Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

# КВАЛІФІКАЦІЙНА РОБОТА

*бакалавр*
Освітній рівень

Система захисту розумного будинку засобами обладнання Cisco
Назва теми

КРКБ. 190116.19.01.13 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *«Кібербезпека»*
Шифр, назва

Виконав студентка 4 курсу, група КБ-19-1 — Підпис — Якубець А.В. (Ініціали, прізвище)

Керівник — 6.06.23 (Підпис, дата) — Кльоц Ю.П. (Ініціали, прізвище)

Нормоконтролер — 07.06.23 (Підпис, дата) — Мостовий С.В. (Ініціали, прізвище)

До захисту допускаю:
Зав. кафедри кібербезпеки — Підпис, дата — Кльоц Ю.П. (Ініціали, прізвище)

6 06 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека

Освітня програма Освітньо-професійна програма підготовки бакалаврів

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"1" 03 2023 р.

**ЗАВДАННЯ**
**НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Якубець А.В

Прізвище, ім'я, по батькові студента

1. Тема роботи Система захисту розумного будинку засобами обладнання Cisco

Керівник роботи Кльоц Ю.П.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01 березня 2023 р. №5

2. Строк подання студентом роботи на кафедру 01 червня 2023 р.

3. Вихідні дані до проекту (роботи) створити систему для захисту розумного будинку засобами обладнання Cisco. Проаналізувати концепцію розумного будинку та його можливості. Створити віртуальну модель розумного будинку в середовищі Cisco Packet Tracer. Запрограмувати та підключити пристрої у віртуальному середовищі. Дослідити можливі потенційні загрози та вразливості . Сформувати алгоритм для покращення роботи розумного будинку та покращити захист існуючої моделі розумного будинку, щоб забезпечити жителям будинку комфорт та безпеку.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Дослідження та аналіз суміжної предметної області, визначення контексту та мети проекту. Обгрунтування використання систем захисту обладнання Cisco. Розробка захищеної системи віртуальної моделі розумного будинку. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): «Модель в Cisco Packet Tracer, системи безпеки», «Датчики та пристрої всередині розумного будинку», «Швидка навігація», «Топологія розумного будинку», «Інтелектуальна мережа розумного будинку».

6. Консультанти розділів кваліфікаційної роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання при |
| | | | |
| | | | |

7. Дата видачі завдання 1 березня 2023 р.

## КАЛЕНДАРНИЙ ПЛАН

| №з/п | Назва етапів (розділів) кваліфікаційної роботи | Термін виконання етапів проекту (роботи) | Прим |
|---|---|---|---|
| 1 | Вибір і затвердження теми кваліфікаційної роботи | Лютий | – |
| 2 | Пошук теоретичної інформації | Лютий | – |
| 3 | Дослідження існуючих рішень | Лютий | – |
| 4 | Постановка задачі | Березень | – |
| 5 | Розробка моделі | Березень | – |
| 6 | Розробка моделі | Квітень | – |
| 7 | Побудова структури системи | Квітень\Травень | – |
| 8 | Оформлення пояснювальної записки згідно вимог | Травень | – |
| 9 | Оформлення графічної частини | Травень | – |

**Студент** _____ Якубець А.В.
Підпис Ініціали, прізвище

**Керівник проекту (роботи)** _____ Кльоц Ю.П.
Підпис Ініціали, прізвище

# АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система захисту розумного будинку засобами обладнання Cisco».

Автор роботи: Якубець Анастасія Володимирівна.

Керівник роботи: Кльоц Юрій Павлович.

Пояснювальна записка: 73 с., 1 додаток, 39 рис., 40 джерел.

Графічна частина: 12 презентаційних слайдів.

СИСТЕМА ЗАХИСТУ РОЗУМНОГО БУДИНКУ ЗАСОБАМИ ОБЛАДНАННЯ CISCO

Метою роботи є розробка системи захисту засобами обладнання Cisco, яка дозволить покращити комфорт і безпеку жителів будинку.

У роботі було досліджено і проаналізовано предметну область, існуючі методи захисту засобами обладнання Cisco, теоретичну інформацію про обладнання та систем захисту. Створено і розроблену систему захисту віртуальної моделі розумного будинку, яка забезпечить жителям будинку комфорт та безпеку у використанні.

06.06.2023

# ANNOTATION


Course project: Protection system of smart house using Cisco equipment

Author of the work: Yakubets A. V.

Supervisor: Klots Y. P.

Amount - 73 pages, 1 application, 39 figures, 40 sources.

Graphic part: 12 presentation slides.

PROTECTION SYSTEM OF SMART HOUSE USING CISCO EQUIPMENT

The purpose of the work is to develop a security system using Cisco equipment that will improve the comfort and safety of the residents of the building.

The work investigated and analyzed the subject area, existing methods of protection by means of Cisco equipment, theoretical information about equipment and protection systems. A protection system for a virtual model of a smart house has been created and developed, which will provide the residents of the house with comfort and safety in use.


06.06.2023

| Форма | Зона | Позиц | Позначення | Найменування | Кільк. | Прим. |
|---|---|---|---|---|---|---|
| А4 | | 1 | КРКБ.190116.19.01.13 ПЗ | Система захисту розумного | 73 | |
| | | | | будинку засобами | | |
| | | | | обладнання | | |
| | | | | Cisco | | |
| | | | | Пояснювальна записка | | |
| А4 | | 2 | КРКБ.190116.19.01.13 Е8 | Модель в Cisco Packet Tracer, | 1 | |
| | | | | системи безпеки | | |
| А4 | | 3 | КРКБ.190116.19.01.13 Е8 | Датчики та пристрої | 1 | |
| | | | | всередині | | |
| | | | | розумного будинку | | |
| А4 | | 4 | КРКБ.190116.19.01.13 Е8 | Швидка навігація | 1 | |
| А4 | | 5 | КРКБ.190116.19.01.13 Е8 | Топологія | | |
| | | | | розумного будинку | | |
| А4 | | 6 | КРКБ.190116.19.01.13 Е8 | Інтелектуальна мережа | 1 | |
| | | | | розумного будинку | | |

| Зм. | Арк. | № Докум. | Підп. | Дата | КРКБ.190116.19.01.13 ВП | | |
|---|---|---|---|---|---|---|---|
| Розробив | | Якубець А.В. | | 6.06.23 | Система захисту розумного будинку засобами обладнання Cisco<br>Відомість проекту | Літера | Аркуш | Аркушів |
| Перев. | | Кльоц Ю.П. | | 6.06.23 | | н | 1 | 1 |
| Н. контр. | | Мостовий С.В. | | 07.06.23 | ХНУ, КБ-19-1 | | | |
| Затв. | | Кльоц Ю.П. | | 6.06.23 | | | | |

## ЗМІСТ

# ВСТУП

На сьогоднішній день, коли технології у сучасному світі все більше проникають у рутинне життя, розумні будинки або їх ще називають « smart house», користуються популярністю і щоденно потреба лише зростає.

Розумний будинок – це певна система, що постійно інтегрує різні пристрої та мережу для стабільної автоматизації різноманітних функцій та підтримання, можливо, навіть удосконалення, рівня комфорту, враховуючи показники енергоефективності та передусім безпеки. Проте, зростаюча кількість пристроїв, які підключені, диктують нові правила та виклики для покращення захисту від несанкціонованого доступу та кібератак.

Коли мова йде про розумний будинок, то потрібно усвідомлювати, що концепція його складається з різних пристроїв та систем, які безперебійно взаємодіють один між одним для того, щоб автоматизувати та поліпшити комфорт жителів, а також забезпечувати безпеку, враховуючи енергоефективність та зручне керування будинком. Усі пристрої мають змогу взаємодіяти між собою та навіть зовнішніми системами, незалежно чи це провідні, чи це бездротові мережі. Така функція дозволяє жителям будинків контролювати безліч аспектів свого рутинного життя з будь-якої точки та в будь-який час через смартфон, планшет і навіть комп’ютер.

Розумні будинки мають дуже велику і цікаву історію появи та розвитку. Еволюція розпочалась ще з простих систем управління, які вже тоді були автоматизовані. Сама ідея розумних будинків була в 1970-х роках, ще тоді коли перші комп’ютерні системи, які могли керувати будинком, лише розпочали набувати незначну популярність, хоча і мали досить обмежений функціонал та були нелегкі у використанні.

Так як технології розвиваються з неймовірною швидкістю, то з’явились бездротові мережі і у зв’язку з цим розумні будинки ставали доступніші та привабливішими для більш широкої аудиторії. У 1990-х роках, так як винайшли Інтернет та мобільні технології, з’явилась можливість дистанційного управління

розумним будинком. Жителі таких будинків за допомогою комп'ютерів, мобільних пристроїв могли моніторити освітлення, опалення і навіть безпеку.

В останні роки технології розумного будинку підались інтеграції та розширенню, і відбулась поява голосового управління, штучного інтелекту та Інтернет речей (IoT), все це дозволяє підключати ще більшу кількість обладнання в мережу та організовувати складні системи автоматизації. Далі винайшли функції у системах, які можуть розпізнавати обличчя, підтримувати систему безпеки, контролювати системи енергозбережень та ще багато іншого.

Сьогодні можна спостерігати, що розумні будинки є як і в новобудовах, так і вже в багатьох існуючих будинках. Поява розумних будинків не лише підвищують зручність в рутинні та підтримання безпеки, а ще й можуть відповідати за енергоефективність та зниження ціни експлуатацій будинків через зменшення енергетичної споживанності.

Також розумні будинки це те, що власники можуть отримувати розширену інформацію і з легкістю контролювати своє житло за допомогою смартфонів, планшетів або голосових асистентів. Таким чином можна віддалено керувати освітлення, терморегуляцію, системи безпеки та навіть медіа, спостерігати за подіями в будинку.

Ще одною перевагою є те, що розумні будинки можуть бути корисними для людей, які мають фізичні обмеження або для людей похилого віку, це якщо говорити з медичної точки зору, адже розумний будингок включає в себе моніторинг стану здоров'я, коли стан погіршується чи наступає небезпека вмикаються автоматичні сповіщення через вбудовані датчики падінь або через схожі функції, які забезпечують подібний догляд і віжповідають за безпеку.

Але не дивлячись на усі плюси таких нововведень, з кожним днем, розумні будинки стають ще більш інтелектуальними і в майбутньому будуть в кожному будинку.

Загалом, все це результат сучасної технології разом з стрімким розвитком інтернету речей. Для власників домівок це не лише контроль, а й про безпеку. Інтерес впровадження лише зростає у різних сферах життя.

Одна з найвідоміших компаній, яка виробляє мережеве обладнання Cisco, впроваджує нові рішення для захисту розумних будинків. Даний виробник відомий своїми першочерговими технологіями та нововведеннями, а також продуктами, що безперечно гарантують надійний захист мереж та систем зв’язку. Саме про застосування розумних будинків обладнанням Cisco є ключовим об’єктом цієї дипломної роботи.

Метою даної дипломної роботи є аналіз та дослідження системи захисту розумного будинку, базою якої є обладнання Cisco. В даній роботі розглянуті головні принципи роботи розумних будинків, плюси та мінуси їх використання, також можливості, а також певні особливості обладнання Cisco для того, щоб забезпечити безпеку розумного будинку.

# 1 ДОСЛІДЖЕННЯ ТА АНАЛІЗ СУМІЖНОЇ ПРЕДМЕТНОЇ ОБЛАСТІ

## 1.1 Визначення концепції та основні можливості розумного будинку

Розумний будинок або ще « smart house» - це будинок, який відноситься до будинку сучасності. Але це не лише про дизайн та інтер'єр, а й про організацію автоматизованих і інноваційних пристроїв, які в поєднанні забезпечують власникам будинку комфорт та контроль безпеки. Мало того, під цією термінологією розглядається і ресурсозбереження для усіх жителів. Саме дане поняття вперше конфігурувалось Інститутом інтелектульної будівлі у Вашингтоні в 1970-х роках[1].

У зв'язку з тим, що кількість обчислювальних можливостей пристроїв збільшується, то концепція «smart» будинку лише має цілком зрозумілий розвиток через появу систем «Інтернет речей», за вимогами якої було проведено первинну перевірку по стандартах та були сформовані основні правила та рекомендації, щоб побудувати до кінця сформований продукт на рівні цілих систем і навіть невеличких деталей. Наразі вже набагато більше різноманітних рішень.

Система розумного будинку має здатність розпізнавати конкретні сценарії, що виникають у приміщенні, та навіть реагувати на них відповідно[2]. Одна зі систем може керувати діями інших підсистем за допомогою попередньо заданих алгоритмів. Основним аспектом інтелектуальної будівлі є інтеграція окремих компонентів в один централізований керований комплекс. Важливим аспектом та характеристикою «розумного будинку», яка робить його унікальним у порівнянні з іншими методами організації простору проживання, є його передова концепція взаємодії людини з житловим середовищем. У такій концепції людина може швидко налаштовувати бажані умови за допомогою однієї команди, а автоматика відстежує режими роботи всіх інженерних систем та електричних пристроїв.

У такому випадку, необхідність використання кількох пультів при перегляді телебачення, багатьох вимикачів для управління освітленням, окремих блоків для управління вентиляцією і опаленням, системами відоспостережень та

сигналізацією, воротами та іншими елементами, є виключеною. В «розумному будинку» достатньо одного натискання на настінну клавішу, пульт дистанційного керування або сенсорну панель, щоб вибрати один зі сценаріїв, і будинок автоматично налаштовує роботу всіх систем згідно з побажаннями власника, часом доби, погодними умовами та рівнем зовнішнього освітлення[3].

Концепція інтелектуальної будівлі включає наступні принципи:

— Створення інтегрованої системи управління будівлею, яка забезпечує комплексну роботу всіх інженерних систем, таких як освітлення, опалення, вентиляція, кондиціонування, водопостачання, контроль доступу та багато інших.

— Відсутність потреби в обслуговуючому персоналі та передача функцій контролю і прийняття рішень підсистемам інтегрованої системи управління будівлею. В цих підсистемах реалізовано "інтелект", який відповідає на зміну параметрів датчиків та подій, таких як непередбачені ситуації.

— Розробка механізму швидкого відключення та передачі управління людині будь-якою підсистемою інтелектуальної будівлі, якщо необхідно. Людина повинна мати зручний і однаковий доступ до керування та відображення всіх підсистем і компонентів "розумного будинку".

— Забезпечення правильної роботи окремих підсистем у разі відмови центральної керуючої системи або інших частин системи.

— Мінімізація вартості обслуговування та модернізації систем будівлі шляхом застосування загальних стандартів у побудові підсистем, автоматичного конфігурування та виявлення нових пристроїв і модулів при їх додаванні до системи.

— В будівлі передбачено наявність комунікаційного середовища, через яке можна підключати пристрої і модулі. Крім того, система управління може використовувати різні типи фізичних каналів для комунікації, такі як провідні лінії низької напруги, електропровідні лінії високої напруги та радіоканал.

У комплексі автоматизації «розумного будинку» знаходяться такі елементи:

— керування освітленням;

— керування електроприводами;

— регулювання клімату;

— керування вентиляційною системою;

— централізоване керування різними системами, наприклад, домашнім кінотеатром;

— мультірум (система звукового розподілу в різних кімнатах);

— системи відеоспостережння;

— охоронно-пожежна сигналізація (ОПС);

— системи контролю доступу;

— моніторинг електричних навантажень та аварійних станів;

— керування інженерним обладнанням за допомогою сенсорних панелей;

— сервер керування.

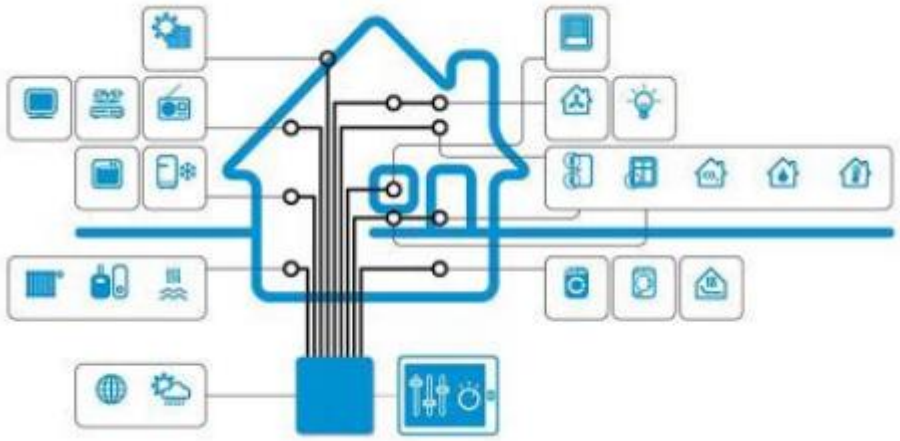


Рисунок 1.1 – концепційна ілюстрація системи розумного будинку

Така будівля має багато переваг, адже система керування дозволяє жителям створювати складні дії у фінкціонуванні в необмеженній кількості, так як всі елементи, що відповідають за виконання можуть функціонувати взаємодіючи та разом[4-6]. Це призводить до того, що впроваджуються ефективні ресурсозберігаючі процедури, а саме:

— Моніторинг доступу та гарантування безпеки.

— Перевірка майже усіх характеристик систем зі швидкою реакцією на зміни.

— Дистанційний контроль і керування будинком, адже усі канали являються цифровими.

Лише одним дотиком можна перетворити порожнє приміщення на затишний гостьовий будинок: автоматично вмикається освітлення, регулюється комфортний мікроклімат, опускаються штори та заповнюється ванна. Немає потреби вставати, щоб елементарно підігріти вечерю – достатньо, щоб хтось заздалегідь поставив її на плиту. Управління домашнім кінотеатром, а також аудіо чи відео аппаратура здійснюється через сенсорні панелі[7].

Завдяки спеціальним регуляторам освітлення, можна не тільки змінювати яскравість лампи при включенні, але й контролювати час, за який досягається яскравість. Функція безперебійного моніторингу освітлення, що зазвичай використовується у приміщеннях придатних для офісів, дозволяє підтримувати встановленого рівня освітленності на робочій поверхні, незалкжно від наявності різних погодніх умов[8]. Автоматчне переключання зовнішнього світла залежно від часу доби і наявності людей поруч не тільки забезпечує додатковий рівень комфорту, а також може відлякувати небажаних гостей. Щоб досягнути такого ефекту використовуються спеціальні датчики світла (рис. 1.2).

Рисунок 1.2 – Датчик світла

Системи постійно моніторять температуру в кожній окремій кімнаті і забезпечують її підтримку в залежності від встановленого рівня, керуючи

клапанами радіаторів або заслінками кондиціонера[9]. Окрім цього, при необхідності система автоматично керує вентиляцією, допомагаючи заощадити кошти завдяки різноманітним режимам роботи, таким як досить комфортний, нічним або режимом «нікого немає в будинку» чи щось типу того. Така зміна режимів необхідна за розкладом чи командою, яку надасть житель будинку. Для певного режиму є достатнім лише одним разом задати потрібну температуру на сенсорі в кожній кімнаті. Системи опалення чи кондиціонування самостійно вимикає свою роботу, щоб зберегти енергетичні ресурси, особливо коли вікна кімнати відкриті для провітрювання. Щоб виконати таакі завдання можна використовувати контролер (рис. 1.3).


Рисунок 1.3 – контролер для підтримки температури

Під час літнього сезону автоматичні панелі жалюзів автоматично нахиляються під певним кутом, що запобігає надмірному проникненню сонячного світла всередину кімнати, однак не обмежуючи пропускання природного світла. Це допомагає уникнути перегріву приміщення і сприяє економії електроенергії, яку витрачає кондиціонер[10].

Система "розумний будинок" здатна звітувати про всі події, які сталися в будинку під час відсутності власників: хто приходив, коли це сталося, тривалість їх перебування, а також розпізнавати обличчя та відслідковувати їхні дії. У разі несанкціонованого проникнення в будинок, система сповістить власника по

телефону і активує сигнал охоронної системи. Крім того, у разі виникнення аварійних ситуацій, наприклад, протікання води, розумний будинок не лише повідомить відповідну службу, але й вживе необхідні заходи для локалізації аварії, наприклад, автоматично зупинить подачу води[11].

У період відсутності власника будинок може імітувати звичний спосіб життя, включаючи освітлення та музику ввечері, створюючи таким чином враження присутності. Система "розумний дім" забезпечує централізований контроль та інтелектуальне керування в приміщеннях житлових, офісних або громадських будівель[12].

Основна структура системи управління включає наступні компоненти:

1. Центральний процесор управління/головний блок управління.

2. Датчики (температури, освітленості, диму, руху тощо).

3. Керуючі пристрої (димери, реле, інфрачервоні емітери тощо).

4. Інтерфейси управління (кнопкові вимикачі, пульти ІЧ, радіопульт, сенсорні панелі, веб/вап інтерфейс).

5. Власна мережа управління, що об'єднує всі зазначені елементи.

6. Керовані пристрої (світильники, кондиціонери, компоненти домашнього кінотеатру тощо).

7. Допоміжні мережі (Ethernet, телефонна мережа, розподілення аудіо та відеосигналу).

8. Програмне забезпечення проекту.

Головна функція центрального процесора полягає в управлінні підпорядкованими пристроями за допомогою різних інтерфейсів, таких як Ethernet, RS-232, RS-485, ІЧ, аналогові та цифрові входи/виходи. Центральний процесор також включає багатозадачну операційну систему, інструментальні засоби програмування та, в деяких випадках, веб-сервер[13].

Датчики розташовуються в стратегічних місцях приміщення і, через проміжні пристрої, підключені до єдиної мережі. Інтерфейси управління забезпечують загальне керування системами "розумного будинку"[14].

Загальний алгоритм роботи системи "розумний будинок" наступний:

— Інформація від датчиків або інтерфейсів передається через внутрішню мережу управління до центрального процесора.

— Програмне забезпечення центрального процесора обробляє отриману інформацію і генерує команди для керуючих пристроїв.

— Команди передаються як через внутрішню мережу, так і через допоміжну мережу.

Способи генерації команд і форма відображення інформації про стан систем визначаються на етапі розробки програмного забезпечення з урахуванням вимог проекту.

