дозволяє планувати деякі задачі, та запобігати виникненню надзвичайних ситуацій. Усі сценарії та список підключених пристроїв можна побачити ввівши публічну ір адресу серверу у браузер. Таким чином користувач може потрапити до дашборду, керувати усіма пристроями віддалено, та додавати нові сценарії.

Сервер підключено до інтернету провідним шляхом, використовуючи провайдера Kyivstar з найбільшою зоною покриття. При відсутності можливості підключення провідним шляхом, користувач може натомість використовувати

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 65   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

будь-який мобільний роутер для прямого підключення до мобільного інтернету, використовуючи того самого, або іншого провайдера.

Вартість реалізованої мережі залежить від елементів, які до неї входять. Загальна ціна усієї мережі складає 39274 грн. Мережу можна значно удешевити, якщо замість власного налаштованого сервера використовувати контролер китайського походження, та забравши з неї усі точки доступу, перейшовши на Mesh зв'язок. Також можна замінити корінні пристрої Cisco на більш дешеві версії. Якщо замінити у мережі перераховані вище елементи, ціна такої системи складе – 27894 грн., що є на 29% дешевше, але значно знизить надійність та гнучкість мережі.

В процесі розробки цієї IoT мережі були виконані усі етапи і завдання, що дозволило досягти мети роботи, а саме – спроектувати та сконфігурувати IoT-мережу для системи “Розумний заміський будинок”.

## ВИСНОВКИ

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 66   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

Метою роботи є розробка та планування IoT-мережі для системи “Розумний заміський будинок”. Поставлена мета досягається рішенням основної задачі роботи: розробкою та сплануванням IoT-мережі та перевіркою її роботи за допомогою програми емулятора. Об’єктом дослідження є IoT-мережа. Предметом дослідження є формалізований опис та схеми IoT-мережі.

У першому розділі було проаналізовано предметну область та теоретичні основи роботи систем IoT. Були оглянуті наявні види IoT пристроїв, та сфера їх використання. Було проаналізовано усі можливі варіанти підключення пристроїв до мережі, а також були сформовані вимоги для розробки самої мережі.

У другому розділі були оглянуті усі наявні існуючі рішення для створення системи “Розумний будинок”, після чого було проведено порівняльний аналіз їх переваг та недоліків. На основі виконаного огляду для виконання проєкту було обрано використання протоколу MQTT, та основну програму для розумного будинку – Cisco Asset Vision, після чого було вибрано пристрої для мережі, з детальним обґрунтуванням та врахуванням плану будинку.

У третьому розділі було проведено повне планування IoT-мережі, та розташування кінцевих пристроїв згідно з планом будинку. Власний IoT-сервер було повністю налаштовано для управління усіма пристроями в IoT-екосистемі та для створення певних сценаріїв поведінки пристроїв у мережі. Було створено декілька базових сценаріїв поведінки пристроїв, після чого усю систему було підключено до інтернету провідним шляхом, залишивши також і можливість підключення за допомогою мобільного інтернету.

Проведений розрахунок витрат показав що повна вартість IoT-системи складає – 39274 грн., з можливістю її удешевлення до 27894 грн. при відмові від більш надійних пристроїв. Після аналізу створеної IoT-мережі було намічено два основних напрямки вдосконалення, це збільшення швидкості доступу мережі до інтернету, та вдосконалення апаратної частини.

Покращення швидкості доступу мережі до інтернету може відбуватися за допомогою використання більш новітнього способу підключення – супутникового.

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>67 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |

Вдосконалення апаратної частини може відбуватися за рахунок заміни корінних пристроїв системи на більш нові, наприклад використання потужнішого серверу, або впровадження нових способів управління системою, наприклад за допомогою голосового помічника.

Отже, можна зробити висновок, що основної цілі кваліфікаційної роботи було досягнуто. Отриманий результат відповідає меті роботи, а розроблена IoT-мережа може бути вдосконалена.

