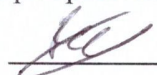


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

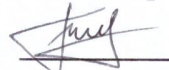
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи безпеки розумного будинку»

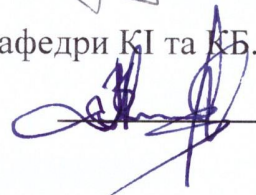
Виконав студент 4-го курсу групи КБ-2
спеціальності 125 «Кібербезпека»

 Олесь Вексей

Керівник Старший викладач кафедри КІ та КБ,

 Олександра Покотило

Рецензент Доцент кафедри КІ та КБ. к.т.н., доцент

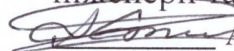
 Володимир Котенко

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Вексей Олесь Ігорович

Тема роботи: «Проект системи безпеки розумного будинку»

Затверджена Наказом університету від 1 березня 2022 р. № 128/с

Термін здачі студентом закінченої роботи 28 червня 2022 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Об'єктом дослідження є процес проектування системи безпеки розумного будинку та аналіз її функціонування шляхом перевірки працездатності мережі.

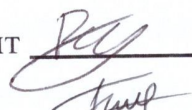
Предметом дослідження є технології, що використовуються при побудові мереж розумних будинків.

Обладнання та програмне забезпечення:

1. Мережевий симулятор Cisco Packet Tracer
2. Образи пристроїв IoT
3. ПЗ Oracle VirtualBox
4. Віртуальна машина з емуляцією смарт пристрою
5. Віртуальна машина з ОС Kali Linux

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

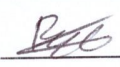
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	 06.03.2022	 06.03.2022
2	Покотило О.А.	 06.03.2022	 06.03.2022
3	Покотило О.А.	 06.03.2022	 06.03.2022

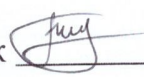
Студент  Олесь Вексей

Керівник  Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	06.03.2022	виконано
2	Розробка плану роботи	30.04.2022	виконано
3	Розробка розгорнутого плану	05.05.2022	виконано
4	Подача чернетки керівнику для перевірки	07.05.2022	виконано
5	Доопрацювання роботи та перевірка керівником	09.05.2022	виконано
6	Затвердження графічних матеріалів у керівника	12.05.2022	виконано
7	Проведення попереднього захисту	28.06.2022	виконано
8	Отримання відгуку керівника	28.06.2022	виконано
9	Допуск завідувача кафедри	28.06.2022	виконано
10	Подання роботи на рецензування	28.06.2022	виконано

Студент  Олесь Вексей

Керівник  Олександра Покотило

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра представляє з себе проект системи безпеки розумного будинку.

Мета і завдання роботи. Метою роботи є проектування системи безпеки розумного будинку.

Досягнення поставленої мети передбачає розв'язання наступних завдань:

— Проведення аналізу поняття «Розумний будинок», його принципів роботи та його складових.

— Аналізу наявних рішень розумних будинків.

— Розробки мережної інфраструктури розумного будинку.

— Проведення перевірки працездатності мережі.

— Перевірка якості та ефективності використаних засобів та компонентів.

Об'єктом дослідження є процес проектування системи безпеки мережі розумного будинку.

Предметом дослідження є технологія проектування системи безпеки мережі розумного будинку.

Пояснювальна записка до випускної кваліфікаційної роботи містить в собі 55 сторінок, 2 таблиці та 37 рисунків. Список використаних джерел містить 22 найменування і займає 3 сторінки.

Ключові слова: РОЗУМНИЙ БУДИНОК, ІОТ, МЕРЕЖА, СИСТЕМА, СЕНСОР, БЕЗПЕКА, ЗАГРОЗА, ВРАЗЛИВІСТЬ, ZIGBEE, Z-WAVE, BLUETOOTH LOW ENERGY, THREAD.

					КІК.КР.Б - 125 - 04 - ПЗ			
Лист	Арк.	№ докум.	Підпис	Дата	Проект системи безпеки розумного будинку	Літ.	Арк.	Аркушів
Розроб.		Вексей О.І.		10.06				
Керівник		Покотило О.А.		20.06			4	57
Реценз.		Котенко В.М.		20.06		ФІКТ, Гр. КБ-2		
Н. контр.		Покотило О.А.						
Затверд.		Єфіменко А.А.		20.06				

ANNOTATION

The final qualifying work of the bachelor is a project of the security system of a smart home.

The purpose and objectives of the work. The purpose of the work is to design a security system for a smart home.

Achieving this goal requires solving the following tasks:

- Analysis of the concept of "Smart Home", its principles of operation and its components.
- Analysis of existing solutions for smart homes.
- Development of network infrastructure of a smart home.
- Carrying out a network health check.
- Checking the quality and effectiveness of the tools and components used.

The object of research is the process of designing a network security system for a smart home.

The subject of research is the technology of designing the security system of the smart home network.

The explanatory note to the final qualification work contains 55 pages, 2 tables and 37 drawings. The list of used sources contains 22 names and takes 3 pages.

Keywords: SMART HOME, IOT, NETWORK, SYSTEM, SENSOR, SECURITY, THREAT, VULNERABILITY ZIGBEE, Z-WAVE, BLUETOOTH LOW ENERGY, THREAD.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ	
АКТУАЛЬНОСТІ ТЕМИ РОБОТИ.....	9
1.1 Можливості та завдання розумного будинку	9
1.2 Безпека розумних будинків	15
1.3 Доступні технології комунікації пристроїв розумного будинку	19
1.4 Постановка технічного завдання	34
РОЗДІЛ 2 РОЗРОБКА ТА ДОСЛІДЖЕННЯ РОЗУМНОГО БУДИНКУ	35
2.1 Моделювання проекту в середовищі Cisco Packet Tracer	35
2.2 Складання схеми у середовищі Cisco Packet Tracer	41
РОЗДІЛ 3 ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ МЕРЕЖІ РОЗУМНОГО БУДИНКУ	44
3.1 Перевірка зв'язку у мережі.....	44
3.2 Перевірка працездатності SMART пристроїв та їх автоматизації	46
3.3 Перевірка вразливостей системи	49
ВИСНОВКИ.....	52
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	53
ДОДАТКИ.....	56

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ІОТ – інтернет речей

Z-Wave – протокол бездротового зв'язку

Bluetooth LE – Bluetooth Low Energy

ZigBee – бездротовий стандарт передачі даних

ENISA – The European Union Agency for Cybersecurity

DoS (DDoS) – (Distributed) Denial-of-service Attack

PAN – Personal Area Network

ISM – Industrial, Scientific and Medical

WSN – Wireless Sensor Network

AES – Advanced Encryption Standard

CCM – Counter with cipher block chaining message authentication code

MIC – Message Integrity Code

WEP – Wireless Equivalent Privacy

WPA – Wi-Fi Protected Area

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Сьогодні кожна людина прагне зробити все, щоб автоматизувати щоденні процеси які відбуваються майже в кожному будинку. Стрімкий розвиток технологій є каталізатором цього процесу. За допомогою сучасних систем можна автоматизувати майже будь-які процеси, що відбуваються у нашому будинку, квартирі чи офісному приміщенні. Дехто використовує ці технології для свого комфорту, а дехто для охорони та безпеки. Велич спектру виконання можливих функцій дозволяє використовувати технології розумного будинку майже у всьому, починаючи від автоматизованого корегування температури у приміщенні, закінчуючи налаштуванням просунутої системи сигналізації чи автоматичного пожежогасіння.