Таким чином, система "розумний будинок" надає зручне та централізоване керування різними пристроями та функціями будинку, забезпечуючи автоматизацію і контроль, що покращує комфорт, енергоефективність та безпеку приміщення.

## 1.2 Актуальні методи та засоби забезпечення ефективності розумного будинку

Актуальні методи та засоби ефективності розумного будинку включають в себе безліч різноманітних технологій та інноваційних рішень, які спрямовані на покращення рівня комфорту, а також ефективності енергетики та передусім безпеку будівлі[15]. Ось деякі з них:

1. Інтегровані системи керування в розумних будинках є комплексними платформами, які об'єднують різноманітні підсистеми, такі як освітлення, опалення, кондиціонування повітря, безпека, аудіо-відео системи та інші. Ці системи надають можливість централізованого управління всіма аспектами будинку шляхом використання зрозумілого та інтуїтивного інтерфейсу.

2. Завдяки використанню розумних датчиків і пристроїв, система "розумного будинку" здатна отримувати актуальні дані про стан приміщення. Ці датчики включають датчики руху, датчики освітленості, датчики вологості та інші, які надають системі реальну інформацію про оточуюче середовище. Це

дозволяє системі автоматично реагувати на зміни, наприклад, включати або вимикати світло, регулювати температуру або контролювати рівень безпеки в будинку.

3. Системи "розумного будинку" дозволяють досягти енергоефективного використання енергії шляхом автоматичного керування освітленням та опаленням, що залежить від присутності людей та рівня освітленості. Крім того, ці системи мають здатність моніторити споживання енергії та надавати користувачам детальну статистику та рекомендації з енергозбереження. Таким чином, розумні будинки допомагають ефективно використовувати енергію, зменшуючи непотрібні витрати та сприяючи збереженню ресурсів.

4. За допомогою технології Інтернету речей (IoT), власники розумних будинків мають можливість віддалено керувати різними аспектами свого будинку, використовуючи мобільні пристрої, такі як смартфони або планшети. Це означає, що вони можуть контролювати освітлення, опалення, безпеку та інші системи з будь-якого місця, де є доступ до Інтернету. Такий віддалений контроль над домашнім середовищем надає зручність та гнучкість, дозволяючи власникам забезпечувати комфорт, ефективність та безпеку свого будинку, навіть коли вони знаходяться поза ним.

5. Один із сучасних методів оптимізації розумного будинку полягає у використанні голосового керування. Інтеграція з голосовими асистентами, такими як Amazon Alexa, Google Assistant або Apple Siri, надає можливість користувачам керувати різними пристроями та системами в будинку за допомогою голосу. Цей підхід забезпечує зручність та швидкість управління, а також спрощує доступ до різних функцій розумного будинку. Завдяки голосовому керуванню, користувачі можуть включати й вимикати пристрої, регулювати освітлення, контролювати температуру, запускати аудіо-відео системи та виконувати інші завдання всього лише за допомогою свого голосу. Це створює зручну та інтуїтивно зрозумілу інтерфейс для взаємодії з розумним будинком.

6. Застосування аналітики даних та штучного інтелекту у системах "розумний будинок" дозволяє автоматично налаштовувати режими роботи пристроїв та систем на підставі отриманих даних. Це означає, що штучний інтелект може вивчити звички та поведінку користувача та оптимізувати розподіл енергії для досягнення максимальної ефективності та комфорту. Наприклад, система може виявити, коли користувач зазвичай перебуває вдома і автоматично налаштувати температуру, освітлення та інші параметри відповідно до цих звичок. Крім того, за допомогою аналітики даних, система може надавати користувачам статистику та поради з енергозбереження, що дозволяє їм приймати освідомлені рішення щодо споживання енергії та оптимізувати його відповідно до власних потреб. Таке поєднання аналітики даних та штучного інтелекту робить розумний будинок більш ефективним, зручним та пристосованим до потреб користувача.

7. Безпека та моніторинг є важливою складовою розумного будинку, яка надає розширені можливості для забезпечення безпеки власників. Це включає в собі різноманітні технології та системи, такі як відеоспостереження, датчики протікання води, димові та вуглекислотні датчики, а також системи контролю доступу і тривоги. Інтеграція цих систем дозволяє власникам відстежувати та контролювати стан будинку з використанням мобільних пристроїв, а також отримувати сповіщення в разі виникнення небезпечних ситуацій. Наприклад, власник може переглядати відеозаписи з камер в режимі реального часу або відтворювати їх записи, контролювати рівень вологості, виявляти потенційні загрози пожежі або витоку газу, а також встановлювати режими контролю доступу для управління входами та виходами з будинку. Все це сприяє підвищенню рівня безпеки, спокою та контролю в розумному будинку.

8. "Відкрите API та інтеграція зі сторонніми пристроями" включають можливості для зв'язку та співпраці різних виробників розумних пристроїв та систем "розумного будинку". Це реалізується через відкриті програмні інтерфейси (API), які дозволяють інтегрувати їх з іншими сторонніми пристроями та сервісами. Ця можливість надає користувачам гнучкість та розширені

функціональні можливості. Завдяки інтеграції, можна створювати складні сценарії та автоматизовані взаємодії між пристроями різних виробників. Наприклад, можна створити сценарій, в якому розумний датчик руху включає освітлення певної марки, підключений до системи іншого виробника. Це розширює можливості розумного будинку та сприяє його інтеграції з широким спектром пристроїв та сервісів[16].

## 1.3 Сучасні системи обладнання розумного будинку

Сучасні системи обладнання розумного будинку представляють собою комплексні технологічні рішення, що включають різноманітні пристрої, датчики, засоби комунікації та програмне забезпечення, з метою забезпечення автоматизованого та інтелектуального управління будинком. Вони створюють розумну інфраструктуру, яка може реагувати на потреби та вимоги мешканців, забезпечуючи оптимальний рівень комфорту, безпеки та енергоефективності[17].

Впершу чергу це центральний контролер (рис. 1.4.), що є основним блоком управління, виконує центральну роль у системі розумного будинку, виступаючи як центральний інтелектуальний орган. Він відповідає за обробку і аналіз даних, отриманих від датчиків, прийняття команд від користувача і керування різними пристроями та системами в будинку. Центральний контролер може мати різні форми, включаючи фізичний пристрій або програмне забезпечення, що функціонує на комп'ютері або сервері. Він взаємодіє з усіма компонентами розумного будинку, забезпечуючи координацію їх роботи та забезпечуючи зручний та ефективний контроль і управління для користувача[18].

Рисунок 1.4 – контролер Z-Wave

Датчики (рис. 1.5) в розумному будинку використовуються для отримання реальних даних про стан приміщення та його оточення. Ці сучасні пристрої можуть бути різного типу, включаючи датчики руху, температури, освітленості, вологості, диму, води та інші[19]. Вони функціонують як чутливі приймачі, які постійно моніторять зміни в оточуючому середовищі.

Коли датчик сприймає певну зміну, він передає зібрані дані до центрального контролера, який виступає як мозок системи розумного будинку. Центральний контролер аналізує ці дані та здійснює необхідні дії відповідно до отриманих вимог або налаштувань. Наприклад, якщо датчик руху виявляє присутність людини, центральний контролер може ввімкнути освітлення або регулювати температуру відповідно до заданих налаштувань.

Таким чином, розумні датчики є важливою складовою системи розумного будинку, оскільки вони забезпечують збір точних інформаційних даних, необхідних для оптимального управління будинком та забезпечення комфорту, енергоефективності та безпеки[20].

Рисунок 1.5 – датчик руху, температури, вологості, освітленості та вібрації

Управляючі пристрої виконують команди, які надійшли з центрального контролера. Вони є різноманітними пристроями, призначеними для забезпечення контролю та керування різними аспектами розумного будинку. Управляючі пристрої можуть включати реле, які використовуються для управління електричними колами, димери для регулювання освітлення, клапани для контролю водопостачання, механізми для відкриття та закриття дверей та вікон, контролери систем безпеки та інші подібні пристрої[21].

Ці управляючі пристрої виконують команди, що передаються з центрального контролера, і відповідають на них, забезпечуючи виконання потрібних дій[22]. Наприклад, реле може включати або вимикати електричні пристрої, димери регулюють яскравість освітлення, клапани керують водними потоками, механізми відкривають та закривають двері та вікна, а контролери систем безпеки моніторять та управляють рівнем безпеки в будинку.

Для забезпечення зв'язку між різними пристроями та системами в розумному будинку використовуються різноманітні комунікаційні технології. Ці технології забезпечують передачу даних та команд між пристроями, що дозволяє їм спілкуватися та координувати свої дії[23]. Ось декілька основних методів комунікації, які використовуються в сучасних системах обладнання розумного будинку:

1. Бездротові протоколи. Використання бездротових протоколів, таких як Wi-Fi, Bluetooth, Zigbee або Z-Wave, є популярним способом забезпечення безпровідного обміну даними та командами між пристроями. Wi-Fi забезпечує

широкий охоплення та високу швидкість передачі даних, Bluetooth використовується для короткодистанційного з'єднання між пристроями, а Zigbee та Z-Wave спеціалізуються на низькій споживанні енергії та мережевій стабільності.

2. Провідні засоби комунікації. Провідні засоби комунікації, такі як Ethernet або Powerline, використовуються для підключення пристроїв до мережі за допомогою проводів. Ethernet є широко використовуваним стандартом для передачі даних по мережі, а Powerline використовує електричні проводи в будинку для передачі сигналу даних.

Ці комунікаційні засоби дозволяють пристроям в розумному будинку ефективно спілкуватися між собою та з центральним контролером. Кожна технологія має свої переваги та особливості, і вибір конкретного методу комунікації залежить від потреб і вимог конкретної системи розумного будинку.

Мобільні додатки стали незамінними інструментами для зручного управління розумним будинком. Власники можуть скористатися спеціальними мобільними додатками, які призначені для роботи на смартфонах або планшетах. Додатки також забезпечують доступ до статистики, надсилають сповіщення та дозволяють налаштовувати різні параметри розумного будинку[24].

Функції включають в себе відеоспостереження, датчики протікання води, диму та вуглекислого газу, системи контролю доступу та тривоги. Інтеграція цих систем дозволяє власникам в режимі реального часу відслідковувати та контролювати стан будинку з використанням мобільних пристроїв, а також отримувати сповіщення в разі виникнення небезпечних ситуацій.

Ви можете інтегрувати систему розумного будинку зі смарт-пристроями, такими як голосові помічники, електронні замки, системи безпеки або системи енергоменеджменту[25]. Це дозволяє створювати гнучкі рішення та забезпечувати взаємодію між різними пристроями для забезпечення зручності та ефективності управління розумним будинком.

Загалом, сучасні системи обладнання розумного будинку пропонують широкий спектр функцій та можливостей, спрямованих на підвищення

ефективності, комфорту та безпеки в будинку. Вони надають власникам зручність у керуванні будинком, дозволяючи використовувати мобільні пристрої для здійснення контролю та налаштувань.

## 1.4 Висновок

Метою проектування кваліфікаційної роботи є аналіз та дослідження системи безпеки розумного будинку, використовуючи модель, створену в середовищі Cisco Packet Tracer. Головні завдання проекту включають вивчення принципів та компонентів системи безпеки розумного будинку, а також оцінку їх ефективності та впливу на загальний рівень безпеки будинку.

Буде проведено аналіз вимог безпеки, а саме: аналітика та вивчення основних вимог до безпеки розумного будинку є одним з центральних завдань цього проекту. До таких вимог входить, наприклад, захист від несанкціонованого доступу, виявлення та попередження про можливі загрози та відповідь на потреби користувача. Також важливо обирати компоненти безпеки та розставляти пріоритетність. У процесі проекту необхідно встановити та вибрати відповідні компоненти системи захисту, такі як сенсори, відеокамери, сигналізаційні пристрої та інші елементи безпеки, які будуть оптимальними для використання в середовищі Cisco Packet Tracer.

Звертається особлива увага на проектування самої моделі мережі. У рамках проекту необхідно розробити архітектуру мережі безпеки для розумного будинку, включаючи оптимальне розташування компонентів, налаштування зв'язків між ними та встановлення правил безпеки.

Окрім проектування, існує реалізація. Детальний опис процедури встановлення та налаштування кожного компонента безпеки буде надано, використовуючи можливості середовища Cisco Packet Tracer.

Перевірка та оцінка: Здійснення тестів на безпеку, аналіз отриманих результатів та оцінка ефективності системи безпеки розумного будинку.

Висновки та рекомендації: Після проведення аналізу отриманих результатів можна зробити наступні висновки щодо системи захисту розумного будинку. Оцінка переваг та недоліків системи дозволяє оцінити її сильні та слабкі аспекти. З урахуванням цих висновків, можна надати наступні рекомендації з метою поліпшення системи та досягнення вищого рівня безпеки. Це про покращення захисту від несанкціонованого доступу: Буде розглядатись можливість використання додаткових методів аутентифікації, наприклад двофакторної аутентифікації, з метою збільшення рівня безпеки при доступі до системи. Також для покращення системи виявлення та попередження про загрози: розглядатимуться можливості додаткового встановлення сенсорів та систем виявлення вторгнень з метою раннього виявлення потенційних загроз і швидкого реагування на них. Варте уваги забезпечення фізичної безпеки приміщення: будуть розглянуті можливість розташування відеокамер в стратегічних місцях для виявлення неправомірного доступу та створення доказової бази в разі виникнення інциденту. Забезпечення постійного оновлення та виправлення: систематично оновлювати програмне забезпечення та компоненти системи безпеки, встановлювати доступні оновлення та застосовувати патчі для запобігання використанню можливих вразливостей. Підвищення освіченості користувачів: Здійснити навчання та передати інформацію користувачам стосовно безпеки в розумному будинку, включаючи рекомендації щодо використання надійних паролів, обережного поводження з особистими даними та правильного користування розумними пристроями.

Дотримання цих рекомендацій сприятиме поліпшенню системи захисту розумного будинку та забезпечить підвищений рівень безпеки для користувачів.

# 2 ОБГРУНТУВАННЯ ВИКОРИСТАННЯ СИСТЕМ ЗАХИСТУ ОБЛАДНАННЯ CISCO

## 2.1 Оцінка ризиків та методи усунення

Якщо говорити про оцінювання ризиків, то варто зауважити методи, які це будуть усувати, адже це важливо при створенні розумних будинків.

Впершу чергу, буде розглянутий ризик з точки зору кібербезпеки. Головний ризик полягає в тому що розумний будинок може спровокувати кібератаки, які призводять до несанкціонованого доступу до обладнання, взламуванню систем безпеки та часткове або повне порушення конфіденційності користувачів[26]. Відразу пропонується метод усунення – це використання сильних паролів, шифрувати дані, регулярно оновлювати ПЗ, захищати мережу Wi-Fi, відокремлювати мережу смарт-будинку від головної мережі, додатково можна встановити програмне та апаратне забезпечення, щоб попередньо виявляти та запобігати кібератаки[27].

Ще одним з ризиків є відсутність покриття зв’язку, і це дуже велика перешкода для того, щоб керувати розумним будинком, таке трапляється після аварій чи відключенні Інтернету. Для вирішення такої проблеми важливо мати резерви зв’язку, це може бути GSM-модуль або локальну мережу, щоб був доступ при втраті основного зв’язку[28].

Якщо говорити про конфіденційність даних, то можливий ризик збору та примінення особистих даних жителів, які порушують приватність цієї особи, тобто персональної інформації. Для усунення цієї проблеми можна забезпечити приватність даних користувачів розумних будинків, виробники обладнання повинні приділяти належну увагу захисту особистої інформації. Це можна зробити шляхом використання різноманітних механізмів для шифрування, для обмеження доступу до даних лише авторизованим особам, анонімізації збираємих даних та отримання згоди користувачів на збір та використання їх даних.

Є ризик фізичної безпеки, він полягає в тому, що злам будинку може взагалі спричинити небезпеку для мешканців, викриваються системи безпек, поломка

дверей або повне вимкнення систем моніторингу розумного будинку. Для уникнення фізичних ризиків необхідно прийняти фізичні заходи безпеки, такі як встановлення міцних дверей та вікон, використання систем відеоспостереження, сигналізації та систем контролю доступу[29]. Крім того, необхідно використовувати надійне програмне забезпечення та обмежувати доступ до системи розумного будинку лише авторизованим користувачам з високим рівнем довіри.

Є ризик відмови або поломки пристроїв. Це спричиняє втрату функціональності системи в цілому[30-33]. Для запобігання виникненню проблем з відмовою пристроїв, критично обирати високоякісне обладнання від надійних виробників. Зберігання резервних копій даних та наявність можливості швидкого відновлення системи також мають велике значення у мінімізації наслідків відмови пристроїв.

Існує залежність від технологій. Це про проблеми, які виникають у разі застаріння чи відмови версії системи. Вирішити можна за допомогою реглярних оновлень ПЗ і обладнання в ілому, що є важливо для підтримки сумісності та функціонування системи в майбутньому.

Так вся система розумного будинку є електричною, може трапитис електропожежа чи відбутись технічні несправності. Щоб такого не відбулось потрібно регулярно проводити чек-ап стану електричних мереж і всього обладнання, а також підтримувати осблуговування ПЗ і мати резервне джерело, щоб неперервно функціонувала система.

Якщо говорити про мешканців розумного будинку, можна передбачити ризик недоступності та незручності використання. Це відбувається тоді коли користувачі не розуміють корисності від такої системи. Тому важливо при створенні інтерфейс користувача розробляти легким та доступним для усіх вікових категорій.

Якщо говорити про економічну сторону, то і тут є ряд ризиків. Не усі можуть дозволити собі впровадження та обслуговування розумного будинку,

тому є різні можливості фінансування, але від цього залежить вибір енергоефективних пристроїв для довгострокової експлуатації.

Останнім є ризик, який відповідає за здоров’я та екологію. Впровадження розумних систем впливає на стан здоров’я та довкілля через появу електромагнітного випромінювання, відбувається переліміт по споживанні енергії і це не контролюється на екологічних ресурсах. Щоб це мінімізувати потрібно обирати екологічні і безпечні компоненти та дотримуватись усіх рекомендацій по безпеці і моніторингу енергоспоживання.

Завершуючи, оцінка ризиків та прийняття відповідних заходів для усунення їх є важливим завданням у контексті розумних будинків з метою забезпечення безпеки, приватності та ефективності систем. Це охоплює широкий спектр аспектів, включаючи кібербезпеку, втрату зв'язку, приватність даних, фізичну безпеку, відмову пристроїв, залежність від технологій, електропожежу, технічні несправності, недоступність та незручність використання, економічні ризики та вплив на здоров'я та екологію.

Для зменшення цих ризиків, необхідно вживати наступні заходи. Використання безпечних мережевих протоколів та кібербезпечних практик, резервних методів зв'язку, шифрування та обмеження доступу до особистих даних, встановлення фізичних заходів безпеки, регулярне обслуговування та оновлення системи, розробка спрощеного та зрозумілого інтерфейсу користувача, бюджетне планування, підтримка енергоефективності та екологічної свідомості — все це важливі кроки у забезпеченні безпечності та надійності розумних будинків.

## 2.2 Опис обладнання Cisco

Компанія Cisco Systems, що також відома під назвою Cisco, займає визначне місце серед провідних технологічних компаній, спеціалізуючись у сфері розробки, виробництва та продажу мережевого обладнання, програмного

забезпечення та послуг зв'язку. Заснована у США в 1984 році, вона швидко набула статусу визнаного лідера у галузі комп'ютерних мереж.

Cisco надає широкий асортимент продуктів та рішень для створення й управління комп'ютерними мережами, включаючи комутатори, маршрутизатори, мережеві контролери, пристрої безпеки, веб-камери, IP-телефонію, відеоконференції, хмарні платформи та інфраструктуру Інтернету речей (IoT). Крім того, Cisco забезпечує послуги мережевого консультування, технічної підтримки та навчання для своїх клієнтів.

Компанія має широкий спектр клієнтів у різних сферах, включаючи підприємства, постачальників послуг, урядові організації та освітні установи. Вона також активно досліджує та просуває нові технології, такі як штучний інтелект, машинне навчання, блокчейн та Інтернет речей (IoT), щоб задовольнити зростаючі потреби ринку[34].

Розділяють декілька головних серій обладнання Cisco. Перший це Cisco Catalyst, відомі ще як комутатори для місцевих або ще локальних мереж. Користуються популярністю Catalyst 9000, Catalyst 6000, Catalyst 3000.

Рисунок 2.1 – комутатор з серії Catalyst

Комутатор, відомий також як "switch" англійською мовою, є пристроєм для підключення й передачі даних між пристроями в локальній мережі (LAN). Цей

пристрій виконує роль центрального маршрутизатора, керуючи рухом даних в мережі та надсилаючи пакети інформації до відповідних пристроїв.

Комутатор виконує ряд завдань, але його основна функція полягає в забезпеченні комутації даних на основі фізичного адресу мережевої карти, відомого як MAC-адрес. Комутатор проводить аналіз MAC-адресів пакетів даних, щоб визначити, які пристрої повинні отримати ці пакети, що допомагає знизити непотрібний трафік в мережі і покращити її продуктивність. Комутатор розподіляє пропускну здатність мережі між підключеними пристроями, забезпечуючи ефективну передачу даних та уникнення конфліктів в мережі.

Також комутатор може підтримувати віртуальні локальні мережі (VLAN), що дозволяє розділити мережу на окремі сегменти і керувати доступом пристроїв. Це забезпечує підвищену безпеку та гнучкість мережі. Комутатори можуть контролювати швидкість передачі даних, враховуючи потреби підключених пристроїв. Це особливо корисно, коли деякі пристрої вимагають більшої пропускної здатності, наприклад, для потокового відео або передачі великих файлів[35].

В цілому, комутатори виконують важливу роль в локальних мережах, забезпечуючи з'єднання комп'ютерів, принтерів, серверів, IP-телефонів та інших пристроїв у мережевому середовищі. Вони дозволяють створити швидку, надійну та ефективну мережу, в якій пристрої можуть спілкуватися та обмінюватися даними.