## ЛІТЕРАТУРА

|      |      |         |        |      |                          |      |
|------|------|---------|--------|------|--------------------------|------|
|      |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк. |
|      |      |         |        |      |                          | 68   |
| Зм.. | Арк. | №докум. | Підпис | Дата |                          |      |

1. 10 способів покращити сигнал Wi-Fi у себе вдома URL: [https://www.bbc.com/ukrainian/science/2015/12/151201\\_how\\_to\\_boost\\_wi-fi\\_signal\\_ug](https://www.bbc.com/ukrainian/science/2015/12/151201_how_to_boost_wi-fi_signal_ug) (дата звернення: 22.05.2024)
2. Автоматичний відкривач вікон TuYa Huurized JOActuator URL: <https://fr.aliexpress.com/item/1005002567269107.html> (дата звернення: 21.05.2024)
3. Бездротовий інтернет – що це таке, види, швидкість URL: <https://mobitech.com.ua/ua/articles/besprovodnoi-internet> (дата звернення: 22.05.2024)
4. Бездротові стандарти. Що таке ZigBee? URL: <https://www.sea.com.ua/ua/besprovodnye-komponenty/news/bezdrotovi-standarti-so-take-zigbee/> (дата звернення: 22.05.2024)
5. Демістифікація шлюзів IoT: механізм безперебійного спілкування в IoT URL: <https://www.dusuniot.com/uk/blog/demystifying-iot-gateway-devices/> (дата звернення: 18.05.2024)
6. Датчики і приводи в IoT – забезпечення промислової автоматизації URL: <https://www.telesphera.net/blog/datchiki-i-privodi-v-iot.html> (дата звернення: 18.05.2024)
7. Датчик диму TuYa smart house 902565 URL: <https://rozetka.com.ua/ua/415098300/p415098300/> (дата звернення: 21.05.2024)
8. Датчик руху та освітленості VIDEX VL-SPC24W URL: <https://rozetka.com.ua/ua/videx-vl-spc24w/p320788627/> (дата звернення: 21.05.2024)
9. Датчик температури та вологості PT-TY800S URL: <https://smartunit.com.ua/p1699727932-datchik-temperatury-vlazhnosti.html> (дата звернення: 21.05.2024)
10. Дротовий (кабельний) інтернет URL: <https://ukrtelecom.ua/internet/drotovyy-kabelnyy-internet.php> (дата звернення: 22.05.2024)
11. Дротові та бездротові мережі – що це, та з якими роутерами їх «їдять» URL: <https://ktc.ua/blog/drotovi-ta-bezdrotovi-merezhi-shcho-ce-ta-z-yakimi-routerami-yih-yidyat.html> (дата звернення: 19.05.2024)

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>69 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |

12. ДСТУ ISO/IEC 27033–6:2018 Інформаційні технології. Методи захисту. Безпека мережі. Частина 6. Забезпечення безпроводового доступу до IP–мережі (ISO/IEC 27033–6:2016, IDT) pp 28

13. Домашня автоматизація за допомогою IoT: як швидко створити рішення для розумного дому URL: <https://www.dusuniot.com/uk/blog/home-automation-using-iot/> (дата звернення 22.05.2024)

14. Домрачева К. О. Аналіз технологій та стандартів зв'язку для мережі IoT / К. О. Домрачева, Н. М. Довженко, В. В. Дмитренко // Наук. зап. Укр. наук.–дослід. ін-ту зв'язку. – 2019. – № 3. – С. 54–62

15. Зуєв В. Бенчмаркінгова природа впровадження технологій інтернету речей у соціальній роботі / Зуєв В., Антонєць К. // Інтернет речей: проблеми правового регулювання та впровадження : матеріали III наук.– практ. конф., 21 листоп. 2019 р., м. Київ / [упоряд.: В. М. Фурашев, С. О. Дорогих, С. Ю. Петряєв]. – К., 2019. – С. 31–79. – Відомості доступні також в інтернеті: <https://cutt.ly/koehs45> (дата звернення: 21.05.2024)

16. Інтернет речей (IoT) – суть, технології і приклади URL: <https://termin.in.ua/internet-rechey-iot/> (дата звернення: 16.05.2024)

17. Інтернет речей: що це таке та де застосовують? URL: <https://cybercalm.org/novyny/internet-rechey-shho-tse-take-ta-de-zastosovuyut/> (дата звернення: 15.05.2024)

18. IoT, або Інтернет речей URL: <https://hub.kyivstar.ua/articles/iot-abo-internet-rechey> (дата звернення: 16.05.2024)

19. Комутатор CISCO CATALYST 2960 URL: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24-s> (дата звернення: 21.05.2024)

20. Огляд протоколів IoT і як вибрати найкращий протокол IoT URL: <https://www.dusuniot.com/uk/blog/best-wireless-protocol-for-your-iot-project/> (дата звернення: 20.05.2024)

21. Основи Інтернету Речей: Датчики та живлення URL: <http://edu.asu.in.ua/mod/book/view.php> (дата звернення: 22.05.2024)

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>70 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |

22. Передача даних в архітектурі ІоТ: MQTT URL: <http://edu.asu.in.ua/mod/book/tool/print/index.php> (дата звернення: 22.05.2024)
23. Проектування Інтернет речей (ІоТ) URL: [https://www.slideshare.net/slides how/iot-79608563/79608563](https://www.slideshare.net/slides/how/iot-79608563/79608563) (дата звернення: 22.05.2024)
24. Розумна розетка TP-LINK міні Тапо P110 URL: [https://rozetka.com.ua/ua/tp\\_link\\_tapo\\_p110/p332487319/](https://rozetka.com.ua/ua/tp_link_tapo_p110/p332487319/) (дата звернення: 21.05.2024)
25. Розумний будинок – плюси і мінуси URL: [https://www.smarthouse.ua/ua/ umnyj-dom-plyusy-i-minusy.html](https://www.smarthouse.ua/ua/umnyj-dom-plyusy-i-minusy.html) (дата звернення: 18.05.2024)
26. Розумний дверний замок NaviCat X8 URL: <https://rozetka.com.ua/ua/397729959/p397729959/> (дата звернення: 21.05.2024)
27. Розумний інфрачервоний пульт TuYa IF Smart URL: <https://ovk.ua/shop/product/smart-wi-fi-ik-pult-dlia-kondicionera> (дата звернення: 21.05.2024)
28. Українські інтернет-провайдери з найбільшою швидкістю доступу (за даними Steam) URL: <https://mezha.media/2023/01/14/ukrainski-internet-provaydery-steam-speed/> (дата звернення: 22.05.2024)
29. Цифровізація: переваги та шляхи подолання викликів URL: <https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv> (дата звернення: 15.05.2024)
30. Що краще: мобільний чи домашній інтернет? URL: <https://linkcom.lviv.ua/shcho-krashche-mobilnyy-chy-domashniy-internet/> (дата звернення: 22.05.2024)
31. Що таке MQTT і для чого він потрібний URL: <https://highload.today/uk/shho-take-mqtt-i-dlya-chogo-vin-potribnij/> (дата звернення 21.05.2024)
32. Що являє собою інтернет речей та які перспективи розвитку має цей напрям URL: <https://gsminfo.com.ua/120474-shho-yavlyaye-soboyu-internet-rechej-ta-yaki-perspektyvy-rozvytku-maye-szej-napryam.html> (дата звернення: 22.05.2024)

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>71 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |

33. 886VA–K9 VDSL Router URL: [https://www.cisco.com/c/en/us/products/colateral/routers/800-series-routers/data\\_sheet\\_c78-613481.html](https://www.cisco.com/c/en/us/products/colateral/routers/800-series-routers/data_sheet_c78-613481.html) (дата звернення 21.05.2024)

34. Bluetooth з низьким енергоспоживанням (BLE): всебічний огляд URL: <https://cqr.company.ua/wiki/protocols/bluetooth-low-energy-ble-a-comprehensive-overview/> (дата звернення: 20.05.2024)

35. Cisco Aironet 3600i URL: <https://networkdiscount.com.ua/ua/p32693912-tochka-dostupa-cisco.html> (дата звернення: 21.05.2024)

36. Cisco UCS C220 M3 LFF URL: <https://servak.com.ua/ua/servers/server-cisco-ucs-c220-m3-lff.html> (дата звернення: 21.05.2024)

37. IEEE. (2012). IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 1: Mac sublayer. IEEE Std 02.15.4e-2012 (Amendment to IEEE Std802.15.4-2011), 121–185.

38. IoT у медицині: від теорії до реальних кейсів URL: <https://hub.kyivstar.ua/articles/iot-u-medyczyni-vid-teoriyi-do-realnyh-kejsiv> (дата звернення: 22.05.2024)

39. Туяа або Smart Life: Що Краще у 2022 році? URL: <https://ishop.kh.ua/tuya-ili-smart-life-cho-luchshe-v-2022-godu.html> (дата звернення: 21.05.2024)

40. Wi-Fi або Ethernet: плюси і мінуси підключень URL: <https://www.agsat.com.ua/ua/info/wi-fi-abo-ethernet-plyusy-minusy-pidklyuchen/> (дата звернення: 19.05.2024)

41. Wi-Fi контролер для керування гаражними воротами, WG-088 URL: <https://techfactory.com.ua/ua/p1544195107-modul-dlya-upravleniya.html> (дата звернення: 21.05.2024)

|     |      |         |        |      |                          |            |
|-----|------|---------|--------|------|--------------------------|------------|
|     |      |         |        |      | КРБКІ.101003.21.01.03 ПЗ | Арк.<br>72 |
| Зм. | Арк. | №докум. | Підпис | Дата |                          |            |