Актуальність теми буде тільки збільшуватись кожного дня, виходячи з аналізу росту розвитку технологій, та збільшення спектру їх застосувань. Тому в даний час ми можемо виходити тільки з вже перевірених часом на сьогодні технологіях та сферах застосування засобів керування розумних будинків, коли в майбутньому, безсумнівно, їх буде ставати тільки дедалі більше.

Методи дослідження. В кваліфікаційній роботі було використано такі методи дослідження: експеримент, симуляція, моделювання та аналіз.

Практичне значення роботи полягає у наступному:

спроектована система безпеки мережі розумного будинку, яка здатна забезпечити автономність буденних процесів що виконуються у будинках.

налаштування пристроїв та датчиків, що об'єднані у мережу розумного будинку.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ

1.1 Можливості та завдання розумного будинку

Прагнення до комфорту та безпеки стимулює нас удосконалювати різні аспекти життя. Саме з цих причин ми рухаємося вперед. Близько 20 років тому уявляти собі масову автоматизацію було абсолютно дико, але прогрес не забрав багато часу, і розумний дім більше не здається футуристичним. Автоматичне приготування кави вранці чи вмикання світла нікого не здивує. Автоматика заповнила буквально всі сфери. І, схоже, вона не піде.



Рисунок 1.1 – Схема розумного будинку

Розумний дім — це загальна назва систем домашньої автоматизації, які складаються з багатьох пристроїв, які можуть позбавити нас від рутинних завдань. Це новий рівень взаємодії з навколишнім світом, коли ми перестаємо думати про багато дрібниць. Розумний будинок вмє вирішувати безліч звичних, рутинних завдань без нашого втручання.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Основними виділяють три завдання у системі розумного будинку:

1. Безпека;
2. Комфорт;
3. Енергозбереження.



Рисунок 1.2 – Вигляд елементів розумного будинку

Перше завдання – безпека. Сучасні технології розвинулись достатньо сильно, щоб запровадити безпеки у домі. Наприклад визначення споживання води, рівня вуглекислого газу, диму, можливості розпізнавати обличчя, викликати охорону та закривати жалюзі, коли спрацює сигналізація.

Друге завдання – комфорт. Більше не потрібно вмикати і вимикати світло, регулювати рівень тепла або вмикати зволожувач повітря. Керування комфортом у приміщенні тепер відбувається централізовано з пристрою на екран телефону, або автономно, без втручання людини.

Третє завдання – енергозбереження. Встановлення розумних розеток, дозволить повністю контролювати електроприлади у приміщенні. Технології розумного будинку дозволяють оптимізувати витрати на електроенергію за допомогою автоматичного керування приладами клімат-контролю, освітлення та іншими споживачами. Такий контроль значно знижує споживання електроенергії. У деяких випадках економія становить 25-30%.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Принцип будови та склад розумного будинку:

Система розумного будинку складається з багатьох електронних пристроїв. Їх кількість залежить від задач та можливостей розумного будинку, або потреб його власника. Автоматизувати можна майже будь-які задачі або дії, але відповідно до складності цих показників, кількість пристроїв у мережі розумного будинку буде збільшуватись.

Існує ряд пристроїв, які вважаються стандартними при побудові мережі розумного будинку, а також ряд інших, менш використовуваних пристроїв.

Пристрої можуть керувати опаленням, постачанням газу та води, електроенергією, системою освітлення, відеонаглядом, сигналізацією, пожежною безпекою, системою контролю доступу та іншим.



Рисунок 1.3 – Схема будови системи розумного будинку

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Зазвичай розумний будинок складається з деяких загальноприйнятих пристроїв, які є типовими та застосовуються у великій кількості систем. Серед них є такі як:

Датчики відкриття вікон та дверей;

Датчики чадного газу і диму;

Датчики руху;

Розумні розетки;

Датчики протікання води;

Датчики вологості та температури;

Смарт лампи;

Системи відеоспостереження;

Розумне відеовічко у дверях;

Відеодомофон

Крім того, пристрої можуть бути доволі різноманітними, кожен може підібрати щось собі до смаку. Так наприклад існують розумні мультиварки, кавоварки, чайники, водонагрівачі, праски, подушки, тощо.

Основним пристроєм у мережі розумного будинку є хаб(контроллер). Він є головним у системі, у більшості випадків без нього не можна побудувати єдину систему. Без нього це просто набір розрізнених пристроїв. Основне завдання хаба це прийом, відправка та обробка інформації з пристроїв для подальшого прийняття рішень.

Хаб складається з декількох компонентів, таких як апаратна та програмна частина. Апаратна частина містить у собі процесор, модуль зв'язку, блок живлення, та елементи керування, такі як дисплей та кнопки управління. Програма частина – це програмне забезпечення, що керує взаємодією інших пристроїв у мережі. Пристрої розумного будинку є мережевими та, як правило, мають у собі вбудований комутатор.

Мережа розумного будинку спочатку будується з хаба, до якого потім додається інша кількість пристроїв.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.4 – Хаб розумного будинку

При побудові системи, необхідно звернути на кількість сумісних протоколів. Чим більше протоколів підтримується – тим краще. На сьогодні найвикористовуванішими протоколами у системах розумного будинку є Bluetooth LE, Z-Wave, ZigBee та Lutron ClearConnect.

Існують і підготовлені набори для побудови системи розумного будинку. Так наприклад на рисунку 1.5, виробником запропоновано набір, до якого входять датчик руху, датчик відкриття дверей та вікон, хаб, розумна розетка та безпроводна кнопка-дзвінок

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.5 – Готове рішення розумного будинку від виробника

Недоліки розумного будинку:

Основний недолік це ціна. Незважаючи на простоту пристроїв, датчиків, камер та сенсорів, вартість системи досить висока. Термін, за який економія за допомогою розумного будинку перекриває його вартість становить близько п'яти років. Ще одним недоліком є обслуговування. Звісно пристрої розумного будинку можуть вийти з ладу, як і будь-які інші прилади. У такому випадку, вирішення неполадок можуть виконати тільки досвідчені робітники, яких досить важко знайти. Також вихід з ладу одного пристрою, може порушити працездатність усієї системи. Третім недоліком є складність установки системи. Так як в основному більшість пристроїв є дротовими, то встановлювати їх потрібно під час ремонту, або робити ремонт під систему розумного будинку.

Головне під час установки системи обрати правильне якісне обладнання та досвідчених спеціалістів. У такому разі шанс виходу з ладу зменшується.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

1.2 Безпека розумних будинків

Безпекою інформаційних технологій визначає те, наскільки комп'ютерна система захищена від крадіжки або пошкодження даних. З розвитком пристроїв зростає і важливість усвідомлення їх безпеки. Так як з кожним днем системи розвиваються, відповідно до цього розвиваються і загрози. Пристрої розумного будинку вимагають надійності, стабільності та стійкості до загроз.

Більшість систем безпеки забезпечують основні функції захисту, такі як моніторинг, виявлення та контроль загроз, запобігання втрати даних, забезпечення конфіденційності та цілісності, захист обладнання та забезпечення надійної та доступної системи.