Наступний пристрій - Cisco ISR (Integrated Services Router) представляє собою інтегровані маршрутизатори (рис. 2.2), які об'єднують в собі функціональність як маршрутизатора, так і комутатора. Вони особливо підходять для використання в розгалужених офісах і віддалених місцях розташування[36].

Рисунок 2.2 – маршрутизатор від Cisco

Маршрутизатор - це пристрій, що використовується в мережах для передачі пакетів даних між різними мережами. Він вирішує, який шлях краще використовувати для передачі даних з одного пристрою до іншого, опираючись на інформацію про мережу та її структуру. Основна функція маршрутизатора полягає у прийнятті, аналізі та виборі оптимального маршруту для передачі пакетів даних[37]. Виконує декілька важливих функцій:

— Маршрутизація - це процес визначення оптимального шляху для передачі пакетів даних від відправника до отримувача, враховуючи наявні маршрути, стан мережі та її пропускну здатність.

— Таблиці маршрутизації - це набори даних у маршрутизаторах, які зберігають інформацію про доступні шляхи до різних мереж та обрані маршрути.

— Фільтрація трафіку - це можливість маршрутизаторів проводити сортування пакетів даних на підставі різних критеріїв, таких як IP-адреси, протоколи, порти та інші, з метою контролю та забезпечення безпеки мережі.

— Підсилення сигналу. Деякі маршрутизатори можуть виконувати функцію підсилення сигналу, що дозволяє зміцнювати сигнали та збільшувати відстань передачі даних.

— Об'єднання мереж. Маршрутизатори можуть забезпечувати інтеграцію різних типів мереж, таких як локальні мережі (LAN), метрополітенські мережі

(MAN) та глобальні мережі (WAN), з метою забезпечення зв'язку та обміну даними між ними.

Загалом, маршрутизатори відіграють важливу роль у встановленні маршрутів для передачі даних у мережі, забезпечуючи ефективну та безпечну комунікацію між пристроями та різними мережами.

Наступний пристрій Cisco ASA (рис. 2.3.) - це група файрволів, які призначені для забезпечення безпеки мережі шляхом захисту від зовнішніх загроз. Вони широко використовуються для створення віртуальних приватних мереж (VPN) та контролю доступу, що дозволяє забезпечити безпеку та обмежити доступ до ресурсів мережі.


Рисунок 2.3 – файрвол Cisco

Файрволи відіграють вагому роль у забезпеченні безпеки мереж та захисту від потенційних загроз зовнішнього середовища. Вони виступають як перешкода між внутрішньою мережею та незахищеною зовнішньою сферою, здатні контролювати трафік, що протікає через них[38]. Виконують наступні функції:

— Забезпечення безпеки мережі. Файрволи виявляють та блокують небажаний трафік, такий як шкідливі програми, віруси, вторгнення та атаки хакерів. Це допомагає запобігти несанкціонованому доступу до мережі та забезпечує захист конфіденційної інформації.

— Управління доступом. Файрволи встановлюють правила та політики доступу, які визначають, які пристрої та користувачі мають право входити в мережу та отримувати доступ до ресурсів. Це дозволяє обмежити доступ лише для авторизованих осіб і запобігти несанкціонованій активності.

— Мережеві ресурси. Файрволи забезпечують створення безпечних тунельних з'єднань для віртуальних приватних мереж (VPN). Це дозволяє забезпечити захищену комунікацію між віддаленими мережами або віддаленими користувачами, що працюють з ресурсами мережі.

— Аналіз мережевого трафіку. Файрволи виконують моніторинг мережевого трафіку та збирають інформацію про активність мережі. Це дозволяє виявляти потенційні загрози, атаки та аномальну поведінку мережі, сприяючи своєчасному реагуванню та забезпеченню безпеки мережі.

Узагальнюючи, файрволи є необхідною складовою мережевої інфраструктури, яка гарантує безпеку, забезпечує конфіденційність та надає доступ до ресурсів. Вони дозволяють організаціям ефективно управляти мережевим трафіком і захищати важливі дані від потенційних загроз.

Ще одним важливим пристроєм від серії Cisco є Cisco Aironet (рис. 2.4) - це лінійка бездротових точок доступу Wi-Fi, які забезпечують можливість підключення до мережі безпосередньо через бездротовий інтерфейс[39]. Вони підтримують різні стандарти бездротового зв'язку Wi-Fi і широко застосовуються в офісних приміщеннях, громадських місцях, готелях та інших середовищах, де необхідний бездротовий доступ до мережі.

Рисунок 2.4 - Cisco Aironet

У даному пристрої, звичайно ж, є як і переваги, так і недоліки. Почнемо з переваг:

— Cisco Aironet забезпечує швидкі та надійні бездротові підключення з високою продуктивністю, підтримуючи різні стандарти Wi-Fi. Це дозволяє передавати дані зі значною швидкістю та надійністю у бездротовому середовищі.

— Точки доступу Cisco Aironet славляться своєю надійністю та стабільністю. Вони гарантують надійне та стійке бездротове підключення з мінімальними перебоями, завдяки надійним компонентам та оптимізованій роботі.

— Cisco Aironet має широкий спектр функціональних можливостей, які включають підтримку різних режимів роботи, управління мережею, захист, розширені налаштування та інші. Ці можливості дозволяють користувачам гнучко налаштовувати мережу згідно з їхніми потребами та вимогами.

— Cisco Aironet демонструє високу сумісність з іншими продуктами Cisco, що сприяє безпроблемній інтеграції та створенню єдиної мережевої інфраструктури. Ця сумісність спрощує управління та підтримку мережі, дозволяючи легко управляти та налаштовувати різні компоненти мережі в одному централізованому середовищі.

Щодо недоліків:

— Ціна обладнання Cisco Aironet може бути вищою в порівнянні з іншими точками доступу, що присутні на ринку, вимагаючи певного інвестування.

— Для оптимального використання функцій та можливостей Cisco Aironet може вимагатися певний рівень знань або спеціалізовані навички в налаштуванні та керуванні цим обладнанням.

— Для ефективної роботи Cisco Aironet може вимагатися наявність додаткового обладнання або інфраструктури, наприклад, мережевих контролерів або додаткових антен. Це може вплинути на загальну складність та вартість впровадження.

Але все відносно і потрібно враховувати, що усі «плюси» та «мінуси» залежить від моделі та конфігурації.

Це лише кілька з серій обладнання, які випускає компанія Cisco, але насправді вона має широкий асортимент продуктів та рішень. Крім обладнання, Cisco також надає різноманітне програмне забезпечення для управління мережами, моніторингу та забезпечення безпеки. До таких програм входять Cisco IOS, Cisco DNA Center, Cisco Security Manager та багато інших.

В процесі створення розумного будинку за допомогою обладнання Cisco, використовуються різні пристрої, які сприяють автоматизації та керуванню різними аспектами домашнього середовища. Неможливо розумний будинок уявити без Cisco Smart Wi-Fi роутерів (рис.2.5). Вони є надійними та продуктивними пристроями, які забезпечують стабільне та швидке бездротове підключення до Інтернету для всіх пристроїв у будинку.


Рисунок 2.5 - Cisco Smart Wi-Fi роутер

Також розумний будинок не може уснувати без камер. Cisco IP-камери (рис. 2.6) надають можливість віддалено спостерігати за подіями, що відбуваються в будинку, завдяки системі відеостеження. Вони забезпечують безпеку та контроль над приміщеннями, дозволяючи збирати відеодокази та здійснювати нагляд за різними областями.


Рисунок 2.6 - Cisco IP-камери

Важливо мати при впровадженні усіх пристроїв ще Cisco Smart Switches (рис. 2.7) дозволяють керувати мережевими підключеннями у будинку, забезпечуючи високу швидкість передачі даних та ефективне управління трафіком. Вони забезпечують гнучкість та контроль над мережею, дозволяючи налаштовувати параметри підключення, моніторити трафік і забезпечувати безпеку мережевого середовища.

Рисунок 2.7 - Cisco Smart Switches

Обладнання, яке варте уваги Cisco Smart Lighting (рис. 2.8) - розумна система освітлення, яка дозволяє зручно та ефективно керувати освітленням у

будинку за допомогою мобільного пристрою або голосових команд. Ця система надає можливість змінювати яскравість, колір та режими освітлення, створювати розклади включення/виключення світла, а також інтегруватись з іншими розумними пристроями для створення автоматичних сценаріїв освітлення.

Рисунок 2.8. - Cisco Smart Lighting

Не всі вбачають важливість Cisco Smart Thermostat (рис.2.9). Насправді, це розумний термостат, який забезпечує автоматичне регулювання температури в будинку з метою забезпечення комфортних умов для мешканців і енергоефективності. Цей пристрій може виявляти присутність людей в приміщенні та враховувати їхні переваги щодо температури, включати або вимикати систему опалення або кондиціонування повітря за необхідністю та регулювати температурні параметри згідно з попередньо встановленими розкладами або налаштуваннями. Він також може бути інтегрований з іншими розумними пристроями для створення цілісної системи управління кліматом у будинку.


Рисунок 2.9 - Cisco Smart Thermostat

Коли будинок великий і має велику територію, то необхідно встановити Cisco Smart Security System (рис.2.10) - це комплексна інтегрована система безпеки, яка включає в себе різноманітні функції та пристрої для забезпечення безпеки будинку (рис.2.11). Ця система включає сигналізацію, яка спрацьовує при спостереженні небажаних подій, таких як вторгнення або пожежа, та сповіщає про них власника або служби безпеки. Вона також включає відеоспостереження, що дозволяє віддалено контролювати та спостерігати за подіями в будинку через відеокамери. Контроль доступу забезпечує обмежений доступ до будинку для невповноважених осіб, наприклад, через електронні ключі, картки або біометричні системи. Крім того, система може мати інші функції безпеки, такі як датчики диму, витоку газу, системи автоматичного виклику служб екстреної допомоги та інші. Cisco Smart Security System надає повний спектр заходів безпеки, які допомагають захистити будинок та його мешканців.

Рисунок 2.10 – Smart Camera, за допомогою якої можна зробити цілу систему.

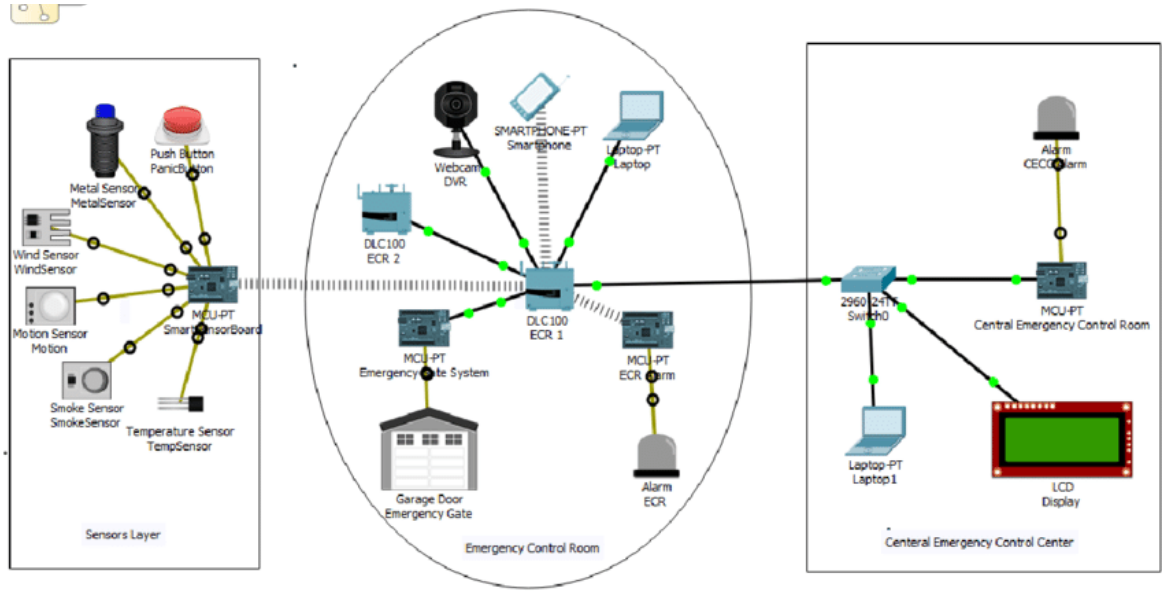



Рисунок 2.11 – модель в Cisco Packet Tracer, системи безпеки

Cisco Smart Appliances - це підключені до мережі пристрої для побуту, такі як холодильники, пральні машини, пилососи та інші. Ці пристрої оснащені спеціальними функціями, що дозволяють їх керувати та контролювати віддалено з використанням мережі Інтернет. Завдяки цьому, ви можете отримати доступ до них через мобільний пристрій або комп'ютер і здійснювати різні операції, наприклад, встановлювати температуру в холодильнику, розпочинати або зупиняти прання у пральній машині, керувати режимами роботи пилососа і багато іншого.

Cisco Smart Appliances дозволяють забезпечити більш зручне та ефективне використання побутової техніки, а також економити енергію та ресурси. Ви можете налаштувати розклад роботи пристроїв, контролювати їх стан та

споживання енергії, а також отримувати повідомлення про стан пристроїв або нагадування про потребу у певних операціях, наприклад, заміні фільтра у пилососі.

Cisco Smart Appliances сприяють автоматизації та удосконаленню вашого домашнього середовища, забезпечуючи зручність, ефективність та більші можливості контролю за побутовими пристроями.

Всі ці пристрої встановлюють зв'язок один з одним, формуючи інтегровану мережу в розумному будинку. Ця мережа створює зручну, безпечну та енергоефективну систему управління різними аспектами побутового життя в будинку.

Інтегруючи ці пристрої, ви отримуєте можливість керувати їх діями та отримувати взаємопов'язану інформацію. Наприклад, при виході з будинку система може автоматично вимкнути світло, відключити неактивні пристрої та активувати безпекову систему. Ви також маєте можливість налаштовувати графік роботи пристроїв, щоб ефективно використовувати ресурси. Наприклад, ви можете автоматично регулювати температуру відповідно до вашого графіка, використовуючи інформацію про ваші активності.

Ці розумні пристрої допомагають спростити і автоматизувати ваші повсякденні рухи в будинку. Вони працюють відповідно до вашого налаштування і забезпечують зручність, безпеку та ефективність управління освітленням, опаленням, електроприладами та іншими системами. Завдяки інтелектуальній мережі, ви стаєте більш свідомим та ефективним у використанні ресурсів, отримуєте більшу зручність та контроль над вашим домашнім середовищем.

## 2.3 Функції безпеки, доступні в обладнанні Cisco

Cisco пропонує розширений набір інструментів та функцій безпеки, які спеціально розроблені для забезпечення захисту розумного будинку. Ці функції включають різноманітні технології, що дозволяють виявляти, блокувати та усувати потенційні загрози, забезпечуючи надійну оборону мережі та

підключених пристроїв. Обладнання Cisco дозволяє налаштовувати правила брандмауера, використовувати системи виявлення та запобігання вторгнень для виявлення та блокування шкідливої активності, встановлювати захищені віртуальні приватні мережі для безпечного обміну даними, а також використовувати різні методи аутентифікації та авторизації для контролю доступу до мережі. В додаток до цього, обладнання Cisco забезпечує захист бездротових мереж, використовуючи шифрування та інші заходи безпеки. Крім того, системи моніторингу та інцидентного реагування допомагають забезпечити постійний контроль над безпекою розумного будинку та швидку реакцію на будь-які потенційні загрози.

У системі обладнання Cisco виявляються вбудовані можливості брандмауера, які забезпечують контроль над потоком мережевого трафіку та блокують небажані підключення або кібератаки. Ці функції брандмауера дозволяють аналізувати та фільтрувати вхідний та вихідний трафік, що проходить через мережу розумного будинку. Вони перевіряють кожен мережевий пакет на відповідність заданим правилам безпеки та забезпечують, що лише дозволений трафік пропускається через систему. Це забезпечує захист розумного будинку, блокуючи небажаний доступ або атаки зовнішніх загроз, таких як хакерські атаки або вторгнення в мережу. Брандмауер Cisco забезпечує надійний контроль трафіку та гарантує безпеку мережі розумного будинку[40].

Обладнання Cisco має можливості виявлення та запобігання вторгнень (IDS/IPS), які сприяють виявленню та блокуванню незвичайної або шкідливої активності в мережі розумного будинку. Ці функції IDS/IPS використовуються для аналізу трафіку мережі та виявлення потенційно шкідливих або небажаних дій.

Функція виявлення вторгнень (IDS) аналізує мережевий трафік та шукає ознаки, що можуть свідчити про атаку або порушення безпеки. Це можуть бути незвичайні шаблони трафіку, спроби несанкціонованого доступу або аномальна активність від пристроїв. Якщо IDS виявляє потенційну загрозу, він може

сповістити адміністратора системи або вжити інших заходів для подальшого розслідування та блокування.

Функція запобігання вторгнень (IPS) діє активніше, блокуючи або відхиляючи шкідливий трафік або вторгнення в реальному часі. Вона використовує правила та шаблони для розпізнавання відомих атак та запобігає їхньому успішному завершенню. IPS може автоматично блокувати доступ пристроїв або виконувати інші заходи для запобігання шкідливій активності.

Ці функції IDS/IPS обладнання Cisco допомагають виявляти та блокувати різні види атак, такі як вторгнення, DDoS-атаки або шкідливе програмне забезпечення. Це забезпечує додатковий рівень захисту розумного будинку, дозволяючи вчасно реагувати на потенційні загрози та зменшувати ризик виконання успішних кібератак.

У системі обладнання Cisco доступна функція веб-фільтрації, яка дозволяє контролювати та фільтрувати веб-трафік в розумному будинку. Ця функція дозволяє блокувати доступ до небезпечних або небажаних веб-сайтів, а також контролювати використання веб-додатків.

Завдяки веб-фільтрації, обладнання Cisco може сканувати веб-трафік і перевіряти веб-сайти на наявність шкідливих або небажаних вмісту, таких як віруси, шпигунське програмне забезпечення або дорослий контент. У разі виявлення таких сайтів, веб-фільтр блокує доступ до них, запобігаючи можливій загрозі для безпеки мережі та пристроїв розумного будинку.

Крім того, функція веб-фільтрації дозволяє контролювати використання веб-додатків, таких як соціальні мережі, медіаплеєри або інші онлайн-сервіси. Адміністратор мережі може налаштувати правила, щоб обмежити доступ до цих додатків або контролювати їх використання, що сприяє безпеці та регулюванню використання інтернету в розумному будинку.

Завдяки функції веб-фільтрації обладнання Cisco забезпечує додатковий рівень безпеки та контролю над веб-трафіком, що дозволяє захистити розумний будинок від небезпек та небажаного контенту в Інтернеті.

У розумному будинку обладнання Cisco дозволяє використовувати віртуальні приватні мережі (VPN), що забезпечують створення зашифрованого тунелю для безпечної комунікації між різними пристроями та мережами.

Завдяки використанню VPN, встановлюється конфіденційне та захищене з'єднання між пристроями в розумному будинку через інтернет. Це досягається шляхом шифрування даних, що передаються по мережі, та створення приватного тунелю, через який проходить вся комунікація. Це забезпечує високий рівень безпеки та конфіденційності, оскільки дані зашифровані і недоступні для сторонніх осіб.

Використання VPN дозволяє захистити розумний будинок від можливих загроз, таких як перехоплення даних, переслідування або несанкціонований доступ. Він також дозволяє забезпечити безпеку підключення до віддалених мереж або інтернет-ресурсів з розумного будинку. VPN створює віртуальну приватну мережу, яка розширює безпечний доступ до інтернету та дозволяє взаємодіяти з мережевими ресурсами з будь-якого місця в розумному будинку.

Завдяки використанню VPN, обладнання Cisco забезпечує захищену та безпечну комунікацію між пристроями та мережами у розумному будинку, що дозволяє зберегти конфіденційність даних та забезпечити надійну безпеку мережі.

Обладнання Cisco надає підтримку різних методів аутентифікації та авторизації, що дозволяють контролювати доступ до мережі та пристроїв у розумному будинку. Ці методи включають використання паролів, сертифікатів або біометричних даних.

Аутентифікація є процесом перевірки та підтвердження ідентичності користувача або пристрою, що намагається отримати доступ до мережі. Обладнання Cisco дозволяє використовувати паролі, які вимагають введення вірного ідентифікаційного коду, а також сертифікати, які підтверджують легітимність користувача або пристрою. Крім того, можна використовувати біометричні дані, такі як відбитки пальців або сканування обличчя, для ідентифікації та автентифікації користувачів.

Авторизація визначає рівень доступу, який користувач або пристрій має після успішної аутентифікації. Обладнання Cisco дозволяє налаштовувати права доступу до різних мережних ресурсів та пристроїв в розумному будинку на основі ідентифікації користувача або пристрою. Це забезпечує контроль над тим, хто має доступ до різних функцій та можливостей в мережі розумного будинку.

Завдяки різним методам аутентифікації, таким як паролі, сертифікати та біометричні дані, обладнання Cisco забезпечує безпеку та контроль доступу до мережі та пристроїв у розумному будинку. Це дозволяє уникнути несанкціонованого доступу та зберегти приватність та безпеку системи розумного будинку.

Обладнання Cisco має можливості, які дозволяють забезпечити безпеку бездротових мереж в розумному будинку, таких як Wi-Fi, шляхом використання шифрування та інших методів захисту для запобігання несанкціонованому доступу.

Cisco надає функціонал, що дозволяє застосовувати різні методи захисту бездротових мереж. Один з таких методів - використання шифрування, яке дозволяє захистити передавані дані в бездротовій мережі від перехоплення та несанкціонованого доступу. Обладнання Cisco підтримує різні протоколи шифрування, такі як WPA2 (Wi-Fi Protected Access 2), які забезпечують високий рівень конфіденційності та безпеки.

Крім того, обладнання Cisco має інші методи захисту бездротових мереж, такі як фільтрація MAC-адрес, налаштування бездротових обмежень, контроль доступу до мережі та використання захищених паролів. Ці методи допомагають запобігти несанкціонованому підключенню до бездротової мережі та забезпечують контроль над доступом до мережевих ресурсів.