Ім'я користувача:  
Кафедра кібербезпеки

ID перевірки:  
1016347713

Дата перевірки:  
11.06.2024 14:59:40 EEST

Тип перевірки:  
Doc vs Internet + Library

Дата звіту:  
11.06.2024 22:30:31 EEST

ID користувача:  
100008300

Назва документа: Гасюк\_плагіат

Кількість сторінок: 49 Кількість слів: 11124 Кількість символів: 80903 Розмір файлу: 5.82 MB ID файлу: 1016149689

## 4.39% Схожість

Найбільша схожість: 0.89% з Інтернет-джерелом ([https://ela.kpi.ua/bitstream/123456789/42161/1/Khyzhniak-O\\_bakalav...](https://ela.kpi.ua/bitstream/123456789/42161/1/Khyzhniak-O_bakalav...))

|                            |    |       |             |
|----------------------------|----|-------|-------------|
| 4.05% Джерела з Інтернету  | 84 | ..... | Сторінка 51 |
| 1.15% Джерела з Бібліотеки | 94 | ..... | Сторінка 52 |

## 0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

## 0% Вилучень

Немає вилучених джерел

## Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 278

## Anti-Plagiarism v-15.257

**Максимальне співпадіння з одним документом 1.0%**

Словники перевірки: en\_US, ru\_RU, ua\_UA. **Помилко в документах: 11%**

|  |          |         |                             |         |
|--|----------|---------|-----------------------------|---------|
| ID: 129707<br>Назва: IoT-мережа для системи "Розумний замський будинок"<br>Додано в БД: 2024-06-11<br>Автора: Гасюк Є.І.<br>Керівники: Мостовий С.В.<br>Консультанти:<br>Опоненти: | Документ |         | Сумарний збіг по Базі Даних |         |
|  | Символи  | Лексеми | Символи                     | Лексеми |
|  | 73432    | 679     | 920 (1%)                    | 11 (2%) |

### Джерело плагіату

| ID | Опис | Наявність плагіату в документі |         |
|----|------|--------------------------------|---------|
|    |      | Символи                        | Лексеми |

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ  
КАФЕДРИ КІБЕРБЕЗПЕКИ  
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: ЮТ-мережа для системи "Розумний замський будинок"

Автор: Гасюк Євгеній Ігорович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Мостовий Сергій Володимирович

Після аналізу звіту подібності зроблено такий висновок:

| № | Висновок  | Позначка про відповідність |
|---|---|----------------------------|
| 1 | Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.  | відповідає                 |
| 2 | Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи |                            |
| 3 | Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.        |                            |
| 4 | Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.  |                            |

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unicheck складає 95,61%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (<https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf>, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи



Сергій МОСТОВИЙ

Завідувач кафедри кібербезпеки



Юрій КЛЬОЦ

**РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ**

освітнього ступеня «бакалавр»

Дипломник Гасюк Євгеній Ігорович

Тема IoT-мережа для системи "Розумний замський будинок"

Спеціальність 123 – Комп'ютерна інженерія

**Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:**

кількість листів креслень 4; кількість сторінок записки 72

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано та налаштовано IoT-мережу для замського будинку, що дозволяє віднести його до категорії "розумних будинків".

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, У першому розділі проведено огляд та аналіз сучасних технологій реалізації IoT-мереж та безпеки даних у них, виконана постановка задачі. В другому розділі виконано аналіз наявних засобів для проектування та моделювання роботи IoT-мереж та обґрунтовано вибір пакету для роботи. В третьому розділі розроблено фізичну та логічну топологію мережі, обрано схему адресації та маршрутизації, проведено конфігування всіх мережних пристроїв, протестовано проходження трафіку через мережу, визначено вартість впровадження проекту.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Практична цінність результатів дослідження полягає в обґрунтуванні вибору засобів та їх налаштуванню для побудови IoT-мереж для замських будинків.

5. Негативні сторони роботи В роботі відсутній деталізований опис розробки схеми адресації.

---

---

---

---

---

---

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

---

---

---

---

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

---

---

---

---

8. Інші зауваження \_\_\_\_\_

---

---

---

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) \_\_\_\_\_

Бойко Юлій Миколайович

професор кафедри ТМІТ, доктор технічних наук, професор

---

---

---

---

« 12 » \_\_\_\_\_ 06 \_\_\_\_\_ 2024р.

 \_\_\_\_\_ (підпис)