Безпека розумного будинку включає в себе систему дистанційного керування, яка може розпізнавати, коли хтось проникає в будинок, або виникає пожежа. Коли виникла загроза, система має автоматично прийняти рішення. Прикладом може бути увімкнення спринклера води, коли спалахнула пожежа. Ця система вмикається автоматично, при спрацюванні датчику диму.

Інший приклад, коли у розумний дім вбудована система сигналізації, та хтось намагається проникнути у приміщення за допомогою ударів, зламу дверей чи вікон, або просто руху у приміщенні, вмикається сигналізація, та в деяких випадках викликає охорону або правоохоронні органи.

Основною причиною встановлення розумних будинків є безпека. Основна частина споживачів живе у містах, де рівень злочинності вищий за норму. ENISA уточнює, що потреба в безпеці розумного дому зростає протягом останніх років, але сьогодні ще існує різниця між безпекою у її традиційному сенсі, та безпекою, що впроваджують розумні будинки. ENISA зауважує, що основна проблема розумних будинків є те, що їх пристрої є занадто слабкими, щоб впоратись з важкими потребами захисту. Також стандарти безпеки не визначені для апаратної частини пристроїв, тобто пристрої мають слабкі ЦП, обмежену кількість оперативної пам'яті, низьку пропускну здатність та слабкі батареї.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.6 – Приклад системи безпеки

Загрози розумному будинку:

Загрози розумному дому поділяються на категорії і мають різні характеристики. Такі характеристики є загальними і забезпечать огляд, який покаже, що існує не тільки один спосіб виконати атаку. Більш конкретні загрози для розумного дому представлені у відповідності з наведеними нижче загрозами.

Фізичні атаки

Фізичні атаки – це ідентифікована атака, яка використовувала постачальника, щоб отримати якомога більше інформації про пристрої. Більш конкретно в контексті розумного дому цей вид загроз може полягати в тому, що зловмисник пошкоджує

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

обладнання та від'єднує кабелі. Іншим прикладом атаки на цю категорію може бути те, що зловмисник використовує глушіння і, отже, порушує трафік і передачу даних.

Ненавмисне або випадкове пошкодження

Ненавмисне або випадкове пошкодження може статися, якщо особи не навчені або якщо мешканці не мають знань. Більш конкретно в контексті розумного дому цей вид загроз може виглядати наступним чином.

Випадкова зміна даних – це тип загрози, який може виникнути в контексті розумного дому і може викликати помилки. Результатом помилок може бути несправність пристрою з підтримкою мережі.

Витік інформації – це коли користувач мережевих пристроїв в розумному будинку випадково розкриває інформацію про датчики через відсутність політики безпеки. Такі пристрої мають обмежені можливості для впровадження програмного забезпечення, яке може працювати з ПЗ безпеки, щоб зменшити ризик витоку даних. Інформація з небезпечних джерел може бути проблемою, якщо пристрої розумного дому спілкуються з датчиками або даними, що зберігаються в хмарі. Непорозуміння у зв'язку між пристроями може призвести до небажаної поведінки. Прикладом такої поведінки є те, що передавач запускає зловмисні сценарії, що може призвести до атаки.

Відсутність планування може спричинити серйозні недоліки безпеки та конфіденційності. Погане планування установки може відбуватися на різних рівнях; рівень компонента, рівень проектування, рівень політики або рівень встановлення. Якщо протоколи та програма розроблені невідповідним чином, це може призвести до відхилення від служби. Це може призвести до серйозних наслідків у аспектах безпеки та конфіденційності.

Збої та несправності

Збій або несправність – це загрози, які найбільш ефективні для зловмисника. Це перший крок в інших методах порушення цілісності системи. Нижче наведено приклади того, як може виглядати така атака.

Несправність Інтернету може вплинути на пристрої, які залежать від хмари чи інтернет-сервісу. Телебачення, яке передає дані з інтернету, не працюватиме, доки

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

не буде відновлено послуги, пов'язані з підключенням домережі. Також буде порушено працездатність віддаленого доступу до пристроїв розумного дому.

Збої в комунікаційній технології можуть бути апаратними, програмними помилками або навмисними атаками. Це може бути одночасно як навмисне, так і ненавмисне виведення з ладу.

Цей тип загрози може призвести до відсутності зв'язку між пристроями і в результаті повної втрати функціональності. Несправність пристроїв, датчиків, приводів у мережі розумного дому може призвести до незначних або серйозних наслідків, залежно від того, який мережевий пристрій має збій.

Несправність живлення є проблемою, оскільки багато менших пристроїв, компонентів і датчиків працюють від батареї, тоді як системи опалення та аудіо-візуальні пристрої вимагають мережевої електроенергії. Перебої в роботі можуть призвести до пошкоджень, таких як відсутність гарячої води, чи несправність системи опалення.

Пошкодження, викликані пристроями та датчиками сторонніх виробників, можуть викликати проблеми, оскільки відновлення або заміна пошкодженої частини може зайняти багато часу. Пристрої стороннього виробника можуть бути ненадійними та ставлять під загрозу безпеку та конфіденційність розумного дому.

Навмисні погрози або зловживання

Навмисні погрози або зловживання, такі як підслуховування, перехоплення або викрадення, можуть бути здійснені зловмисником. Метою такого типу загроз може бути отримання доступу або виявлення або впровадження слабких місць. Після виконаної атаки користувач або резидент міг втратити контроль над мережевим пристроєм або даними конфіденційності, і тому конфіденційність і цілісність були порушені.

Шахрайство з ідентифікацією може стати проблемою, оскільки розумний дім зберігає та обробляє інформацію користувачів для різних типів послуг. Зловмисник може підробити цю інформацію і здаватися легальним користувачем. Зловмисник із таким типом підробленої особи може отримати несанкціонований доступ до прав адміністратора та втрутитися в налаштування розумний дому.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

DDoS або DoS, може легко поставити під загрозу зв'язок і трафік між підключеними пристроями. DoS-атака може бути специфічною для даних, як-от спуфінг або флуд, коли зловмисник вказує, які дані слід надіслати з одного хоста. Якщо атака поширена, дані будуть надіслані з кількох хостів. Результатом такого типу загрози або атаки є запобігання використанню та обслуговування пристрою.

Маніпулювання інформацією, знайденою в датчиках і мережевих пристроях, може призвести до наслідків. Датчики або пристрій можуть отримувати неправдиву і неточну інформацію. Це може призвести до обходу функцій безпеки та розкриття облікових даних. Це також може призвести до шантажу, шахрайства та підвищення привілеїв.

Викрадання/перехоплення трафіку може стати причиною дій з метою отримання несанкціонованої інформації. Багато датчиків і пристроїв виробляють велику кількість даних, пов'язаних з користувачами розумного дому, таких як відсутність, присутність та дії резидента.

1.3 Доступні технології комунікації пристроїв розумного будинку

У цьому розділі представлені комунікаційні технології, які використовуються в розумному домі. Кожна комунікаційна технологія представлена характеристиками, безпекою та вразливими місцями.

Модель OSI відіграє важливу роль у мережевих пристроях. OSI-модель представлена для кожної комунікаційної технології та додатково пояснена в таблиці.