Завдяки функціоналу безпеки обладнання Cisco, бездротові мережі, такі як Wi-Fi, в розумному будинку можуть бути ефективно захищені від несанкціонованого доступу. Використання шифрування та інших методів безпеки дозволяє забезпечити конфіденційність даних та надійну безпеку мережі розумного будинку.

Cisco пропонує комплексні рішення для моніторингу безпеки та інцидентного реагування в розумному будинку. Ці рішення дозволяють виявляти потенційні загрози та надавати швидку реакцію на інциденти для забезпечення безпеки та нормальної роботи мережі.

Системи моніторингу безпеки Cisco забезпечують постійний нагляд за мережею розумного будинку з метою виявлення потенційних загроз. Вони аналізують мережевий трафік та спостерігають за аномальною або підозрілою активністю. Це може включати виявлення незвичайних підключень, атак на мережу, спроб перехоплення даних або несанкціонованого доступу. При виявленні таких загроз системи моніторингу безпеки Cisco генерують сповіщення або спрацьовують автоматичні заходи для забезпечення безпеки мережі.

Крім моніторингу, Cisco також пропонує рішення для інцидентного реагування. Ці рішення дозволяють швидко реагувати на виявлені загрози та вживати заходів щодо їхнього усунення. Це може включати автоматичне блокування небезпечного трафіку, перепрограмування мережевих правил або активізацію системи попередження адміністратора. Крім того, рішення Cisco дозволяють відновити нормальну роботу мережі після інциденту шляхом відновлення заблокованих ресурсів або переключення на резервні системи.

Моніторинг безпеки та інцидентне реагування, що пропонує Cisco, гарантують постійну охорону мережі розумного будинку. Вони допомагають виявити загрози та швидко реагувати на них, забезпечуючи безпеку та надійну роботу системи.

Функції безпеки, які надає обладнання Cisco, допомагають забезпечити високий рівень захисту розумного будинку від кібератак, несанкціонованого доступу та небажаних подій. Ці функції гарантують збереження конфіденційності, цілісності та доступності системи.

Обладнання Cisco забезпечує ефективний захист шляхом використання різних механізмів безпеки, таких як брандмауер, виявлення та запобігання вторгнень, веб-фільтрація, віртуальні приватні мережі та інші. Ці функції

працюють разом, щоб виявляти, блокувати та відвертати потенційні загрози для розумного будинку.

За допомогою брандмауера, обладнання Cisco контролює рух трафіку мережі та блокує небажані підключення або кібератаки. Виявлення та запобігання вторгнень дозволяє виявляти незвичайну або шкідливу активність в мережі та блокувати її перед тим, як вона спричинить шкоду. За допомогою веб-фільтрації, обладнання Cisco блокує доступ до небезпечних або небажаних веб-сайтів і контролює використання веб-додатків.

Використання віртуальних приватних мереж (VPN) дозволяє забезпечити безпечну комунікацію між пристроями та мережами у розумному будинку шляхом використання зашифрованого тунелю. Це забезпечує захист конфіденційності передаваних даних та запобігає їх перехопленню.

Завдяки цим функціям безпеки, обладнання Cisco забезпечує надійний захист розумного будинку, зберігаючи конфіденційність даних, цілісність системи та доступність пристроїв та мережі.

## 2.4 Висновок

Врахувавши всі «за» та «проти» важко не підкреслити переваги вибору саме обладнання Cisco і все має цілком логічні обгрунтування:

— Cisco є провідним виробником мережевого обладнання та систем захисту, що характеризується високою надійністю. Вони спеціалізуються на створенні обладнання високої якості, яке працює стабільно та надійно. Використання систем захисту Cisco допомагає запобігати можливим загрозам та атакам на мережу, забезпечуючи надійність функціонування обладнання.

— Системи захисту обладнання Cisco пропонують широкий асортимент функцій і можливостей для забезпечення безпеки мережі. Вони включають у себе різноманітні функції, такі як мережевий інспектор безпеки, системи виявлення вторгнень, контроль доступу, шифрування трафіку та багато інших, що сприяють ефективному управлінню та захисту мережі.

— Системи захисту Cisco розроблені з урахуванням потреб різних масштабів мереж та компаній. Вони можуть легко розширюватись від невеликих офісних мереж до великих корпоративних мереж з великою кількістю вузлів. Це надає можливість використовувати системи захисту Cisco у будь-якому розмірі мережі та гарантує їх ефективну функціональність.

— Cisco пропонує рішення безпеки, які вповні інтегруються з іншими продуктами та рішеннями Cisco. Це дозволяє забезпечити повністю інтегровані системи безпеки, які здатні працювати разом з іншими компонентами мережі. Інтеграція з іншими рішеннями Cisco створює комплексну систему безпеки, що гарантує високий рівень захисту у всіх аспектах мережі.

— Cisco надає постійну підтримку своїх систем захисту, включаючи оновлення програмного забезпечення та виправлення вразливостей. Це дозволяє користувачам завжди мати доступ до найновіших захисних технологій та забезпечує постійну безпеку мережі. Cisco гарантує, що їх системи захисту постійно оновлюються, щоб враховувати змінюючіся загрози та забезпечувати надійний рівень захисту для користувачів.

Так як сфера є досить перспективна і завжди буде вимагати сучасних рішень, то на ринку є і конкуренти Cisco, такі як: Juniper Networks, Huawei та Check Point Software Technologies.

Juniper Networks, як провідний конкурент Cisco у галузі мережевих технологій, пропонує різноманітне мережеве обладнання та рішення безпеки. Незважаючи на це, Juniper Networks може мати меншу розповсюдженість та екосистему порівняно з Cisco, що може вважатися їхнім недоліком.

Huawei, як глобальний постачальник мережевих технологій та систем безпеки, пропонує широкий спектр продуктів і рішень, які конкурують з Cisco. Однак, Huawei може зіткнутися з обмеженою присутністю на деяких ринках та проблемами, пов'язаними з безпекою даних, що створюють певні ризики для користувачів.

Check Point Software Technologies зосереджується на наданні рішень безпеки мережі та вогневих стін. Вони пропонують передові технологічні рішення

для захисту від загроз та атак. Однак, їхнім недоліком може бути менша розмаїтність мережевого обладнання порівняно з Cisco.

Також перед реалізацією даної дипломної роботи потрібно зауважити про важливість цієї теми на сьогоднішній час.

Так як зростає популярність на впровадження розумних будинків і вони стають з кожним днем все більше популярніші і не менш з тим, їхнє зростання зумовлює важливість досліджень різноманітних систем захисту. Розумні будинки мають великий потенціал стати невід'ємною частиною людського рутинного життя і варто зрозуміти весь потенціал ризиків та знайти способи вирішення загально. Буде розглядатись модель і всі методи та підходи будуть вимагати індивідуальних рішень, щоб жителям цього будинку забезпечити належну безпеку та комфорт. Мова йде про не лише будинок, а й про особистий простір усіх членів сім'ї. Коли в будівлі проживають довгий час або планують це робити, то це про захист приватності і не тільки, а ще й особистої інформації, яка може бути конфіденційною. Розумні будинки за весь час накоплюють багато інформації про мешканців, навіть звички, усі пристрасті та відстежують поведінку. При попередніх дослідженнях систем захисту вдалось створити механізм, що гарантує конфіденційність, цілісність інформації та захисту персональних або просто важливих даних, аби для того, щоб уникнути неправомірності використання та доступу.

Щоденно зростає кількість кібератак та вторгнень. Розумні будинки чутливі до таких явищ та можуть спричинити негативні наслідки в умовах безпеки жителів та заподіяти шкоду для інфраструктури будівлі. Дослідження таких систем може виявити майбутні вразливості і надати ряд рекомендацій щоб ефективно протидіяти кібератакам.

Ну і елементарно, завжди можна вбачати ріст навіть найдосконалішої системи. Покращення технічного розвитку. Все це сприяє появі нових технологій та нововедень. Адже це про створення цілої бази знань та кращих практик, які можуть знадобитись для виробників при розробці або ж покращенні своєї продукції, які безперечно будуть краще пристосовуватись до ряду вимог безпеки.

Тому, досліджувати сисистеми захисту розумних будинків є надважливим завданням, яке в майбутньому буде сприяти захисту приватності для жителів цієї будівлі, їх безпеці та розвитку безпечніших технологій для майбутнього в усьому світі.

# 3 РОЗРОБКА ЗАХИЩЕНОЇ СИСТЕМИ ВІРТУАЛЬНОЇ МОДЕЛІ РОЗУМНОГО БУДИНКУ

## 3.1 Загальні підходи до формування віртуальної моделі

"Розумний будинок" відноситься до зручного домашнього середовища, в якому пристрої та апаратні засоби можуть бути керовані віддалено з будь-якого місця за допомогою мобільного або іншого мережевого пристрою через Інтернет-підключення. У розумному будинку пристрої взаємодіють між собою через Інтернет, дозволяючи користувачу контролювати такі функції, як безпечний доступ до будинку, температура, освітлення, домашній кінотеатр та інші.

Всі пристрої в розумному будинку з'єднані між собою та доступ до них можна отримати за допомогою одного центрального пристрою, такого як смартфон, планшет, ноутбук або ігрова консоль. Завдяки системі домашньої автоматизації, користувач може керувати замками дверей, відеокамерами, системою клімат-контролю, освітленням та навіть побутовими пристроями, такими як холодильник чи пральна машина, з однієї системи. Ця система встановлюється на мобільному або іншому мережевому пристрої, дозволяючи користувачу створювати графіки часу для виконання певних змін у будинку.

Самонавчальні вміння належать до розумних побутових приладів, дозволяючи їм вивчати графіки власника будинку та адаптуватися за потребою. Розумні будинки, що мають можливість керування освітленням, дозволяють власникам зменшити споживання електроенергії та зекономити на витратах. Деякі системи домашньої автоматизації повідомляють власника про будь-які рухи в будинку, коли він відсутній, тоді як інші можуть активувати сигналізацію або звернутися до поліції чи пожежної служби в невідкладних ситуаціях. "Розумний будинок" є однією з технологічних складових "Інтернету речей" (IoT) (рис. 3.1).

Пристрої можуть бути зв'язані між собою за допомогою проводового або бездротового з'єднання. Бездротові системи є більш простими у встановленні, що призводить до зниження вартості реалізації. З іншого боку, проводові системи вважаються більш надійними, але мають певний недолік - вищу вартість.

Встановлення такої системи може вимагати від власників будинків витрати десятків тисяч доларів.

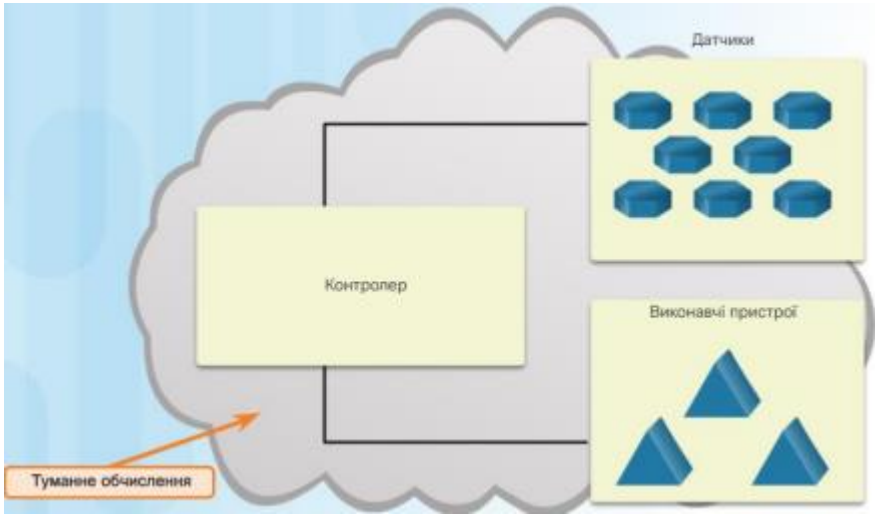



Рисунок 3.1 – Зразок топології IoT

Контролери відповідають за збір даних з датчиків та забезпечення мережевого або Інтернет-з'єднання. Контролери можуть бути оснащені різноманітними функціями та можливостями. Контролери можуть мати можливість приймати негайні рішення, або вони можуть передавати дані на більш потужний комп'ютер для проведення аналізу. Цей більш потужний комп'ютер може бути підключений до тієї ж локальної мережі, що і контролер, або може бути доступний тільки через підключення до Інтернету.

Датчики часто працюють у взаємодії з виконавчими механізмами. Виконавчі механізми отримують електричний струм і перетворюють його на фізичну дію. Наприклад, якщо датчик виявляє перевищення температури в приміщенні, він передає дані про температуру на мікроконтролер. Мікроконтролер може передавати ці дані до виконавчого механізму, який у свою чергу активує кондиціонер.

Більша половина сучасних пристроїв, особливо лічильники повітря в шахтах та лічильники води вимагають у всіх фермерських середовищах бездротового підключення, щоб функціонувати. Так як, багато датчиків виконують свою роботу за допомогою акумуляторів та сонячних батарей, то при створенні такої системи важливо врахувати усі нюанси зі споживанням енергії

вище перерахованих пристроїв. З метою покращення та забезпечення більшої доступності для усіх людей, з різним економічним статусом, рекомендується використовувати опції з низьким рівнем енергоспоживання.

Інтелектуальний будинок можна уявити як складний механізм, де кожен елемент виконує свою специфічну функцію, подібно до складання пазла. У такому контексті, безперебійний зв'язок між всіма цими елементами має велике значення. Для забезпечення комунікації між пристроями використовуються як дротові, так і бездротові протоколи. Розглянемо найпопулярніші протоколи, які забезпечують ефективну взаємодію між елементами системи.

Протокол 1-Wire є простим у реалізації і досить надійним дротовим протоколом. Основна лінія передачі інформації використовує двонаправлену шину, яка складається з пари дротів. Перший дріт відповідає за передачу даних і живлення, а другий використовується як заземлення. Така мережа має топологію з однією шиною, де обладнання підключається до загального кабелю. Можливе використання витої пари як основи для цього протоколу, при цьому пристрої підключаються через RJ-розетки. Передача даних може здійснюватись на значні відстані, до 300 метрів, за виконання певних умов. Для підключення обладнання достатньо всього двох проводів, що також робить його вигідним з точки зору вартості. Проте, слід відзначити, що низька стійкість до відмов є одним з недоліків цього зв'язку. Зазвичай його вибирають економні користувачі, які планують використовувати лише основний набір функцій "розумного дому".

Незважаючи на свою сорокарічну історію, протокол X10 активно застосовується. Його головним перевагою є висока універсальність. X10 може працювати як дротовий протокол, але для його використання не потрібно спеціально прокладати кабель. Він передає сигнал по стандартному електропроводу. Більше того, X10 може забезпечувати зв'язок з бездротовими пристроями. Для цього використовуються трансивери, які перетворюють сигнал у формат, придатний для передачі по кабелю. Серед переваг застосування X10 можна виділити зручне керування, простий і швидкий монтаж, а також зручні і

гнучкі налаштування окремих елементів мережі. Цей протокол також доступний за ціною.

Проте X10 має кілька значних недоліків. По-перше, протокол є дуже повільним. Передача однієї команди або адреси займає приблизно ¾ секунди, що стає досить помітним при використанні двостороннього зв'язку. Крім того, в мережі X10 може бути передана лише одна команда в конкретний момент часу. Також для використання протоколу може знадобитися певна модифікація існуючої електропроводки.

Протокол KNX відноситься до одного з найскладніших стандартів, що потребують складності в інсталяції та проектуванні. Для передачі інформації можуть використовуватися електрична мережа, радіоканал або вита пара. Зазвичай віддається перевага останньому варіанту, де шина укладається разом з силовими дротами в процесі будівництва. Топологія мережі може бути різноманітною, включаючи лінійну, зіркову або деревовидну структури.

Протокол KNX пропонує зручне управління та широкий функціонал. Його перевагами є просте перепрограмування, можливість модернізації, а також незалежне проектування та монтаж сигнальних і силових ліній. Крім того, протокол дозволяє підключати велику кількість пристроїв до мережі.

Однак, слід зазначити, що протокол KNX має деякі недоліки, такі як відносно повільна передача даних і висока вартість. Важливо враховувати, що цей протокол призначений переважно для професійного використання.

Wi-Fi є популярним бездротовим протоколом, який використовується майже в будь-якій домашній системі. Основне призначення Wi-Fi - забезпечення управління розумним будинком з мобільного пристрою. Існують спеціальні програми для різних платформ, які дозволяють це зробити. Wi-Fi також використовується для зв'язку з автономними пристроями, що працюють окремо від автоматизованої системи. Плюсом Wi-Fi є можливість розгортання мережі без необхідності прокладання кабелю. Частоти, на яких працює протокол, не створюють перешкод і є безпечними для людей. Обладнання, яке підтримує Wi-Fi, широко поширене, що гарантує його сумісність з іншими пристроями.

Однією з головних переваг Wi-Fi є висока швидкість передачі даних. Проте, слід відзначити деякі недоліки цього стандарту, такі як висока вартість модулів, їх велика енергоємність і обмежена можливість тривалої роботи обладнання від автономних джерел живлення.

Cisco Packet Tracer являється повноцінним інструментом щоб симулювати мережі та пристрої, але він не є спеціалізованим засобом щоб створити віртуальну модель «smart house». Недивлячись на це, можна використовувати дане середовище для того, щоб створити основну мережу інфраструктури, що забезпечує конект між різноманітними девайсами розумного будинку.

Основні підходи формування цієї віртуальної моделі включають в собі наступній кроки:

— Визначення типів усіх пристроїв розумного будинку для моделювання, це термостати, лампочки, сигналізація безпеки та інших. Можна обрати з наявних в Packet Tracer, а можна і самостійно створити власні, за допомогою існуючих компонентів.

— Підключення до мережі обладнання. Потрібно створити віртуальну мережу, додаючи необхідні маршрутизатори, комутатори та інші. Підключити пристрої до мережі використовуючи усі наявні мережеві порти.

— Налаштування обладнання. Потрібно налаштувати кожний пристрій, яких входить в систему розумного будинку в залежності від функцій та можливостей, кожного з них.

— Сценарій. Щоб сторити сценарії роботи віртуальної моделі розумного будинку також знадобиться Packet Tracer. Це може бути увімкнення світла в певній кімнаті, де сенсор руху буде виявляти активність. Є функції програмування та покращення, які вже є в середовищі Cisco.

Також потрібно зауважити, що Cisco Packet Tracer е надасть усіх можливостей повноцінної системи розумного будинку, це як і інтеграції з рельними сенсорами, усіма датчиками чи обладнання сторонніх виробників. Таке середовище призначене суто для навчання мережевими технологіями і моделюванням базових сценаріїв роботи пристроїв у мережі.

3.2 Розробка модифікованої моделі розумного будинку в середовищі Cisco Packet Tracer

Початковим кроком для розміщення пристроїв на їхніх відповідних і остаточних місцях є створення схеми будинку. В цьому контексті була завантажена схема майбутнього житла, на якій розташовані всі пристрої Інтернету речей (IoT), що утворюють потрібну інтелектуальну мережу всередині будинку - Home Cluster (рис.3.2).

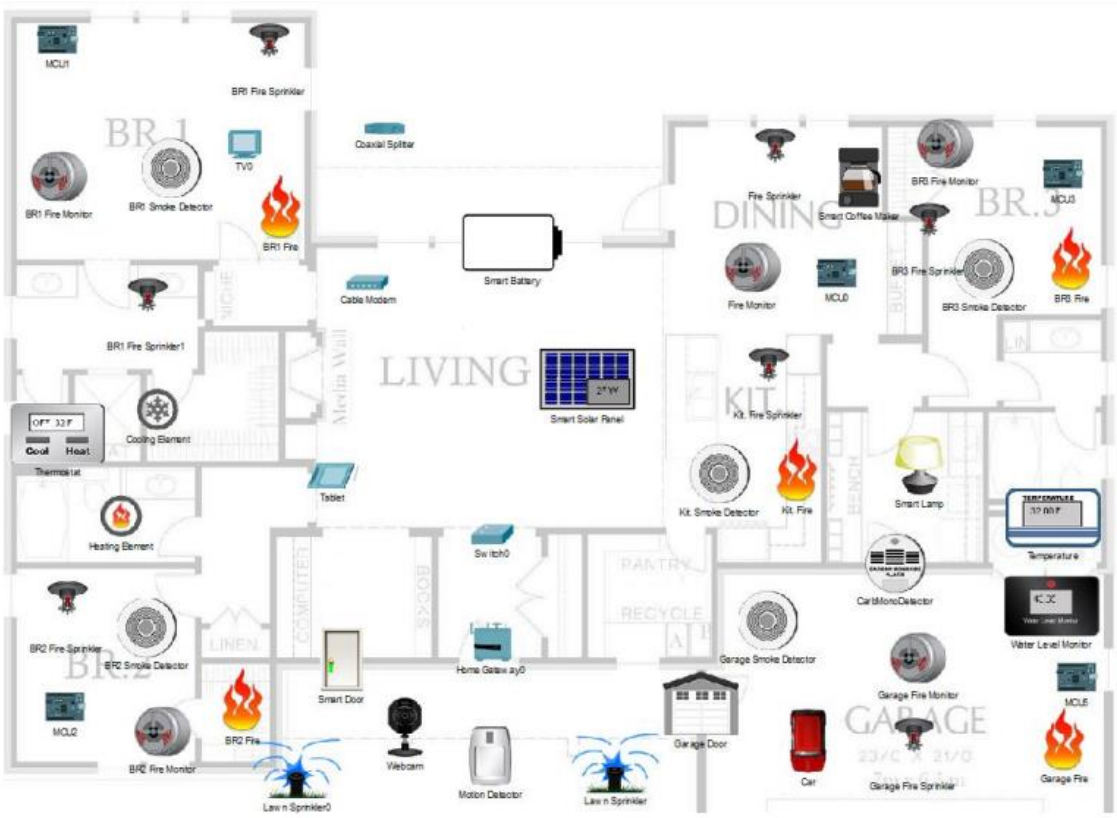



Рисунок 3.2 – датчики та пристрої всередині розумного будинку

В модель входять такі пристрої та датчики: BR Fire Monitor, BR Fire Sprinkler, BR Smoke Detector використовуючи двічі, Cable Modem, Car, Coaxial Splitter, Cooling Element, Fire, Garage Door, Heating Element, Home Gateway, Lawn Sprinkler, MCU, Motion Detector, Smart Battery, Smart Coffe Maker, Smart Door, Smart Solar Panel, Tablet, Temperature, Termostat, TV, Water level Monitor, Webcam.

Були створені кнопки швидкої навігації для забезпечення зручності користування (рис. 3.3). При натисканні кнопки "Home", користувач буде перенесений всередину "розумного будинку", де він зможе спостерігати

налаштовані IoT-пристрої. А при натисканні кнопки "IPS-Internet", користувач буде перенаправлений до кластеру IPS-Інтернету, де він зможе моніторити свій IoT-дім з будь-якої точки світу. Це надає можливість віддаленого спостереження за домашньою системою незалежно від місця перебування.

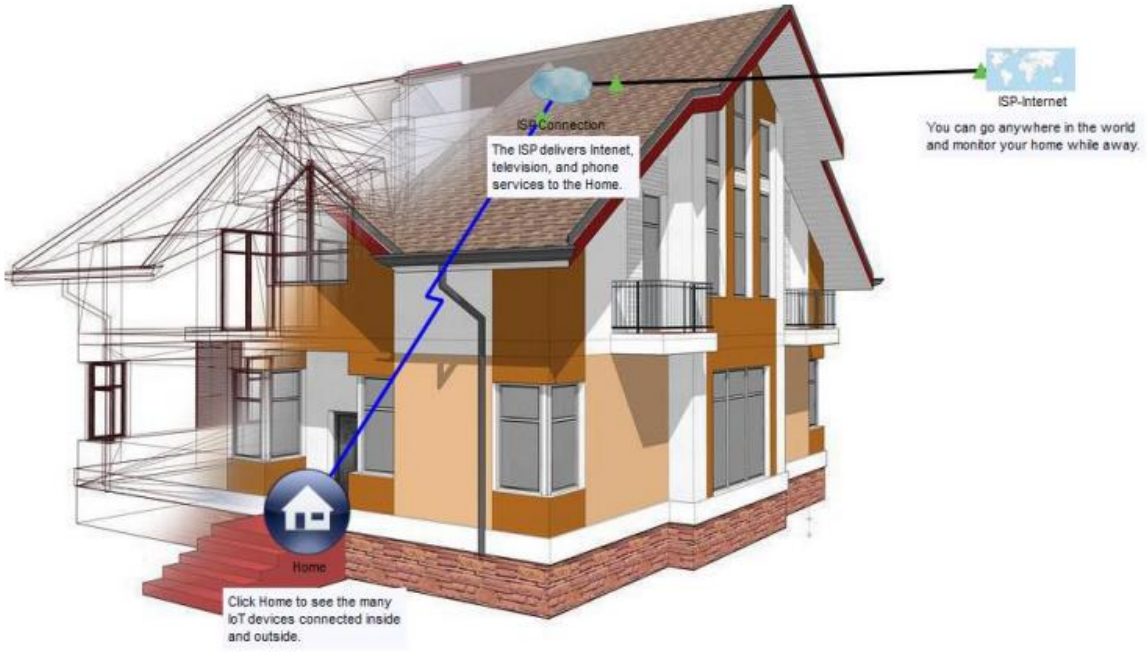



Рисунок 3.3 – Швидка навігація

Мережа (рис.3.4) також складається з:

— інтелектуальних пристроїв (IoT Devices);

— датчики, які потрібні для збору інформації;

— мікроконтролер є пристроєм, який групує датчики та передає інформацію від сервера до кінцевих вузлів. Він виконує роль посередника, який забезпечує комунікацію між сервером і датчиками, дозволяючи передавати дані від центральної системи до кінцевих пристроїв;

— домашній шлюз є ключовим пристроєм, який використовується для управління системою та забезпечення з'єднання з зовнішньою мережею. Він виконує роль центрального вузла, який координує комунікацію між різними пристроями в домашній мережі та забезпечує доступ до Інтернету. Домашній шлюз забезпечує управління різними функціями та послугами розумного

будинку, такими як освітлення, опалення, безпека, а також забезпечує з'єднання зі зовнішніми сервісами і додатками для дистанційного керування та моніторингу;

— канали передачі даних є важливим компонентом комунікаційних систем, що включає в себе як логічні, так і фізичні засоби передачі інформації. Логічні канали визначають параметри передачі даних, такі як швидкість передачі, пріоритети, рівень безпеки, а також можуть включати протоколи і алгоритми, що регулюють потік даних. Фізичні канали, у свою чергу, забезпечують фізичний шлях передачі даних, включаючи кабелі, оптичні волокна, бездротові канали та інші технології зв'язку;

— хмара є зовнішньою платформою або сервісом, який забезпечує можливість доступу до обчислювальних ресурсів та зберігання даних через Інтернет. У відношенні бази даних, хмара може виступати як централізоване сховище для зберігання статистичних даних, службової інформації та інших даних, що використовуються в системі. За допомогою хмарних рішень, користувачі можуть зручно зберігати, обробляти та отримувати доступ до цих даних з будь-якого місця за допомогою Інтернету. Хмарні сервіси зазвичай надають масштабованість, надійність та гнучкість, що дозволяє ефективно управляти даними та забезпечує простоту використання для користувачів.

— мобільні пристрої є асортиментом пристроїв, що використовуються користувачем для управління системою розумного дому.

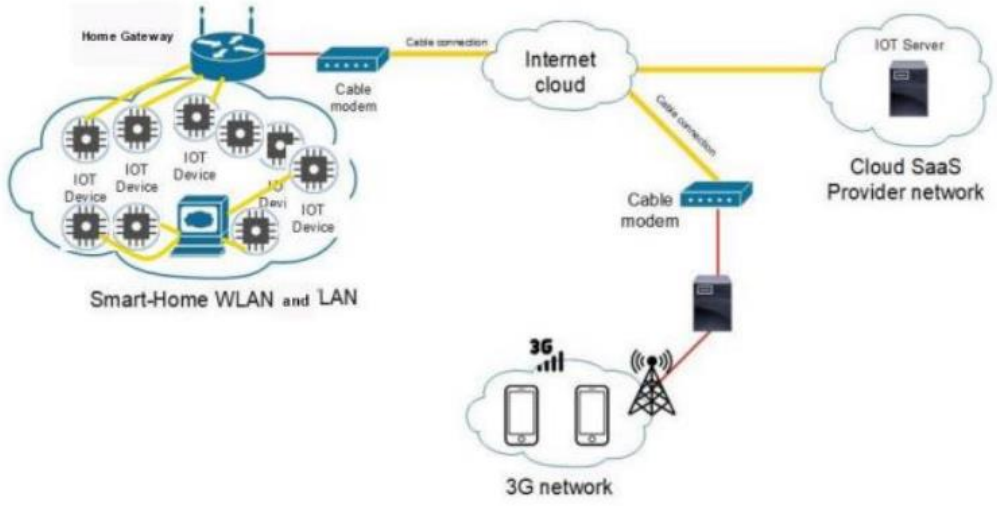



Рисунок 3.4 – Топологія розумного будинку

Користувачеві потрібно самостійно налаштувати бездротову (WLAN) та провідну (LAN) мережі для з'єднання з керуванням "розумним будинком". Користувач може підключатися до системи, будучи внутрішній мережі Wi-Fi, а також віддалено підключатися до панелі управління за допомогою смартфона через мережу 3G/4G. Також було створено два веб-сервери. Перший - Entertainment веб-сервер (рис.3.5), на який користувач може зайти для розваг, введши www.entertainment.com у пошуковій стрічці браузера на планшеті або мобільному пристрої.

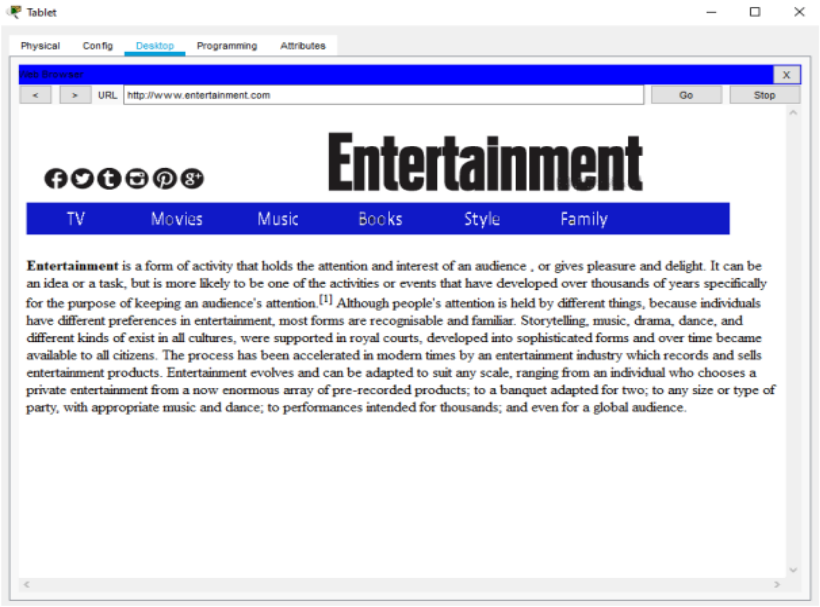



Рисунок 3.5 – HTTP сторінку веб-серверу Entertainment

Сервер для реєстрації нових користувачів у мережі– Registration веб-сервер (рис.3.6). Можна у пошуковому рядку з планшета чи телефону ввести www.register.com і далі просто зареєструвати усіх жителів будинку або друзів, яким довіряєте, щоб була змога управління будинком, після чого буде доступ до функцій конфігурації. На рисунку 3.7 зображені поля, де потрібно вводити логін та пароль для входу в систему. Окрім цього, даний веб-сервер використовується як віддалений для налаштування та управління обладнанням, але це потрібно передбачити і в системі встановити (рис.3.8).

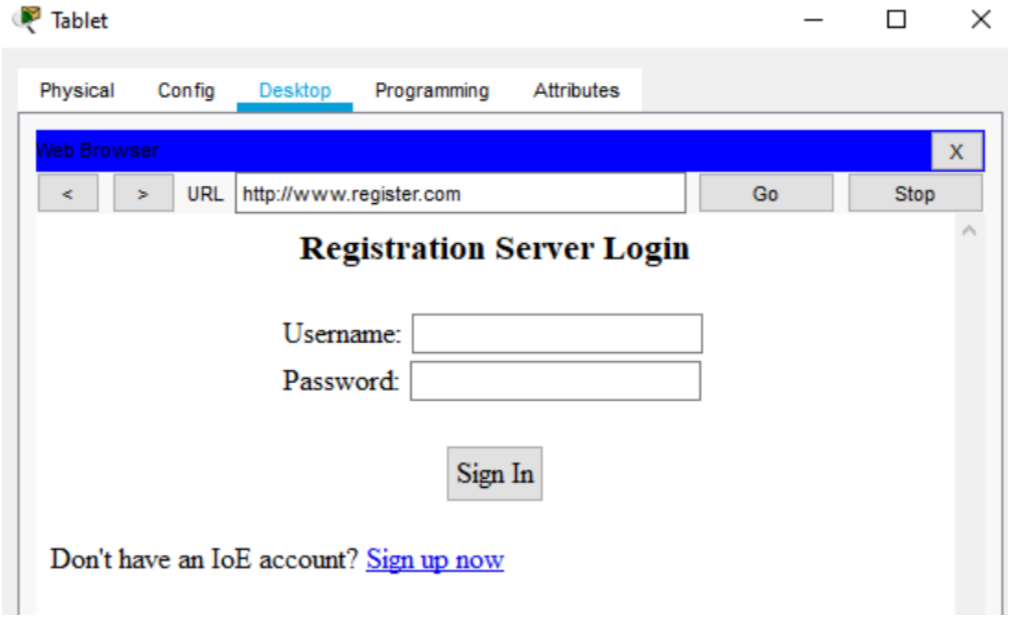



Рисунок 3.6 – Сторінка авторизації

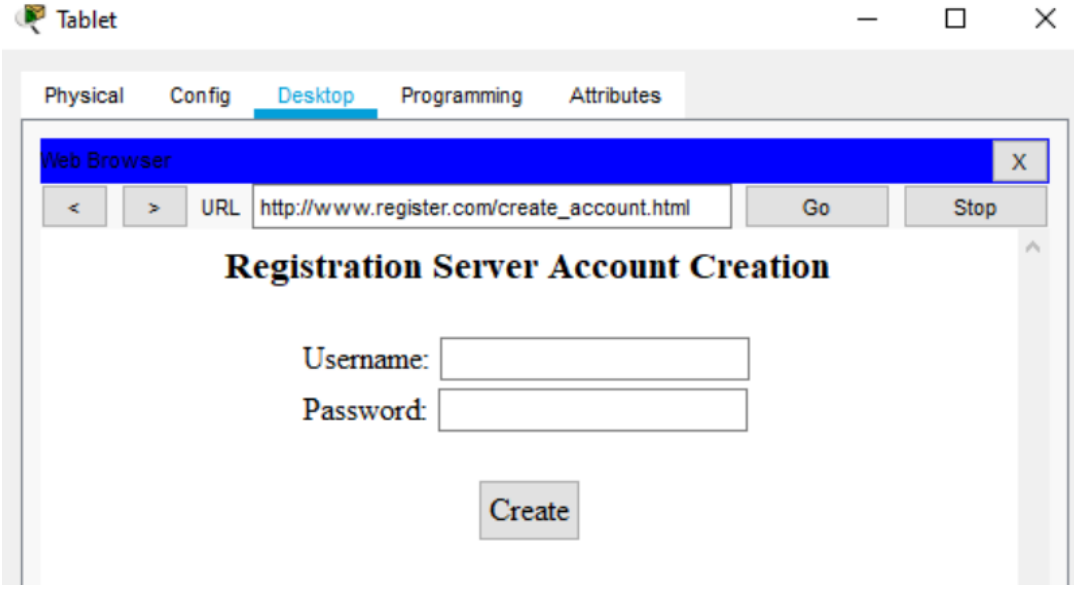



Рисунок 3.7 – Сторінка створення аккаунта

Для забезпечення зв'язку між елементами схеми, ми використовуємо реєстраційний сервер, який підключається до роутера IoT Register за допомогою мідного кросоверного кабелю, а сервер Entertainment підключається до Entertainment роутера та роутера IoT Register відповідним чином. Роутери з'єднуються між собою за допомогою портів Gigabit Ethernet (для серверів використовуються порти Fast Ethernet). Роутер IoT Register з'єднується з головним роутером (Main Router) за допомогою мідного кросоверного кабелю, використовуючи порти Gigabit Ethernet. Головний роутер в свою чергу

підключений до комутатора ISP та центрального офісного сервера. Центральний офісний сервер підключений до провайдера Telefonica за допомогою коаксіального кабелю Cell Tower, який поширює сигнал 3G/4G для мобільних пристроїв. Крім того, комутатор підключений до DNS сервера за допомогою мідної витої пари через інший порт Fast Ethernet.

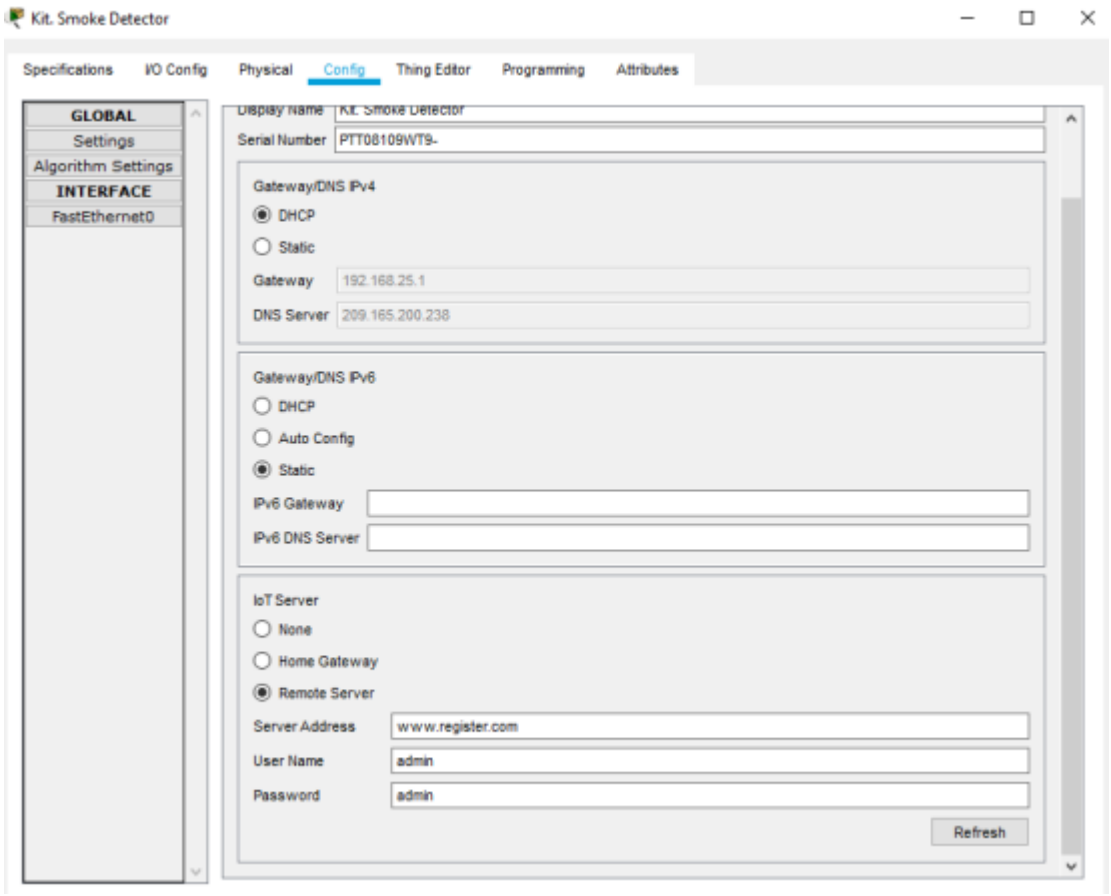



Рисунок 3.8 – конфігурація детектору диму, який використовується як віддалений сервер

В хмарі ISP було додано порти PT-Cloud-NM-1CFE та два порти PT-Cloud-NM1CX, щоб забезпечити підключення до локальної мережі (LAN), модема та сервера стільникового зв'язку відповідно. Для цього використовується коаксіальний кабель, який з'єднується з коаксіальним спліттером. Коаксіальний спліттер, у свою чергу, підключений до телевізора та модема.

З метою проведення більш точного тестування, була відключена можливість отримання сигналу 3G на планшеті. Натомість, для смартфону ми ввімкнули цю

можливість і вказали назву провайдера - Telefonica, яка є однаковою для вишки і сервера.

Мікроконтролери були підключені до інтелектуальних пристроїв IoT Custom Cable дротом. Цим же дротом були з'єднані батарея, кавоварка, веб-камера, "смарт-двері" і сонячна батарея для забезпечення їх роботи за допомогою сонячної енергії. Також було з'єднано термостат з приладом опалення і охолодження.

Пристрої в розумній мережі передають сигнали до домашнього шлюзу. Для подальшої роботи були налаштовані IP-адреса шлюзу, SSID - HomeGateway, а також використано шифрування WPA2-PSK та встановлено пароль для шлюзу.

Домашній шлюз використовується для моніторингу поведінки та контролю якості мережі. Він збирає дані з різних компонентів системи, аналізує отримані пакети даних, створює CSV-файли і надсилає їх на сервер. Також він передає сигнали іншим елементам розумної мережі і ініціює наявність служб TCP, DNS та HTTP.

Розумні мережі часто поєднують бездротові і дротові зв'язки. Для цього розглянуті обидва варіанти. Були підключені пристрої сонячної панелі та акумулятора, які забезпечуватимуть безперебійне живлення. Для цього використовується широко відомий протокол KNX, який є європейським стандартом для проектування розумних мереж.

Ми розглянемо налаштування дротового зв'язку на прикладі детектора диму на кухні. В списку "З'єднання" ми вибираємо елемент з назвою Copper Straight Through (мідна звита пара) і підключаємо детектор до комутатора 2960. Комутатор додано до схеми, щоб мати можливість підключати більше інтелектуальних пристроїв. Комутатор 2960 з'єднано з доступним інтерфейсом домашнього шлюзу FastEthernet0/24 - FastEthernet0/1.

Оскільки лампи-індикатори світяться зеленим кольором, ми продовжили налаштування. Для цього ми відкрили детектор, перейшли до розділу Advanced, вкладки Config і встановили ім'я, IP-адресу та віддалений сервер, вказавши IP-

адресу шлюзу, логін і пароль для доступу до системи. Аналогічним чином ми підключили інші пристрої фізичної LAN мережі.

Розглянувши налаштування бездротової мережі на прикладі "розумної кавоварки" (рис.3.9). Спочатку ми додали бездротовий модуль - в розділі Advanced на вкладці I/Oconfig обрали бездротовий адаптер PT-IOT-NM-1W. На вкладці Config ми встановили ім'я і сервер IoT - Home Gateway. На вкладці Wireless0 ми вказали SSID - HomeGateway, тип аутентифікації WPA2-PSK і пароль. Важливо відзначити, що тип з'єднання можна змінити в будь-який момент. Ми налаштували доступ з кінцевих пристроїв для керування та моніторингу мережі - планшета та смартфона. Специфікація конфігурації полягає в тому, що не потрібно обирати тип адаптера. Інші налаштування аналогічні описаним вище.