Таблиця 1.1

Рівні моделі OSI та атаки на цих рівнях

Рівень моделі OSI	Атаки
Рівень 7. Прикладний	SQL-ін'єкції, віруси
Рівень 6. Представлення	SSL- та HTTP атаки
Рівень 5. Сеансовий	«Викрадення сеансу», Telnet DDoS
Рівень 4. Транспортний	DoS, SYN-флуд

Рівні моделі OSI та атаки на цих рівнях

Рівень 3. Мережевий	MITM
Рівень 2. Канальний	MAC-фільтрація/спуфінг
Рівень 1. Фізичний	Фізичне ушкодження

ZigBee

ZigBee — це малопотужна бездротова технологія, побудована як сітчаста топологія на основі стандарту IEEE 802.15.4 для персональної мережі (PAN) з акцентом на додатках для моніторингу, контролю та виявлення. В основному він працює в діапазоні ISM 2,4 ГГц і має номінальний діапазон 100м. ZigBee Alliance працює над тим, щоб стати стандартом для пристроїв розумного дому, від систем температури та освітлення до моніторів безпеки та детекторів диму. Найвищий діапазон даних становить до 20 Кбіт/с у діапазонах 913 МГц та 868 МГц та 250 Кбіт/с для діапазону 2,4 ГГц. ZigBee використовує стандарт IEEE 802.15.4 як фізичний рівень і рівень каналів передачі даних, тоді як протокол заснований на моделі OSI і працює на верхніх рівнях, від мережі до рівня програми.

Технологія ZigBee була випущена в 2001 році і оновлена до ZigBee Pro Specification в 2007 році, остання повністю зворотно сумісна, основна відмінність полягає в тому, що функція забезпечує кращу безпеку. Версія Pro часто використовується, коли мережа ZigBee дуже велика і кращі функції безпеки важливі для мережі.

ZigBee зарекомендував себе як один з провідних комунікаційних протоколів для бездротових сенсорних мереж (WSN), а переваги технології — низька вартість і низька складність. Відомими обмеженнями є обмеження вузлів, обмежений обсяг пам'яті, обмежене споживання енергії та комунікаційні обсяги, такі як швидкість передачі даних.

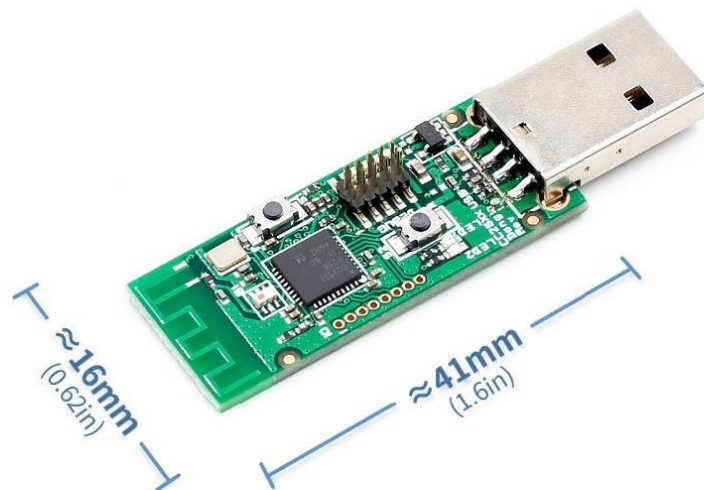


Рисунок 1.7 – Приклад модулю ZigBee

Безпека та вразливості

У технології ZigBee є чотири концепції, які вважаються важливими для безпеки:

ZigBee підтримує два різних рівня безпеки, один з яких називається «Комерційна безпека», який має високий рівень безпеки, і стандартний рівень безпеки, який називається Residential Security. Відмінності між ними в основному полягають у розподілі та управлінні ключами.;

У мережі з підтримкою ZigBee один з блоків під назвою Trust Center відповідає за безпеку. Центр довіри надає механізм безпеки з трьома різними типами ключів безпеки: мережевий ключ, головний ключ і ключ посилення. Центр довіри також відповідає за вибір рівня безпеки та керування ключами. Потім блок ZigBee ділиться ключем корпоративної мережі, а ключ з'єднання може бути розділений між двома пристроями

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

ZigBee, ключ з'єднання є від головного ключа і важливий для довгострокової безпеки між двома пристроями ZigBee.

Аутентифікація та шифрування даних Дані шифруються за допомогою 128-бітного стандарту шифрування AES з режимом CCM, який дозволяє аутентифікацію та шифрування даних під назвою AES-CCM. CCM корисний лише для 128-бітних криптографічних блочних шифрів. ZigBee використовує модифіковану версію CCM під назвою CCM*, це дозволяє використовувати або аутентифікацію, або шифрування. У звичайній версії CCM потрібні обидва.

Щоб переконатися, що цілісність і свіжість даних є належним, можна використовувати код цілісності повідомлення (MIC). MIC перевіряє, що дані не були змінені під час транспортування та згенеровані за допомогою протоколу CCM*.

Для підвищення безпеки в рамках технології ZigBee виділено деякі вимірювання лічильника. Одне з удосконалень називається «WZ-lcp», що є протоколом/схемою для підвищення безпеки та захисту як від активних, так і від пасивних атак у розумному домі. “WZ-lcp” використовує новий метод аутентифікації, використовується шифрування XOR і обчислення виконується двічі.

Обмеження в рамках технології, згаданій раніше, обмеження вузлів, обмежений обсяг пам'яті, обмежене споживання енергії та комунікаційні можливості, ускладнюють впровадження механізму безпеки як криптографії з відкритим ключем для підвищення безпеки. Більш пізні версії ZigBee пропонують покращення, наприклад, енергоспоживання, але технологія все ще має багато недоліків, які можуть призвести до збоїв у безпеці.

Виділеними атаками можуть бути фізичні атаки (наприклад, вандалізм і саботаж), атаки на ключ (тобто спроба відновити криптографічний ключ схеми шифрування) і атаки відтворення та ін'єкції (тобто мережева атака, під час якої дані шахрайським шляхом повторюються або затримуються), як можливі загрози та вразливості безпеки в технології ZigBee.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

В іншому дослідженні ZigBee згадується, що датчики та приводи часто працюють від батарейок і мають дуже низький робочий цикл. Низький робочий цикл означає співвідношення між часом активного радіо та періодом мовчання, який мережа попередньо визначила для інтервалів пробудження для збереження акумулятору. Однак це може відкрити двері для атаки DoS, коли зловмисник може неодноразово атакувати пристрої. Таким чином, нескінченний цикл DoS-атаки може призвести до розрядження акумулятора або його значного зменшення циклу роботи.

Безпека ZigBee спрямована на втручання, саботаж або маніпулювання даними. Фізична атака також може бути здійснена проти технології ZigBee, і це повинно бути враховано при формуванні мережі. Оскільки ZigBee часто використовується для керування моніторингом та зондуванням, які можуть містити критичні системи керування, наприклад, промислове підприємство чи домашню систему безпеки, дуже важливо мати на увазі, що проект мережі ZigBee виконується таким чином, щоб пристрої були захищені від фізичної атаки. Це можна зробити, розмістивши пристрої у важкодоступних місцях, але також захищаючи їх за допомогою спостереження. Якщо зловмисник краде пристрій ZigBee, з нього можна витягти дані, а також збережені ключі безпеки.