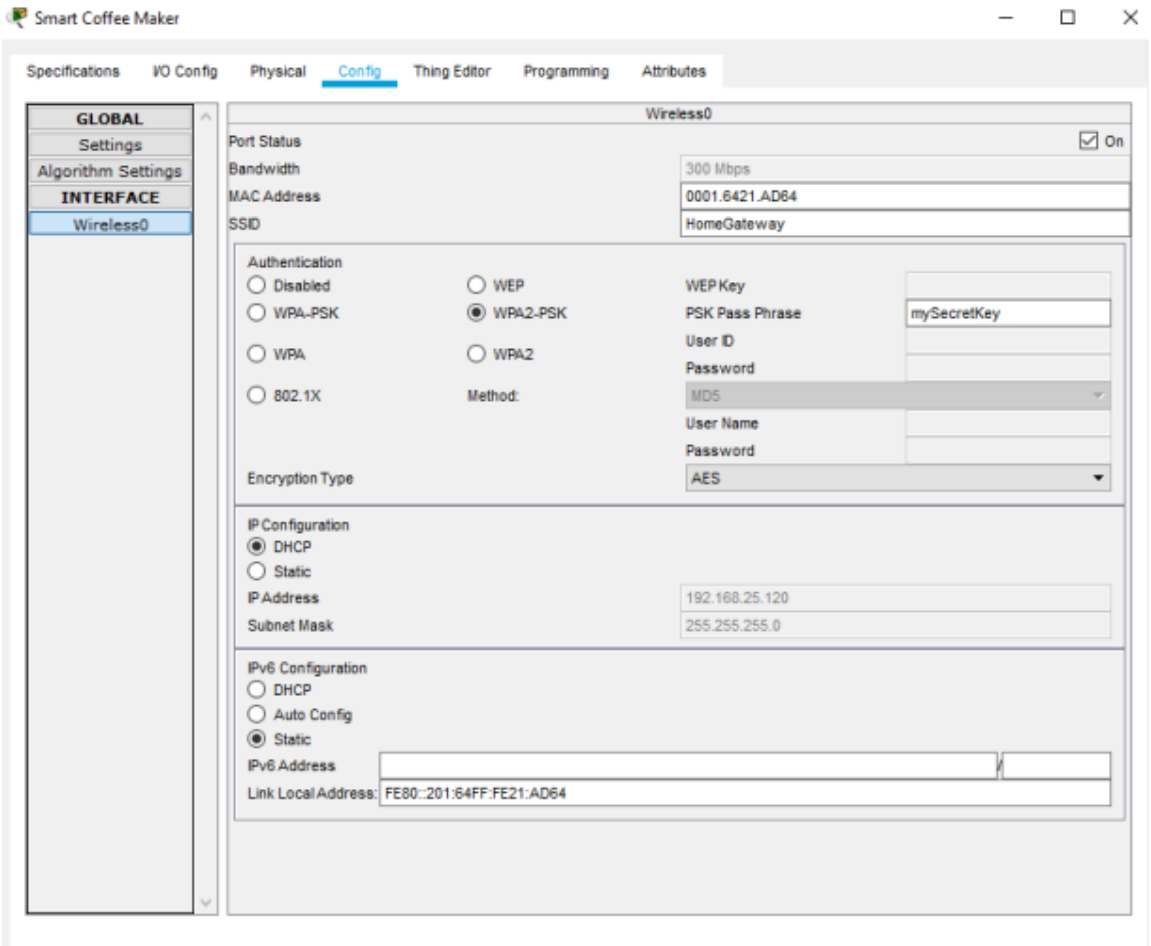



Рисунок 3.9 – налаштування девайсу

Для забезпечення моніторингу мережі за допомогою мобільних пристроїв, на вкладці Desktop був обраний веб-інтерфейс шлюзу. В ньому була вказана адреса серверу, логін і пароль для входу. Для отримання доступу до екрану керування пристроями системи використовується (рис.3.10), на якому розташована панель, де можна вмикати або вимикати пристрої, контролювати налаштування та здійснювати інші дії (рис.3.11).

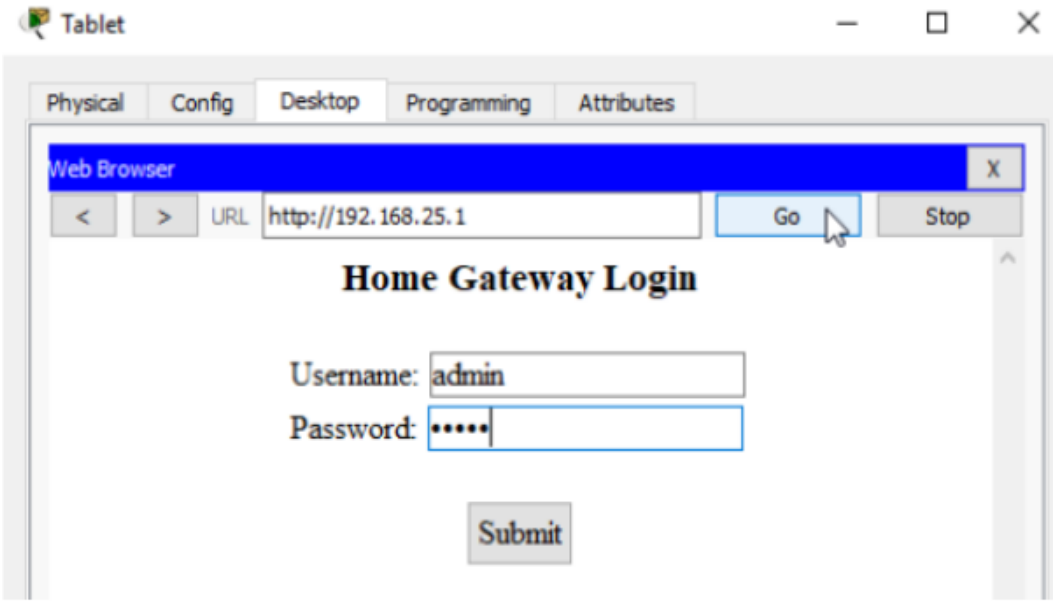



Рисунок 3.10 – доступ через планшет до веб-ресурсу

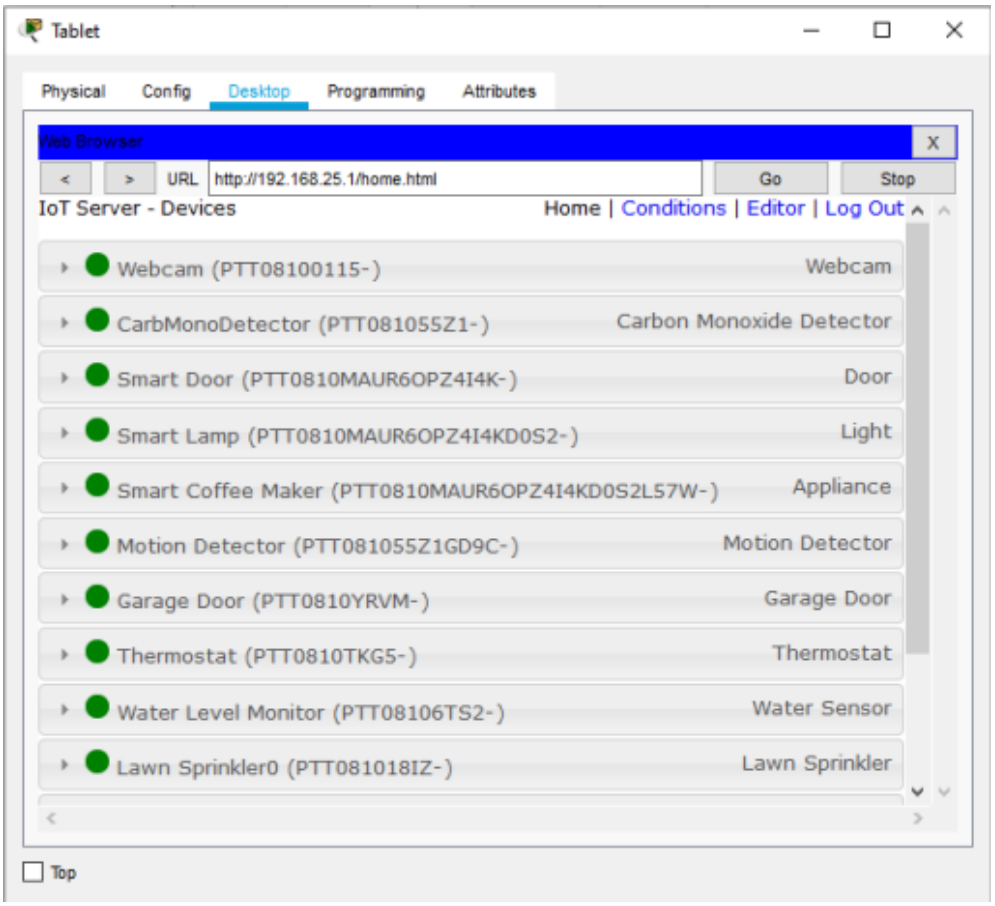



Рисунок 3.11 – веб інтерфейс для керування інтелектуальною мережею

На рисунку 3.12 зображена схема, що була отримана в результаті реалізації проекту "Smart Home". Якщо потрібно розширити цю мережу, це можна зробити за допомогою аналогічних дій з будь-якого з доступних у симуляторі кінцевих пристроїв, використовуючи вже наявні комунікаційні канали.

Після того, як дані від пристроїв досягають шлюзу у формі пакетів, вони розсилаються всім "розумним" елементам мережі. Залежно від конфігурації цих елементів згідно з певними правилами, вони реагують на ці дані відповідним чином. Наприклад, якщо отримують сигнал від вхідних дверей, кавоварка та освітлення вмикаються.

Для створення системи було використано комбінований тип зв'язку, що включав в себе внутрішню Wi-Fi мережу для планшету та стільниковий 3G/4G зв'язок для смартфона. Була реалізована можливість реєстрації нових користувачів у системі "домашній дім" та встановлення нових правил взаємодії пристроїв як віддалено, так і безпосередньо вдома.

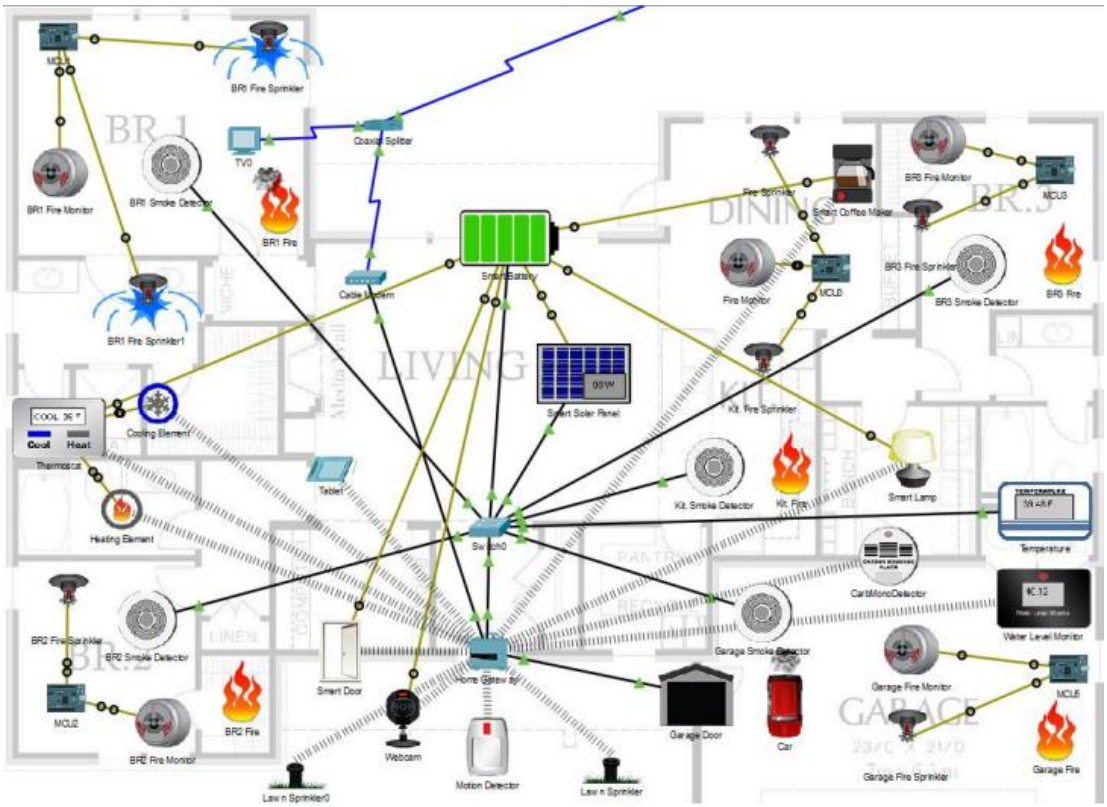



Рисунок 3.12 – Інтелектуальна мережа розумного будинку

Внаслідок виконання початкових налаштувань був розроблений проект робочої мережі "розумного будинку". Всі підключені пристрої були перевірені і стали доступними для управління та контролю.

## 3.3 Програмування та підключення обладнання Cisco

Користувач Cisco Packet Tracer має можливість створити модель "розумного будинку" і відтворити реальну поведінку датчиків, мікроконтролерів та пристроїв. Очевидно, що деякі з цих пристроїв потребують особливого налаштування та програмування. Смарт-пристрої можна активувати шляхом натискання лівої кнопки миші разом з клавішею Alt на клавіатурі. Крім того, пристрої також можуть активуватися автоматично залежно від зміни параметрів оточуючого середовища. Наприклад, у даній роботі використовується смарт-сонячна батарея, яка живить пристрої в домі протягом дня за рахунок енергії сонячних променів. Для налаштування взаємодії між пристроями можна скористатися веб-

інтерфейсом. Якщо функціонал веб-інтерфейсу не вистачає, то в Cisco Packet Tracer 7 є можливість програмування пристроїв відповідно до бажань користувача. У даному проекті були реалізовані і детально описані обидва ці варіанти.

Користувач має доступ до спеціального вікна під назвою "Home" у веб-браузері, яке спрямоване на управління системою "розумного будинку". За необхідності, він може перейти на вкладку "Conditions" і створити свої власні правила, що встановлюють умови взаємодії між інтелектуальними пристроями. Ці правила програмуються на основі простих "якщо-то" умов. Це знову підтверджує простоту налаштування інтелектуальної системи для звичайного користувача. Наприклад, налаштовано, що веб-камера активується, коли спрацьовує датчик руху. Інтерфейс взаємодії є зручним і зрозумілим для користувача (рис.3.13).

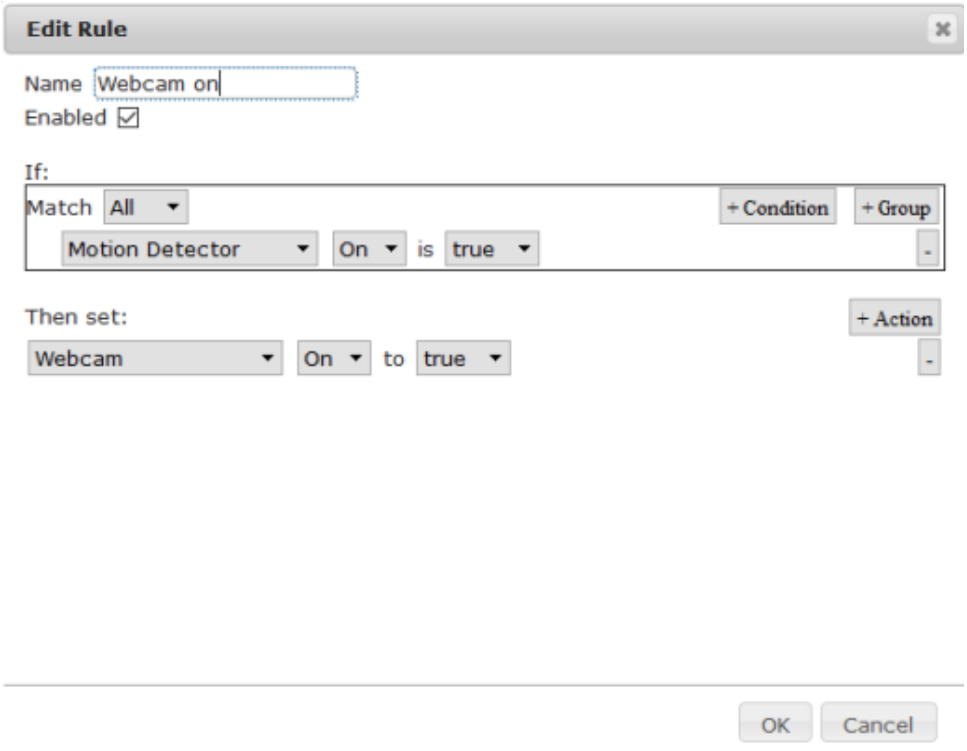



Рисунок 3.13 – налаштування веб-камери автоматичного вмикання при зафіксованому русі

Для того аби перевірявся рух детектора необхідно активізувати переміщення миші в поєднанні з натисканням клавіші Alt на клавіатурі. Автоматично – 5 секунд. Коли курсор рухається до датчика, він вмикається і

камера також активізує свою роботу. На рисунках 3.14 та 3.15 продемонстровано active та passive стан пристроїв. На рисунку 3.15 спрацьовує датчик руху і відповідно вмикається камера. Після цього ми маємо змогу спостерігати над тим, що на вулиці відтворюється. Розумні двері на автоматі зачинаються і навіть забезпечують безпеку жителям будинку.

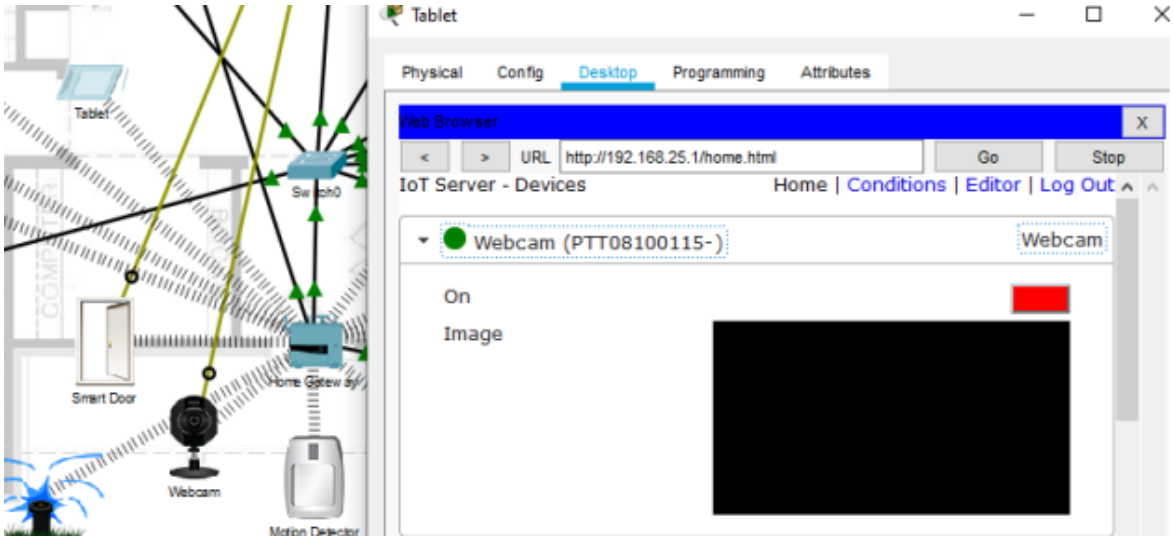



Рисунок 3.14 – Пасивний стан датчиків

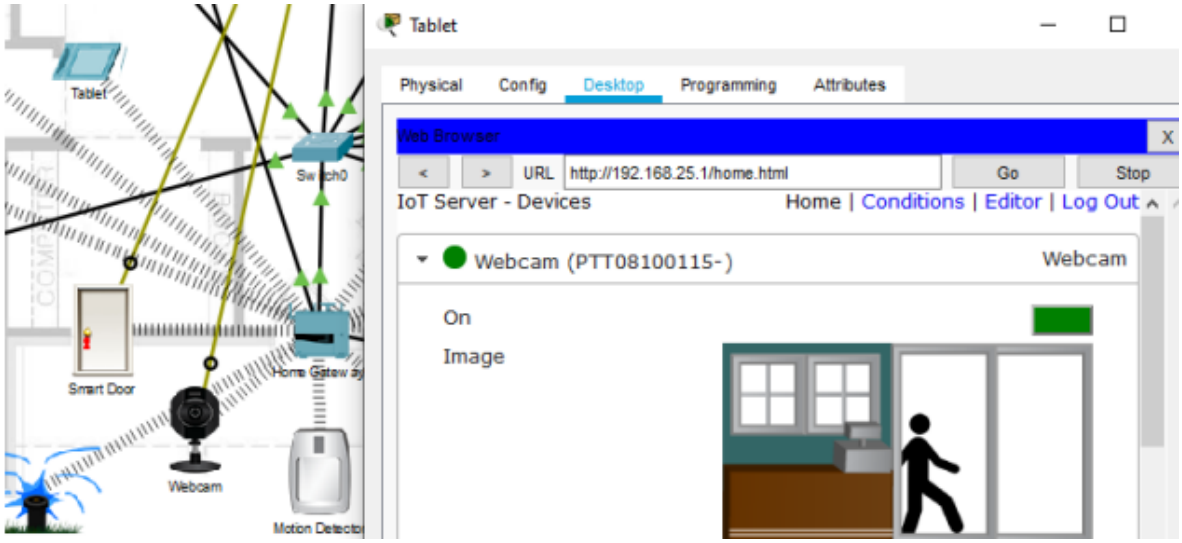



Рисунок 3.15 – Активний стан датчиків

Також можна налаштувати підйомник дверей у гаражі, щоб це було автоматично. Цей процес буде відбуватись коли детектор чадного газу > 0.2. Активація буде відбуватись за допомогою натискання курсору + Alt. Це буде відкривати двері, якщо власник запустив мотор автомобіля. Така функція також

гарантує уникнення газових аварій. На рисунку 3.16 продемонстровано умови, при яких двері зачинені, а на рисунку 3.17 можна побачити протилежне.


Рисунок 3.16 – рівень чадного газу < 0.2

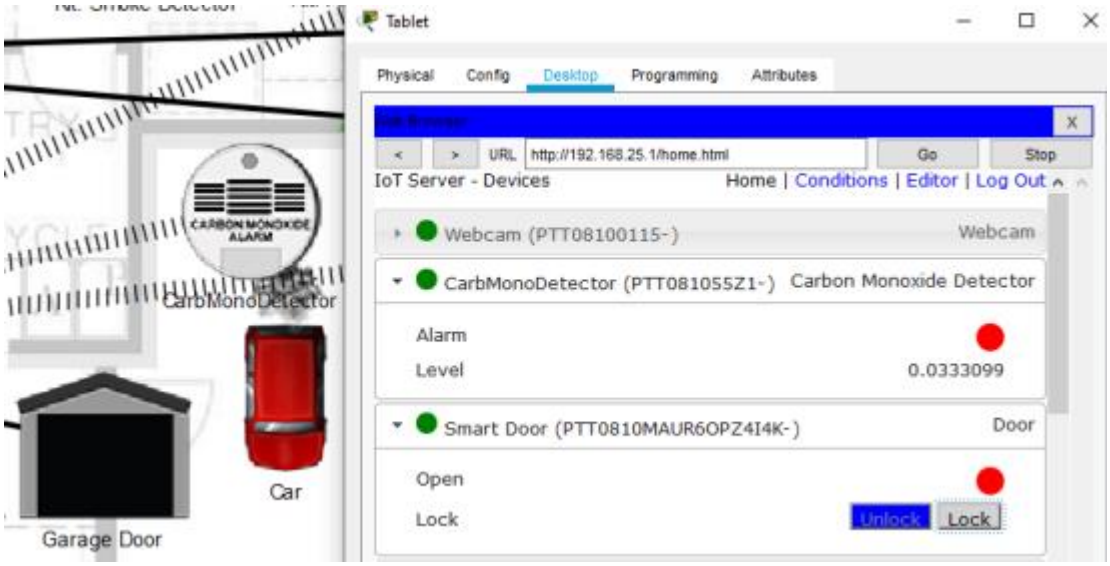



Рисунок 3.17 – рівень чадного газу > 0.2

Розглянемо сонячну панель та акумулятор, які є альтернативними джерелами енергії. Між собою два пристрої пов’язані кабелем IoT і кожен окремо під’єднаний до шлюзу. Графік природнього світла можна спостерігати у вкладці «Навколишнє середовище» (рис. 3.18).

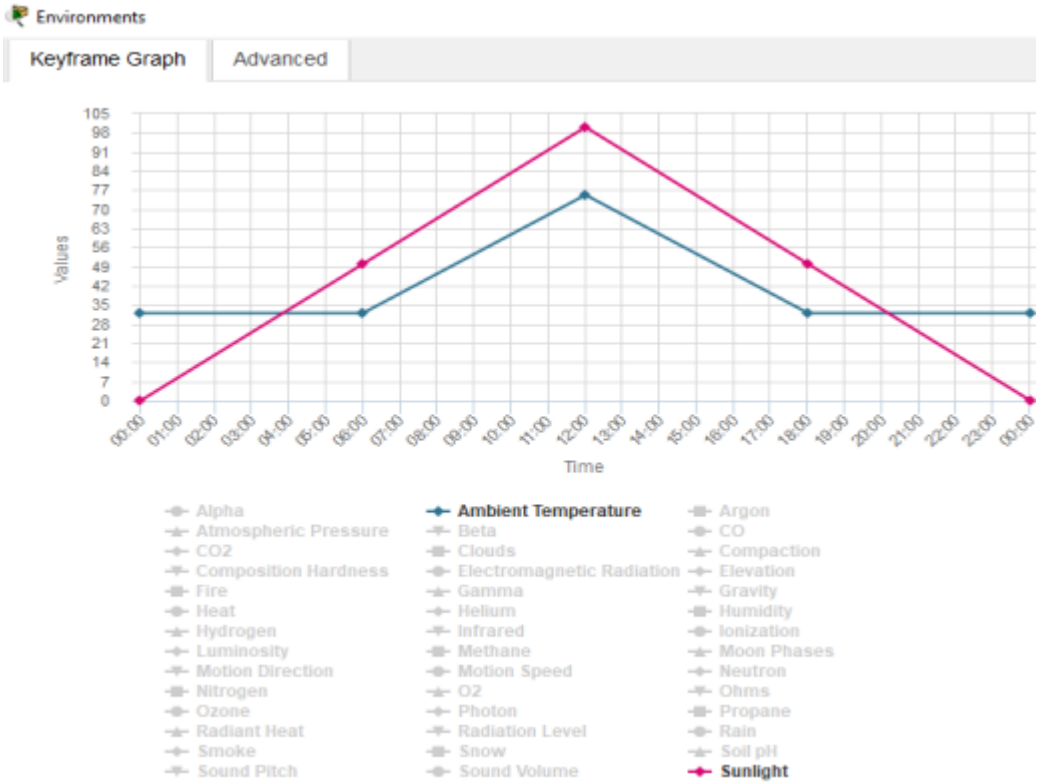



Рисунок 3.18 – діаграма змін температури та світла протягом дня

Можна сказати, що сонячна батарея отримує достатньо ресурсів за весь день і з легкістю забезпечить кавоварку, веб-камери, лампи (рис.3.19).

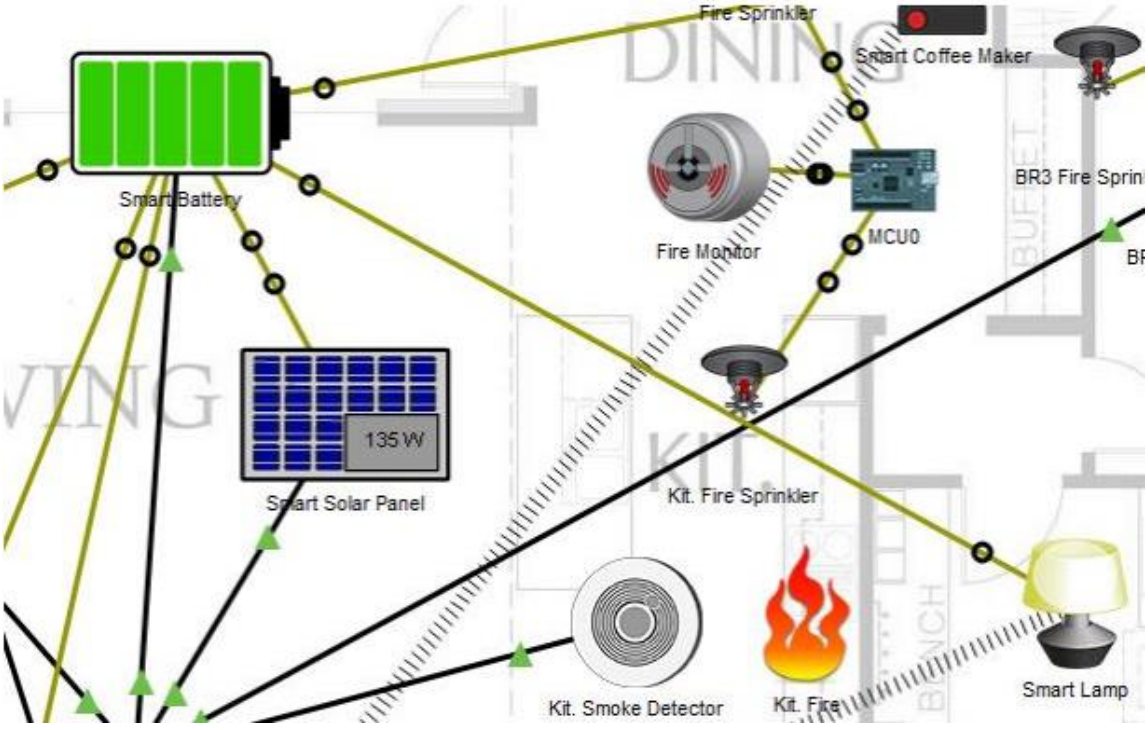



Рисунок 3.19 – розподіл заряду

Важливим аспектом є пожежна безпека у спальні. Сама протипожежна система реалізована за допомогою датчиків диму, моніторингом пожеж та розприскувачем і запрограмовано у мікроконтролері. Все приладдя розташоване у кожній кімнаті, але розприскування (рис.3.20) буде лише в тій, де це потрібно найбільше.

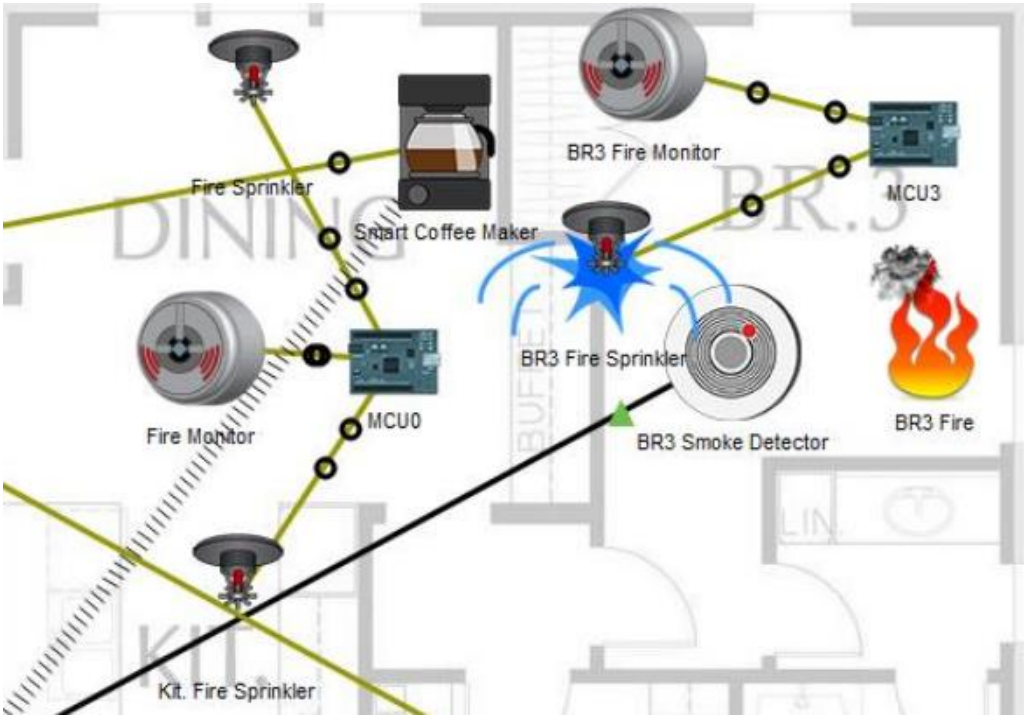



Рисунок 3.20 – Робота пожежної системи

Встановлення розприскувачів поза будівлею та в самій будівлі дуже відрізнялось при програмуванні, щоб був чіткий розрахунок при використанні водою (рис.3.21).

| | | | | |
|---|---|---|---|---|
| Edit Remove | Yes | Turn on sprinkler | Match all:<br>• Water Level Monitor Water Level < 20 cm<br>• Lawn Sprinkler Status is false | Set Lawn Sprinkler0 Status to true<br>Set Lawn Sprinkler Status to true |
| Edit Remove | Yes | Turn off sprinklers | Match all:<br>• Lawn Sprinkler Status is true<br>• Water Level Monitor Water Level > 50 cm | Set Lawn Sprinkler0 Status to false<br>Set Lawn Sprinkler Status to false |

Рисунок 3.21 – правила розприскування за межами будівлі

У системі розумного будинку забезпечений клімат контроль. Ось чому використані датчики температури для моніторингу загалом. Тому існують певні правила при програмуванні термостату (рис. 3.22).

| | | | | |
|---|---|---|---|---|
| Edit Remove | Yes | Cooling | Thermostat Temperature >= 75.0 °F | Set Thermostat Auto Cool Temperature to 68.0 °F |
| Edit Remove | Yes | Heating | Thermostat Temperature < 32.0 °F | Set Thermostat Auto Heat Temperature to 68.0 °F |

Рисунок 3.22 – правила охолоджування та нагрівання

Якщо термостат охолоджується і температура менша за 32 градуси за Фаренгейтом, то вмикається підігрів, а коли температура більша за 75 градусів, то вмикається охолодження. Також це можна скоригувати по годинах дня (рис.3.23).

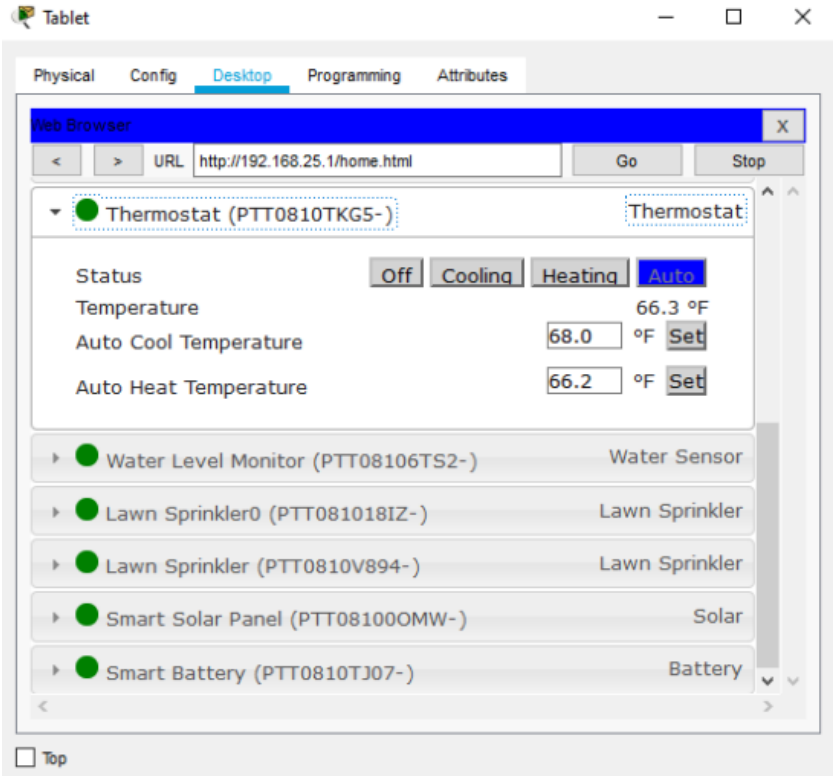



Рисунок 3.23 – конфігурація термостату

Таким чином, програмно реалізована уся система.

## 3.4 Розробка систем захисту

Кожний розумний будинок є індивідуальним по дизайну, а також по реалізації мережі. Тому є ряд рішень 2023 року для того, щоб покращити систему захисту, а також підвищити рівень комфорту та безпеки усіх жителів.

Саме в даній моделі розумного будинку, відеоспостереження на досить хорошому рівні. Але з приводу фізичної безпеки, можна додати сигналізацію, і надати доступ для автоматичного відкриття дверей лише власникам, які є повнолітніми та свідомими. Також не дозволяти реєструватись для управління будинком друзям та родичам, які в ньому не проживають. Власникам рекомендую постійно оновлювати ПЗ усього обладнання, так як це не лише про функціонування, а ще й про кіберзахист. Багато виробників та розробників девайсів Cisco розумного будинку з кожним днем покращують програмне забезпечення методами шифрування, впроваджують різні методи виявлення та запобіганні кібератак, вдосконалюють механізми автентифікації та загалом розробляють імунітет до кібезлочинців.

Також рекомендую впровадити машинне навчання та штучний інтелект для аналізу та виявленню потенційних загроз, для цього створенні додатки, які також можна підключити, щоб постійно переглядати звітність і перевіряти чи немає небезпечної активності.

Ну і на кінець, пропоную впровадити інтеграцію з обліковими записами, щоб встановити індивідуальні права доступу. Керування користувачами та перегляду активності по всій системі.

Усі ці покращення не лише забезпечать високий рівень безпеки 2023 року, а ще й допоможуть жителям будинку на повну насолоджуватись усіма перевагами цієї технології без зайвих ризиків.

# ВИСНОВКИ

У даній дипломній роботі було детально розглянуто систему захисту розумного будинку з використанням обладнання Cisco. Вивчення широкого спектру функцій безпеки, доступних у цьому обладнанні, дозволило виявити їхню ефективність у боротьбі з кібератаками, несанкціонованим доступом та небажаними подіями.

Аналізуючи різні аспекти безпеки, було підкреслено, що обладнання Cisco має значні переваги, що допомагають забезпечити безпеку розумного будинку. Вбудовані функції брандмауера забезпечують контроль руху трафіку мережі та блокування небажаних підключень або кібератак. Функції виявлення та запобігання вторгнень (IDS/IPS) сприяють виявленню та блокуванню небезпечної або аномальної активності в мережі. Веб-фільтрація дозволяє блокувати доступ до небезпечних або небажаних веб-сайтів та контролювати використання веб-додатків.

Застосування віртуальних приватних мереж (VPN) дозволяє забезпечити безпеку комунікації між пристроями та мережами у розумному будинку шляхом створення зашифрованого тунелю. Аутентифікація та авторизація, підтримувані обладнанням Cisco, дозволяють ефективно контролювати доступ до мережі та пристроїв шляхом використання паролів, сертифікатів або біометричних даних.

Використання обладнання Cisco для захисту розумного будинку сприяє збереженню конфіденційності, цілісності та доступності системи. Важливими елементами є регулярні оновлення програмного забезпечення, налаштування системи моніторингу та журналювання, а також постійне підвищення свідомості користувачів про правила безпеки.

Узагальнюючи, система захисту розумного будинку засобами обладнання Cisco є ефективним рішенням для забезпечення безпеки та захисту від сучасних загроз. Вона пропонує комплексний підхід до безпеки розумного будинку та сприяє забезпеченню спокою та захищеності користувачів у повсякденному житті.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ


1. Dickson B. How to prevent your IoT devices from being forced into botnet bondage [Електронний ресурс] / Dickson. – 2015. – Режим доступу до ресурсу: https://techcrunch.com/2016/08/16/how-to-prevent-your-iot-devicesfrom-beingforced-into-botnet-slavery/.

2. Patrascu M. Integrating Services and Agents for Control and Monitoring: Managing Emergencies in Smart Buildings. Service Orientation in Holonic and MultiAgent Manufacturing and Robotics. / Patrascu., 2014. – 544 с.

3. Cisco Networking Academy. Introduction to IoT [Електронний ресурс] / Cisco. – 2020. – Режим доступу до ресурсу: https://1331758.netacad.com/courses/1012514

4. Dickson B. How to prevent your IoT devices from being forced into botnet bondage [Електронний ресурс] / Dickson. – 2015. – Режим доступу до ресурсу: https://techcrunch.com/2016/08/16/how-to-prevent-your-iot-devices-from-being-forcedinto-botnet-slavery/.

5. Smart Home Statistics [Електронний ресурс] / Jaleesa Bustamante – 2020. – Режим доступу до ресурсу: https://ipropertymanagement.com/research/iotstatistics

6. Power Load Event Detection and Classification Based on Edge Symbol Analysis and Support Vector Machine [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.hindawi.com/journals/acisc/2012/742461/.

7. Євтух Б.В. «Система управління розумним домом. Підсистема забезпечення безпеки», [Електронний ресурс] /Євтух. – 2015. – Режим доступу до ресурсу: http://cad.kpi.ua/attachments/093_2015_%D0%B5%D0%B2%D1%82%D1%83%D1%85.pdf

8. An Overview of Home Automation Systems [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7791223/.

9. Smart Home [Електронний ресурс] / James Chen – 2020. – Режим доступу до ресурсу: https://www.investopedia.com/terms/s/smart-home.asp

10. Що таке розумний будинок? Все що потрібно знати про систему Розумний Дім [Електронний ресурс]. – Режим доступу до ресурсу: https://bron.ua/article/schotake-rozumnij-budinok-vse-scho-potrbno-znati-pro-sistemu-rozumnij-dm/5/

11. Fortune Business Insights [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.fortunebusinessinsights.com/industry-reports/internet-ofthings-iot-market-100307

12. Розумне освітлення [Електронний ресурс]. – Режим доступу до ресурсу: https://milight.com.ua/ua/umnoe-osveshchenie/

13. Internet of Things In Smart Home [Електронний ресурс] – 2019 – Режим доступу до ресурсу: https://scand.com/company/blog/internet-of-things-in-smart-home/

14. Технологія розумного будинку: як AI створює простір, комфортний для життя [Електронний ресурс]. – Режим доступу до ресурсу: https://www.everest.ua/tehnologiya-rozumnogo-budynku-yak-ai-stvoryuye-prostirkomfortnyj-dlya-zhyttya/

15. Old versions of Cisco Packet Tracer - V7.1, v7.0, v6.3, v6.2 [Електронний ресурс]. – 2020 – Режим доступу до ресурсу: https://www.geekdashboard.com/cisco-packet-tracer-download/

Al-Qutayri, Mahmoud & Jeedella. Integrated Wireless Technologies for Smart Homes Applications [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: https://www.researchgate.net/publication/221907506_Integrated_Wireless_Technologies_for_Smart_Homes_Applications

17. Котунова, Д. Г. Огляд DIY елементів для систем «Smart Home» / Д. Г. Котунова, О. М. Павловський // XIII Науково-практична конференція студентів, аспірантів та молодих вчених «Погляд у майбутнє приладобудування», 13-14 травня 2020 р., м. Київ, Україна : збірник праць конференції. – Київ : КПІ ім. Ігоря Сікорського, 2020. – С. 35–38.

18. Andrea Finardi. IoT simulations with Cisco Packet Tracer [Електронний ресурс]. – 2017. – Режим доступу до ресурсу:

https://www.theseus.fi/bitstream/handle/10024/150158/Andrea%20Finardi%20%20Master%20of%20Engineering%20%20Information%20technology.pdf?sequence=1&isAllowed=y

19. Моніт Я.В. Система «Розумний будинок» з відкритим програмним забезпеченням/ Я.В.Моніт // XIX науково-технічна конференція студентів та молодих учених «Гіротехнології, навігація, керування рухом та конструювання авіаційно-космічної техніки», 15-16 лютого 2016 р. – К.: «Політехніка», 2016. – С. 43-44.