Однак ця атака працює лише на чіпах ZigBee від деяких виробників, тому автоматична система важлива для виявлення та повідомлення про відсутні одиниці. Якщо пристрій відсутній, ключі безпеки необхідно оновити безпосередньо, щоб зупинити можливе несанкціоноване використання всієї мережі ZigBee.

Wi-Fi

За даними Wi-Fi Alliance, всесвітньої мережної компанії, Wi-Fi є найпоширенішою технологією бездротового зв'язку. Це основна технологія для інтернет-трафіку і використовується 13 мільярдів пристроїв. Це також робить його однією з найпопулярніших технологій для розумних будинків. Сигнал Wi-Fi можна використовувати для різноманітних речей у розумному домі, але перевага надається операціям розпізнавання, тобто розпізнавання руху та виявлення падінь через його чутливість до динаміки навколишнього середовища.

		Вексей О.І.			KIK.KP.B – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Розумний дім, заснований на Wi-Fi, вважається економічно ефективним і пропонує комфортне розгортання.

Згідно з цим дослідженням, стандарт Wi-Fi IEEE 802.11ah є найбільш актуальним розробленим стандартом. IEEE 802.11ah забезпечує покращення обмеженого діапазону, а завдяки останнім розробкам може забезпечити більший діапазон і, отже, полегшити підключення до програм і пристроїв.

Стандарт Wi-Fi IEEE 802.11ah працює на частотах 2,4 ГГц і 5 ГГц і зменшує складність реалізації. Раніше встановлені стандарти Wi-Fi в сімействі 802.11 є більш ефективними в найближчій точці доступу і не можуть надавати послуги користувачам у великих будинках.

Стандарт 802.11ah працює на рівнях 1 і 2 відповідно до моделі OSI.

IEEE 802.11ah - це стандарт, який показаний як Wi-Fi 6, ймовірно, буде одним із відомих на ринку. Стандарт додає, наприклад, ефективність, гнучкість і масштабованість, що означає, що нові та існуючі мережі можуть збільшити як швидкість, так і пропускну здатність. Розширення систем розумного дому та Інтернету речей змусило розробку покращитися, і новий стандарт є результатом цього.

Безпека та вразливості

Відомими проблемами з технологією Wi-Fi є WEP (Wireless Equivalent Privacy) і WPA (Wi-Fi Protected Area), оскільки обидва можуть бути зламаними. WPA2 є покращенням, і якщо його правильно налаштовано, зломиснику потрібно більше часу, щоб зламати систему.

У січні 2018 року Wi-Fi Alliance оголосив, що повинні бути нові вдосконалення специфікації WPA2. Удосконалення під назвою WPA3 включає вимоги до аутентифікації, шифрування та конфігурації. Фактично, покращений захист для мереж, які використовують аутентифікацію на основі пароля, з покращеною конфіденційністю у відкритих мережах, паліативним захистом від відмови в обслуговуванні та більш надійним криптографічним алгоритмом. WPA3 створить механізм для пристроїв IoT без або з обмеженим інтерфейсом користувача для надійних мереж.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Відомі вразливості щодо Wi-Fi можуть полягати в тому, що зловмисник дублює точку доступу і отримує несанкціонований доступ до системи розумного дому. Коли зловмисник продовжує дублювання точки доступу, можна реалізувати систему за допомогою шкідливого програмного забезпечення. Крім того, є повідомлення про те, що WPA2 було порушено, коли зловмисник використовував інструменти бездротової мережі для виявлення мереж та інформації про мережі з наміром отримати несанкціонований доступ або використати систему.

Ще одна загроза, до якої уразливий Wi-Fi, — це атака DoS. DoS-атака має на меті вимкнути або поставити під загрозу доступність мережі. Це можна зробити за допомогою Flooding DoS-атаки або атаки зловживання протоколом, що називається «DeAuthentication DoS», який спрямований на зв'язок між користувачем і бездротовою точкою доступу Wi-Fi. На рівні 2 моделі OSI кадри керування 802.11 надсилаються у вигляді простого тексту та транслюються, що дає можливість підрозділам у межах досяжності виявляти мережі та вимагати підключення. Це є причиною багатьох проблем безпеки, якщо зловмисник ловить кадр керування відкритим текстом, він може підробити пакети. Два потенційних типи кадрів, які можна використовувати для стану DoS в протоколі 802.11, це кадри DeAuth (DeAuthentication) і DisAssoc (DisAssociation).

Отримання фрейму DeAuth або DisAssoc перемістить жертву з автентифікованого стану в точці доступу і не дозволить обмін пакетами даних.

Завдяки наведеній вище інформації інсайдерові чи зловмиснику ззовні легко використовувати такий інструмент, як Wireshark, щоб здійснити підслуховування мережевого трафіку та отримати цінну інформацію про мережу, яку на наступному етапі можна використати для атаки.

Z-Wave

Z-wave було розроблено в 2001 році. Найновішим оновленням комунікаційної технології є ZWave Plus яке було випущено в 2013 році, та містило у собі покращення, як кращий термін служби акумулятора та більший діапазон бездротового зв'язку. Z-Wave — це малопотужний протокол бездротового зв'язку для домашньої автоматизації, спеціально для застосування дистанційного керування

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

в житлових і невеликих комерційних середовищах. Z-Wave впроваджено у величезну кількість продуктів по всьому світу, наприклад. домашній кінотеатр, автоматизована обробка вікон, контроль басейнів і спа-салонів і автоматизовані показання лічильників.



Рисунок 1.8 – Реле з технологією Z-Wave

Z-Wave реалізовано на чотирьох нижніх рівнях моделі OSI: фізичному, каналі передачі даних, мережевому та транспортному рівні. ZigBee також побудований на топології мережевої мережі, що означає, що пристрої працюють як ретранслятори сигналів, і мережа буде міцнішою, якщо ви установите більше пристроїв. Сигнал легко проходить через більшість стін, підлог і стель, що призводить до великого радіусу дії приблизно до 100 метрів на відкритому повітрі, оскільки будівельні матеріали зменшують радіус дії в приміщенні, навіть якщо він добре переміщається. Для найкращого ефекту рекомендується використовувати один пристрій Z-Wave приблизно через кожні 30 футів або ближче.

Z-wave несумісний з IP і не може підключатися безпосередньо до Інтернету або до пристрою користувача без контролера для керування пристроями. Контролер діє як шлюз, який керує взаємодією між пристроями Z-wave і смартфоном через Інтернет або з локальної мережі. Добре відомо, що Z-Wave є власним протоколом, який належить Sigma Designs і рекламується Z-wave Alliance, який продав майже 100 мільйонів пристроїв.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Безпека та вразливості

Sigma Design спробувала покращити безпеку на Z-wave, і нещодавно вони оголосили про нову систему безпеки для цієї технології. Реалізація нової мікропрограми в рамках останньої платформи вплине на шлюзи та пристрої, які отримали оновлення мікропрограми, пристрої, які не мають оновлення, можуть мати потенційні проблеми з безпекою.