20. Розумний будинок — з чого він складається та чи потрібен вам [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://nachasi.com/2018/06/25/smart-house-faq/

21. Львівський стартап uMuni працює над системою енергозбереження, яка економить до 15% [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://ain.ua/2015/10/29/lvovskij-startap-umuni-rabotaet-nad-sistemojenergosberezheniya-kotoraya-ekonomit-do-15/

22. Cisco Blogs [Електронний ресурс]. Режим доступу до ресурсу: https://blogs.cisco.com/

23. Cisco Official Website [Електронний ресурс]. Режим доступу до ресурсу: https://www.cisco.com/

24. CNET [Електронний ресурс]. Режим доступу до ресурсу: https://www.cnet.com/

25. Digital Trends [Електронний ресурс]. Режим доступу до ресурсу: https://www.digitaltrends.com/

26. Engadget [Електронний ресурс]. Режим доступу до ресурсу: https://www.engadget.com/

27. Wired [Електронний ресурс]. Режим доступу до ресурсу: https://www.wired.com/

28. Wilson C, Hargreaves T, Hauxwell-Baldwin R. Smart homes and their users: a systematic analysis and key challenges [Електронний ресурс]. – 2018. –

Режим доступу до ресурсу: https://link.springer.com/article/10.1007/s00779-014-0813-0

29. What's new in Cisco Packet Tracer 7.0. Retrieved from Packet Tracer Network. [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: http://www.packettracernetwork.com/features/packettracer-7-newfeatures.html

30. D. Kundu, M. E. Khallil, T. K. Das, A. A. Mamun, and A. Musha. Smart home automation system using on IoT [Електронний ресурс] / Kundu, Mamun. – 2020. – Режим доступу до ресурсу: https://www.ijser.org/onlineResearchPaperViewer.aspx?Smart-Home-AutomationSystem-Using-on-IoT.pdf

31. O. Taiwo, A. E. Ezugwu, N. Rana, and S. i. M. Abdulhamid. Smart home automation system using ZigBee, Bluetooth and Arduino technologies [Електронний ресурс] / Taiwo. – 2020. – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007%2F978-3-030-58817-5_43

32. V. Govindraj, M. Sathiyanarayanan, and B. Abubakar. Customary homes to smart homes using internet of things (IoT) and mobile application [Електронний ресурс] / V. Govindraj, M. Sathiyanarayanan, and B. Abubakar. – 2018. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8358532/

33. C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin. Benefits and risks of smart home technologies [Електронний ресурс] / Wilson. – 2020. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S030142151630711X?via%3Dihub

34. C. J. Diane. How smart is your home? [Електронний ресурс] / Diane. – 2021. – Режим доступу до ресурсу: https://scholar.google.com/scholar_lookup?title=How%20smart%20is%20your%20home?&author=C.%20J.%20Diane&publication_year=2012

35. K. Ashton. That “internet of things” thing [Електронний ресурс] / Ashton. – 2019. – Режим доступу до ресурсу: https://scholar.google.com/scholar_lookup?title=That%20%E2%80%9Cinternet%20of%20things%E2%80%9D%20thing&author=K.%20Ashton&publication_year=2009

36. Libelium. 50 Internet of Things Applications [Електронний ресурс] / Libelium. – 2021. – Режим доступу до ресурсу: http://www.libelium.com/top_50_iot_sensor_applications_ranking

37. Liu T, Yuan R, Chang H. Research on the internet of things in the automotive industry. In: ICMeCG 2012 international conference on management of e-commerce and eGovernment, Beijing, China [Електронний ресурс] / Liu. – 2018. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S0263224118306912?via%3Dihub

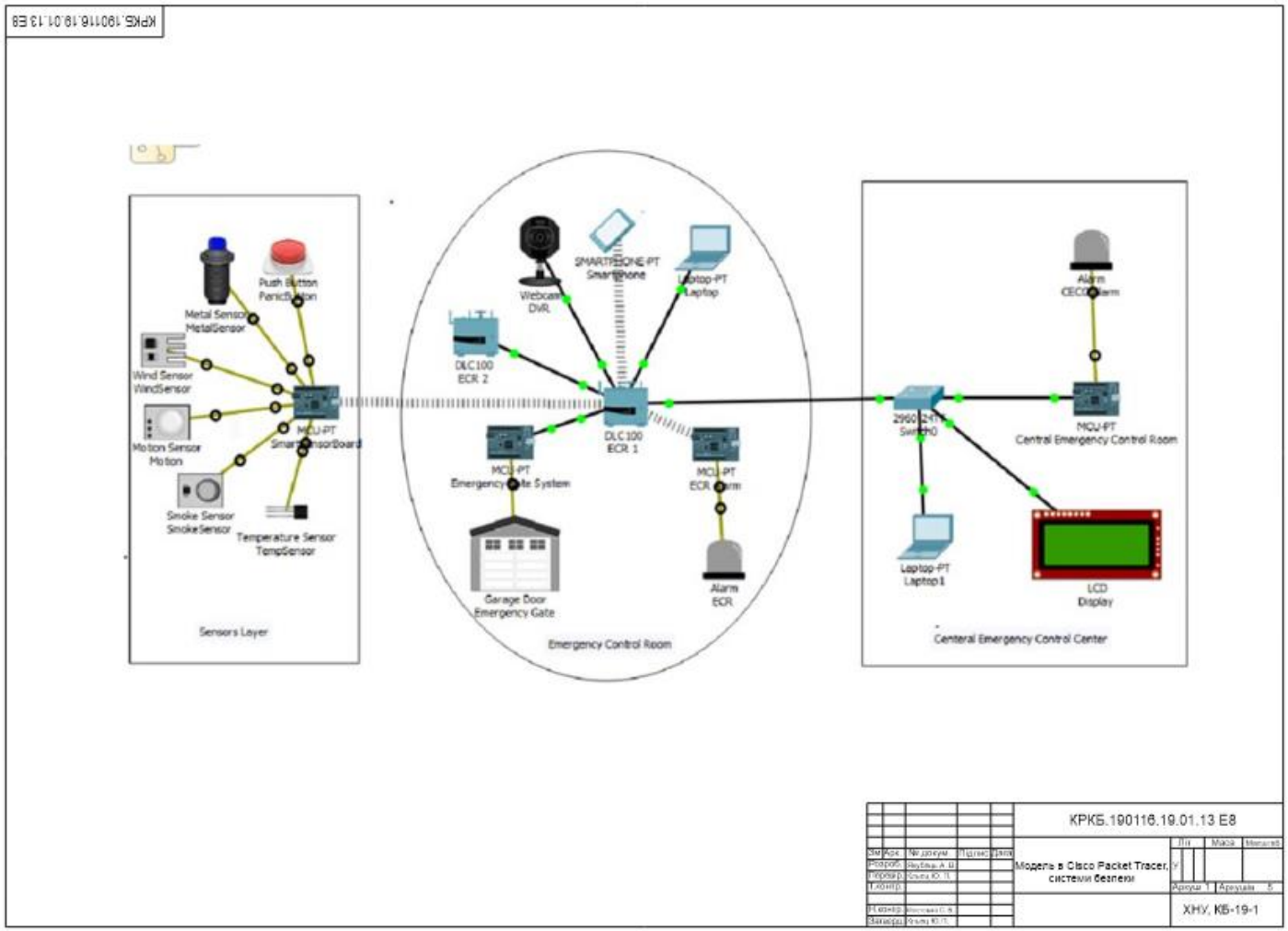
38. Behrendt F. Cycling the smart and sustainable city: analyzing EC policy documents on internet of things, mobility and transport, and smart cities [Електронний ресурс] / Behrendt. – 2019. – Режим доступу до ресурсу: https://www.mdpi.com/2071- 1050/11/3/763

39. Sfar AR, Natalizio E, Challal Y, Chtourou Z. A roadmap for security challenges in the internet of things. Digit Commun Netw [Електронний ресурс] / Sfar AR, Natalizio E, Challal Y, Chtourou Z. – 2018. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S2352864817300214?via%3Dihub

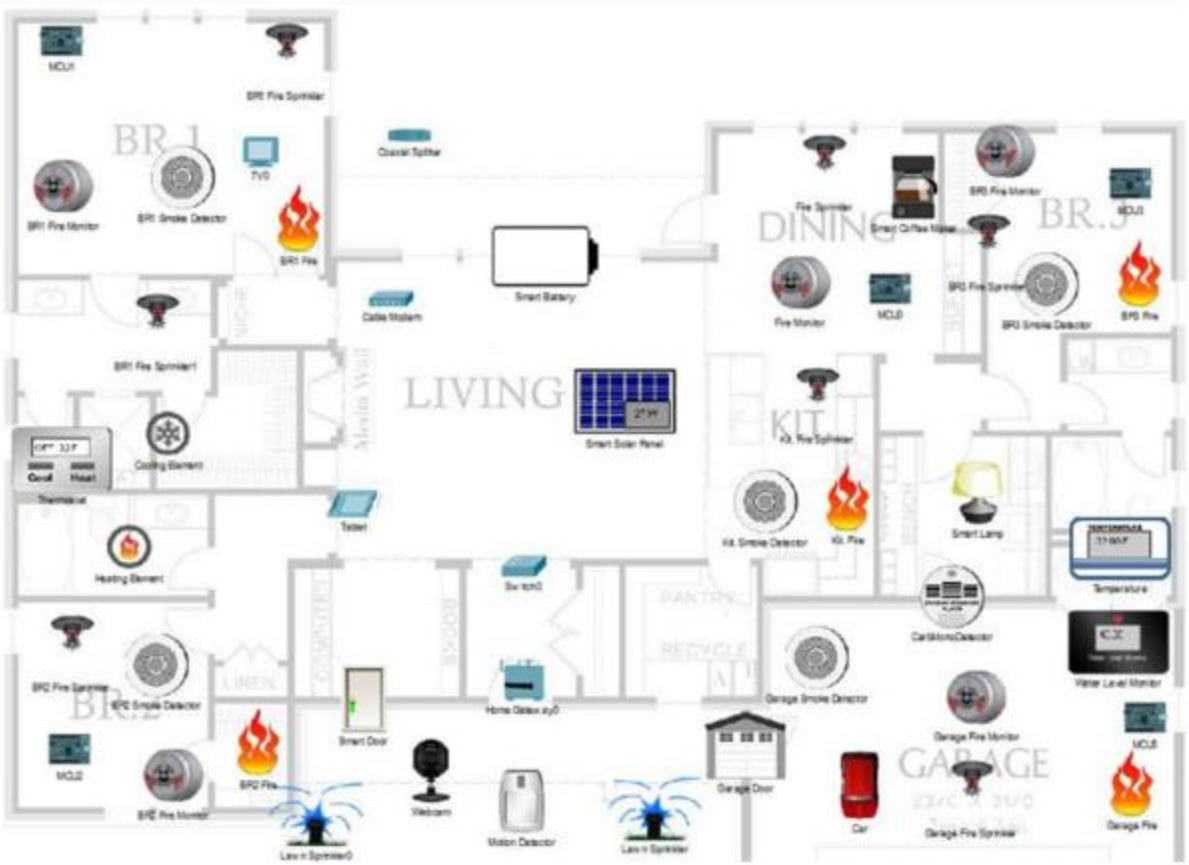
40. Uncovering IoT Threats in the Cybercrime Underground [Електронний ресурс] // Trend Micro Research. – 2019. – Режим доступу до ресурсу: https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-inthe-cybercrime-underground.pdf

# ДОДАТОК А

Копія графічної частини

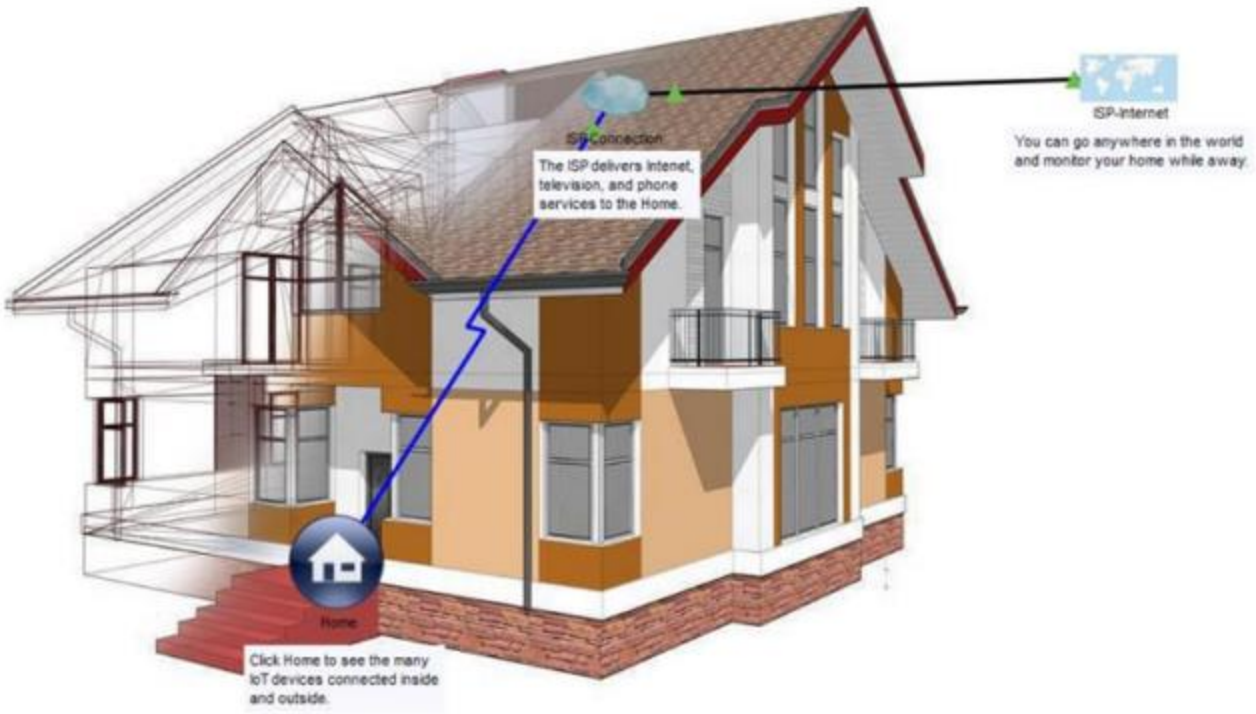


КРКБ.190116.19.01.13 Е8



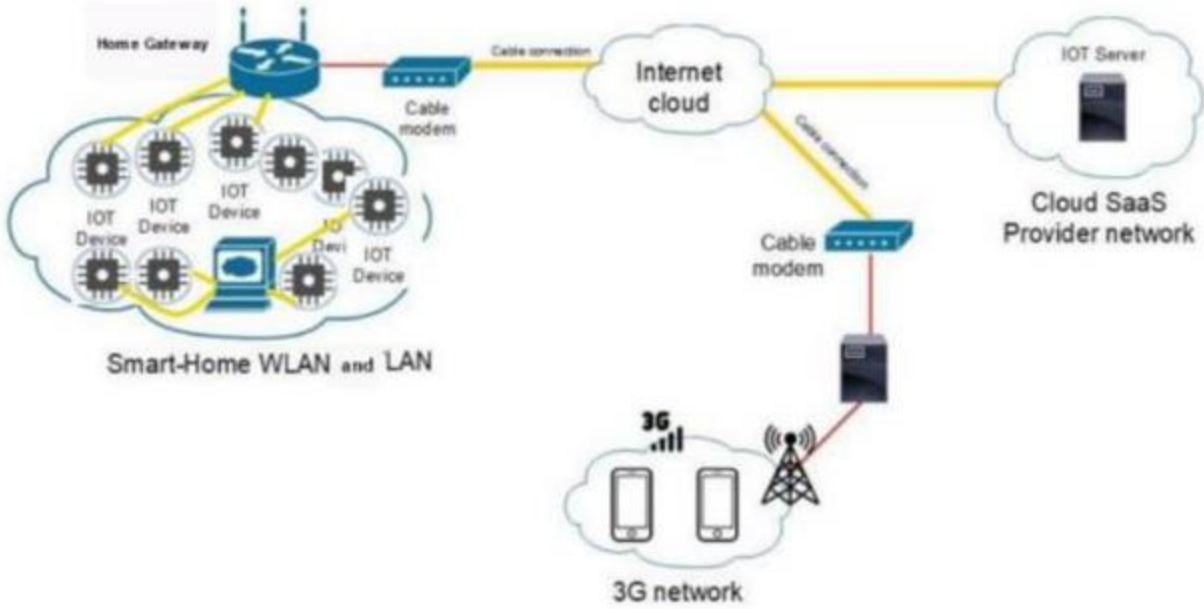

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | КРКБ.190116.19.01.13 Е8 | | |
| Зм. | Арк. | № докум. | Підпис | Дата | | | | |
| Розроб. | | Якубець А. Ш. | | | Датчики та пристрої всередині розумного будинку | Літ. | Маса | Масштаб |
| Перевір. | | Ольга Ю. П. | | | | У | | |
| Т.контр. | | | | | | Аркуш 2 | Аркушів 5 | |
| Н.контр. | | Дмитренко О. В. | | | | ХНУ, КБ-19-1 | | |
| Затверд. | | Ольга Ю. П. | | | | | | |

КРКБ.190116.19.01.13 Е8



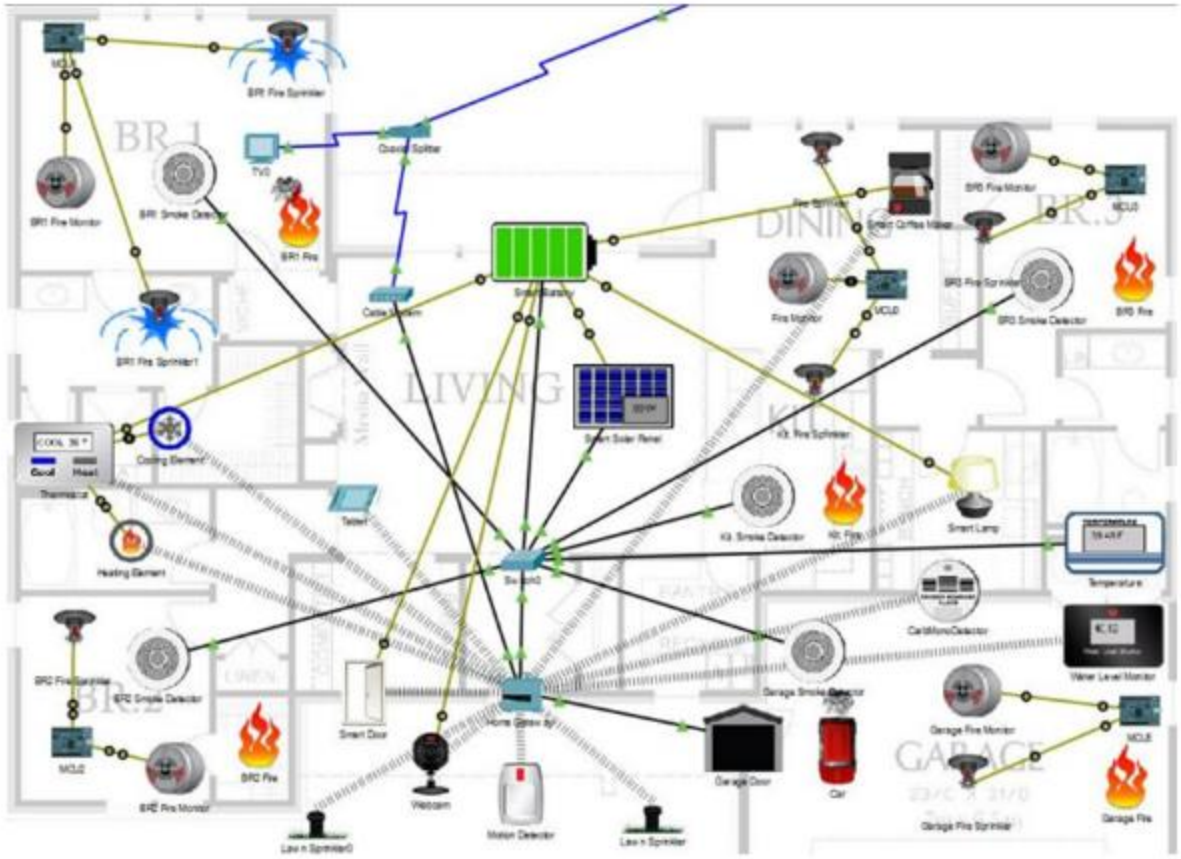

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | КРКБ.190116.19.01.13 Е8 | | |
| Зм. | Арк. | № докум. | Підпис | Дата | | | | |
| Розроб. | | | | | Швидка навігація | Літ. | Маса | Масштаб |
| Перевір. | | | | | | У | | |
| Т.контр. | | | | | | Аркуш 3 | Аркушів 5 | |
| Н.контр. | | | | | | ХНУ, КБ-19-1 | | |
| Затверд. | | | | | | | | |

КРКБ.190116.19.01.13 Е8




| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | КРКБ.190116.19.01.13 Е8 | | |
| Зм. | Арк. | № докум. | Підпис | Дата | | | |
| Розроб. | | Якубець А. Ш. | | | Топологія розумного будинку | Літ. | Маса | Масштаб |
| Перевір. | | Ольга Ю. П. | | | | У | | |
| Т.контр. | | | | | | Аркуш 4 | Аркушів 5 | |
| Н.контр. | | Іванішин С. К. | | | | ХНУ, КБ-19-1 | | |
| Затверд. | | Ольга Ю. П. | | | | | | |

КРКБ.190116.19.01.13 Е8




| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | КРКБ.190116.19.01.13 Е8 | |
| Зм. | Арк. | № докум. | Підпис | Дата | | | |
| Розроб. | | Якубець А. Ш. | | | Інтелектуальна мережа розумного будинок | Літ. | Маса | Масштаб |
| Перевір. | | Ольга Ю. П. | | | | У | | |
| Т.контр. | | | | | | Аркуш 5 | Аркушів 5 | |
| Н.контр. | | Васильєв О. В. | | | | ХНУ, КБ-19-1 | | |
| Затверд. | | Ольга Ю. П. | | | | | | |