Відомі вразливості та загрози для Z-Wave, наприклад, «Атака видання себе за іншу особу», яка є атакою, коли опонент приймає ідентичність однієї з законних сторін або комунікаційних технологій. Зазвичай цей тип атаки здійснюється шляхом надсилання електронного листа на адресу, де відправник маскує себе як надійне джерело, щоб отримати доступ до конфіденційної інформації. Інша атака, наприклад «Атака чорної діри», яка схожа на DoS. Передбачається, що маршрутизатор передає пакети, але замість цього відкидає їх, коли відбувається ця атака.

KNX RF

KNX — це технологія дротового та бездротового зв'язку, KNX і KNX RF (радіочастота). KNX — це скорочення від «connexio», що на латині означає підключення. KNX був розроблений в 1991 році і на той час був найпоширенішою технологією в області вентиляції, опалення та кондиціонування повітря, яка називалася HVAC. Багато пристроїв були сумісними з KNX, і в 2006 році KNX став стандартом ISO/IEC. KNX RF базується на OSI-моделі і працює на рівні каналів, транспорту та мережі. Іншими носіями, які використовуються в дисципліні KNX, є вита пара, Ethernet та лінія електропередачі. KNX RF використовується з тими ж діапазонами, що й промислові, наукові та медичні. Частота становить від 868 МГц до 2,4 ГГц.

Безпека та вразливості

KNX не визначає жодних вимірювань безпеки в рамках технології, окрім паролів, що передаються у звичайному тексті. Це вважається вразливістю, оскільки, якщо зловмисник підслуховує передачу повідомлень, він може отримати паролі і, отже, отримати несанкціонований доступ до системи. KNX був додатково

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

розроблений з KNX Data Security, який забезпечує технологію шифрування, перевірки цілісності та аутентифікації за допомогою 128-бітного AES.



Рисунок 1.9 – Актуатори з технологією KNX RF

Безпека та вразливості

KNX не визначає жодних вимірювань безпеки в рамках технології, окрім паролів, що передаються у звичайному тексті. Це вважається вразливістю, оскільки, якщо злоумисник підслуховує передачу повідомлень, він може отримати паролі і, отже, отримати несанкціонований доступ до системи. KNX був додатково розроблений з KNX Data Security, який забезпечує технологію шифрування, перевірки цілісності та аутентифікації за допомогою 128-бітного AES.

Bluetooth LE

Bluetooth Low Energy - це технологія бездротового зв'язку. Комунікаційна технологія є широко використовуваною технологією зв'язку, і майже кожен має досвід роботи з Bluetooth.

Цей метод є дешевим способом передачі даних і вимагає, щоб використовувані пристрої підтримували технологію зв'язку Bluetooth LE. Bluetooth LE працює за стандартом IEEE 802.15.1 і частотою від 2,4 ГГц до 2,485 ГГц, а номінальний діапазон становить 10 м, що вважається малим діапазоном. Споживання електроенергії приладами, що використовуються в цій технології, зменшено, а

		Вексей О.І.			KIK.KP.B – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

термін служби тривалий завдяки використанню батарейок. Використання Bluetooth LE забезпечує пряме з'єднання між пристроями, що використовуються, і немає різниці між використанням мобільного телефону, планшета чи пристроїв розумного дому. Топологія мережі побудована як топологія Star-Bus і працює як вузли один-до-багатьох.

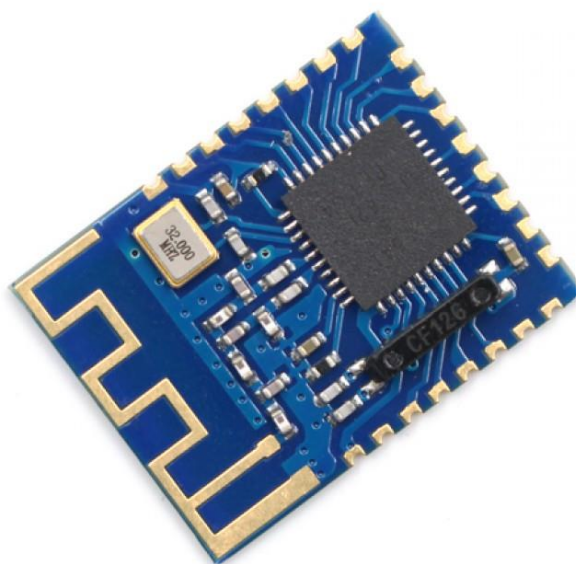


Рисунок 1.10 – Модуль Bluetooth LE

Безпека та вразливості

Bluetooth LE пропонує функції безпеки для захисту інформації під час обміну нею між підключеними пристроями. Функції безпеки поділяються на два режими, режим 1 і режим 2. Кожен режим має різні рівні.

Режим 1 має кілька рівнів, які забезпечують шифрування. Рівень 1 не передбачає жодних функцій безпеки, а це означає, що немає шифрування чи аутентифікації. Рівень 2 не передбачає аутентифікації, але створення пари відбувається з шифруванням. Рівень 3 забезпечує повну безпеку як аутентифікацію, так і шифрування для створення пари. Шифрування не настільки міцне, як хотілося б. Рівень 4 забезпечує надійніше шифрування та аутентифікацію. Шифрування використовує алгоритм AES-CCM на додаток до еліптичної кривої P-256. AES-CCM — це хеш-функція з ключем, яка заснована на симетричному шифрі як AES.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Шифрування приймає ключ шифрування, одноразовий код шифрування та корисне навантаження як вхідні дані.

Режим 2 має кілька рівнів, які забезпечують підписання даних. Підписання даних забезпечує цілісність, але не конфіденційність даних. Рівень 1 не вимагає аутентифікації з підписом даних під час з'єднання пристроїв у пару. Рівень 2 вимагає аутентифікації з підписом даних під час з'єднання пристроїв.

Немає захисту від пасивного прослуховування, навіть якщо шифрування та аутентифікація реалізовані в технології. Це дає змогу зловмиснику або пасивному підслуховувачу визначити LTK (довгостроковий ключ), CSRK (ключ розпізнавання підпису з'єднання) або IRK (ключ визначення ідентифікації).

Функція «Просто працює», яка є методом сполучення, не забезпечує захист MITM, коли пристрої об'єднані в пару, що означає, що коли використовується функція Just Works, технологія слабка для MITM-атак. Якщо це станеться, зловмисник може маніпулювати даними, які передаються між пристроями.

Пара ключів ECDH, якщо вони слабкі, вони можуть мінімізувати захист від прослуховування для SSP. Ця слабкість може дозволити зловмиснику визначити секретні ключі посилання. Тому всі пристрої повинні мати міцні пари ключів. Під час створення пари пристроїв ключ доступу забезпечує захист пристрою під час використання SSP. Слабкість виявляється, коли ці ключі доступу статичні, і це може призвести до MITM-атаки. Таким чином, ключі доступу мають бути унікальними та унікальними для кожної пари. Якщо пристрій налаштовано на певний режим безпеки і пристрій може повернутися до іншого режиму безпеки під час підключення до пристрою, який не підтримує той самий режим або рівень, може статися, що пристрій повернеться до режиму безпеки 1, який не забезпечує ніякої безпеки.

Коли спроби аутентифікації повторюються, в пристрої має бути впроваджено технологію Bluetooth LE, щоб пристрій міг впоратися із загрозою без збоїв. Ця реалізація повинна полягати в тому, що існує необмежена кількість запитів на аутентифікацію, але якщо запити налаштовані на очікування відповіді, зловмисник

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

може підкрататися між спробами та отримати інформацію про секретний ключ посилання через виклики відповіді.

Розглянута вразливість у Bluetooth LE може полягати в тому, що якщо ключі, які використовуються для керування та підтримки підключення, зберігаються неналежним чином, їх може отримати зловмисник. Дані між наскрізними пристроями шифруються та аутентифікуються лише в певних точках. На проміжній точці дані розшифровуються, тому важливо мати додатковий захист для пом'якшення цієї проблеми. Загалом функції безпеки не є частиною стандарту. У корпорації з розробником можна покращити безпеку.

Технологія Bluetooth LE знаходиться в зоні ризику для запланованих атак і загроз, таких як:

Bluesnarfing - мета якого - отримати доступ до пристрою з підтримкою Bluetooth за допомогою мікропрограми.

Bluejacking - цю атаку можна провести на будь-якому мобільному пристрої з увімкненим Bluetooth. Зловмисник надсилає повідомлення користувачеві пристрою, і на пристрої можна вносити зміни. Це може завдати шкоди користувачу або пристрою, якщо це задумано.

Bluebugging – ця атака використовує недоліки безпеки у мікропрограмі, щоб отримати доступ до пристрою. Атака виконує дії без інформування користувача, а метою атаки, окрім отримання доступу, може бути розміщення або підслуховування телефонних дзвінків, надсилання повідомлень або використання інших служб.

Car Whisperer - використовує стандартний ключ доступу (якщо користувачі не вибрали випадковий пароль) і націлений на пристрої Bluetooth, встановлені в автомобілях.

DoS - як і більшість бездротових технологій, Bluetooth LE чутливі до такого роду атак. Мета цієї атаки може бути різною, але головна мета – перешкодити руху.

Fuzzing attack – ця атака надсилає шкідливі дані на пристрій і чекає реакції.

Якщо є реакція, зловмисник може припустити, що в стеку протоколів є

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

слабкість, яку він чи вона може скористатися. Підслуховування в парі – зловмисник збирає кадри, які надсилаються при з'єднанні між пристроями, і надалі визначає секретні ключі та отримує з них розшифровані дані.

Secure Simple Pairing Attacks - існує багато інструментів, щоб змусити пристрій використовувати таку функцію, як «Просто працює», а після цього використовувати пристрій MITM-атакою через відсутність захисту

Thread

Thread вийшов на ринок у 2016 році компанією Thread Group і на момент написання розширюється як комунікаційна технологія і підтримується кількома найбільшими компаніями в цій галузі; Apple, Siemens і Samsung. Thread розроблений і класифікований для домашньої автоматизації. Ця комунікаційна технологія має бути унікальною з точки зору взаємодії, безпеки, потужності та архітектури пристроїв розумного дому. Thread має бути малопотужним мережевим протоколом, здатним підключати як пристрій-пристрій, так і пристрій-хмара, мати нульову точку збою та бути заснований на стандарті IEEE 802.15. Thread призначений для використання як у малих, так і у великих мережах з пристроями малої потужності, а номінальний діапазон становить 30 м, що вважається середнім.

Thread працює на радіостандарті IEEE 802.15.4. Стандарт IEEE 802.15.4 розроблений для роботи з низьким споживанням енергії та низькою затримкою. Further Thread використовує протокол IPv6 для зв'язку, який є бездротовим мережевим протоколом, де 6LoWPAN є основою, яка є аббревіатурою від «IPv6 over Low-Power Wireless Personal Area Networks». OSI-модель є центральною частиною того, як комунікація працює в рамках технології. Реалізація протоколу потоку бере участь у рівнях 3 і 4, тоді як стандарт IEEE 802.15.4 бере участь у рівнях 1 і 2.

Інтернет-протокол є ключем до доступу до Інтернету, і оскільки Thread заснований на IPv6, ця технологія надає пристроям можливість безперешкодно спілкуватися з домашніми, хмарними та мобільними пристроями. IPv6 дозволяє технології Thread підключатися як до користувачів, так і до пристроїв.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

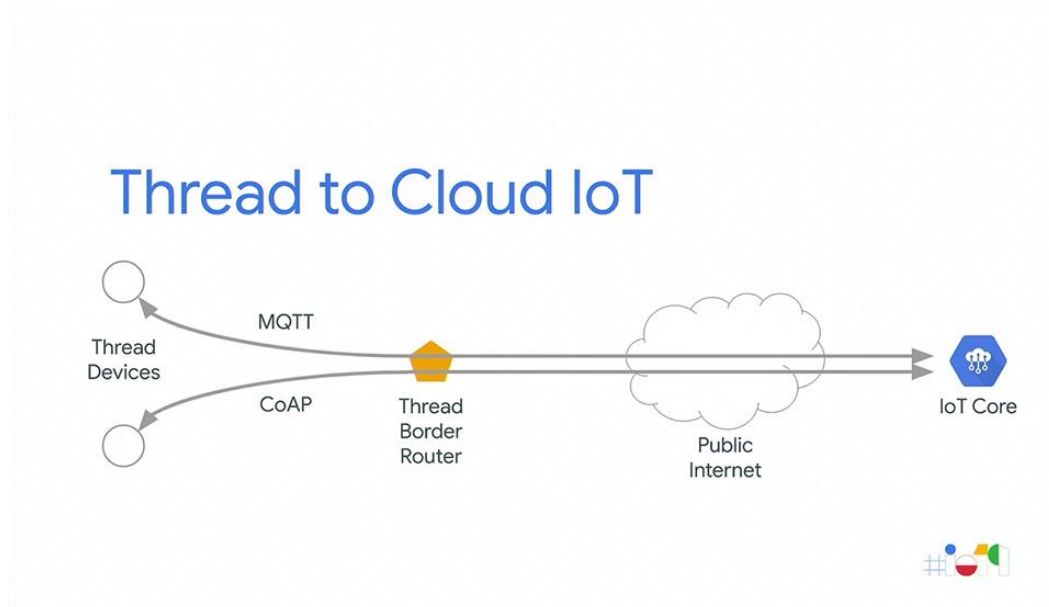


Рисунок 1.11 – Схема роботи Thread

Безпека та вразливості

Thread не має точки збою, оскільки вона, як технологія, може вилікуватися сама. Таким чином, мережа з реалізованим Thread є стійкою і може переналаштуватися, коли новий пристрій додається або видаляється з мережі.

Стійкість важлива з точки зору безпеки, але додатково до функції самонастроювання додається безпека, наприклад, тільки автентифіковані пристрої можуть приєднатися до мережі. Зв'язок захищений за допомогою шифрування.

Шифрування — це фундаментальна безпека комунікаційної технології Thread. Метод шифрування — це шифрування AES-CCM, а обмін ключами відбувається за допомогою методу, заснованого на еліптичній кривій Діффі-Хелмена P-256, яка є стандартизованою NIST еліптичною кривою. Метод обміну ключами за допомогою еліптичних кривих називається «Juggling Password-Authenticated Key Exchange, J-PAKE» і діє як угода про ключ, а підпис Schnorr NIZK (Non-Interactive Zero-Knowledge) працює з аутентифікацією між одноранговими користувачами.

Поки що авторам не вдалося знайти жодної вразливості для цієї комунікаційної технології. Технологія Thread є безпечною відповідно до технічних документів Thread Groups, і авторам є відомі вразливості, які можуть бути використані.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

1.4 Постановка технічного завдання

Дана дипломна робота може послужити підґрунтям для створення нових систем розумних будинків з використанням усіх сучасних технологій. Призначенням розробки є побудова та налаштування, а також перевірка працездатності системи розумного будинку, налаштування автоматизацій, та перевірка безпеки мережі.

В цьому розділі було проаналізовано будову розумного будинку, технології які в ньому використовуються, їх переваги та недоліки а також особливості засобів що використовуються у розумному будинку. З першого розділу можемо побачити, що системи розумних будинків активно розвиваються в сучасному світі через їх важливість та актуальність. Розглянуті технології показують свій стрімкий розвиток протягом останнього часу. Це означає що системи розумних будинків будуть ставати дедалі зручнішими та безпечнішими, матимуть більш гнучкі налаштування та більший функціонал.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

РОЗДІЛ 2 РОЗРОБКА ТА ДОСЛІДЖЕННЯ РОЗУМНОГО БУДИНКУ

2.1 Моделювання проекту в середовищі Cisco Packet Tracer

Мережа розумного будинку це система домашніх пристроїв, здатних виконувати дії і вирішувати певні повсякденні завдання без участі людини. Функціонально пов'язуються між собою усі електроприлади будівлі, якими можна керувати централізовано — з пульта-дисплею. Прилади можуть бути під'єднані до комп'ютерної мережі, що дозволяє керувати ними за допомогою ПК та надає віддалений доступ до них через Інтернет. Завдяки інтеграції інформаційних технологій у домашні умови, усі системи та прилади узгоджують виконання функцій між собою, порівнюючи задані програми та зовнішні показники (обстановки).

Для проектування системи розумного будинку було обрано середовище програмного забезпечення Cisco Packet Tracer, так як у ньому є достатній набір пристроїв розумного будинку, а також їх гнучке налаштування та програмування.

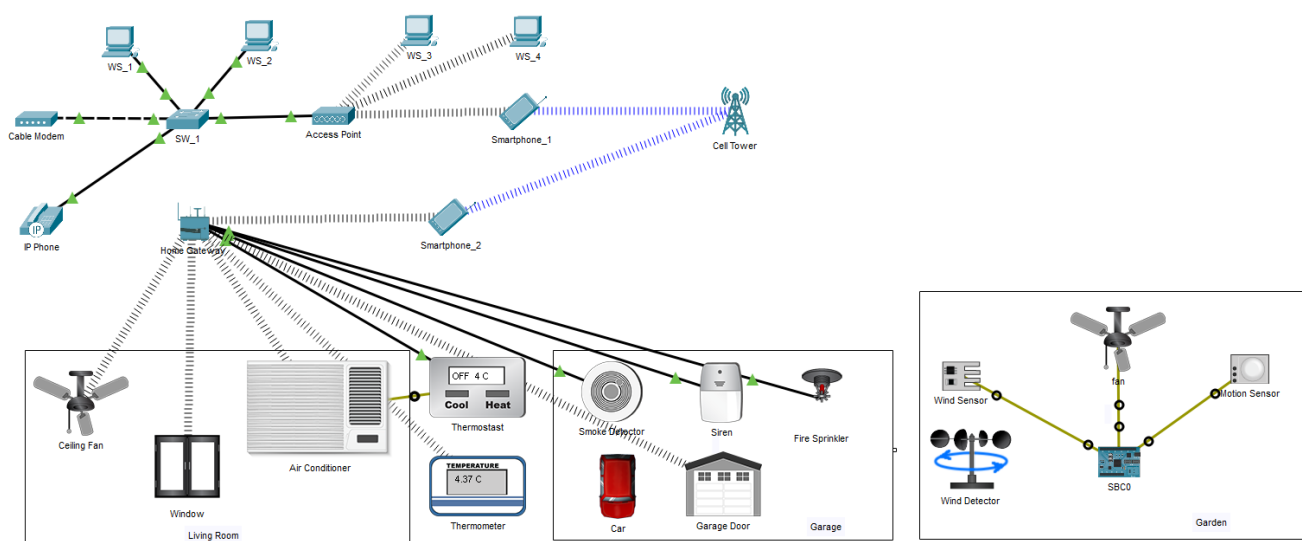


Рисунок 2.1 – Проект мережі

На рисунку 2.1 логічне відображення проекту мережі розумного будинку. Мережа умовно поділена на 2 секції. Перша містить у собі набір комутації та мережевих пристроїв, а друга – це пристрої розумного будинку, які під'єднані до домашнього шлюзу. У другій секції знаходиться три умовних зони:

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

Зона жилої кімнати

Зона гаражу

Вулична зона

Зона №1

У першій зоні зібрані пристрої що відповідають за комфорт. З них два датчики, що забезпечують моніторинг температури повітря, та у випадку термостату, керують приладами комфорту. За допомогою можливостей середовища Cisco Packet Tracer, було запрограмовано декілька функцій, що забезпечують автоматизацію контролю температури.

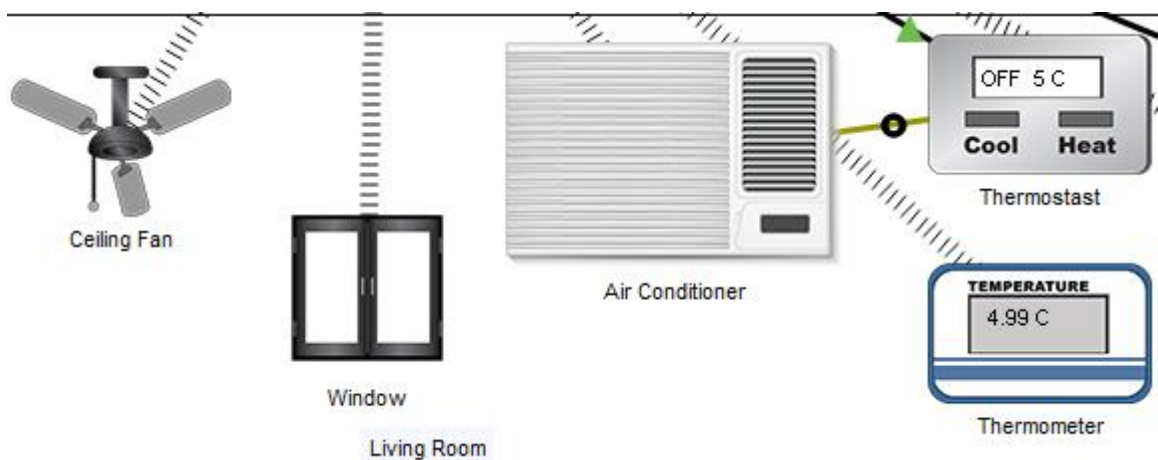


Рисунок 2.2 – Зона жилої кімнати

Так, наприклад, при певній температурі вмикається вентилятор, або відчиняється/зачиняється вікно.

The screenshot shows the IoT Monitor interface with a table of device conditions and actions. The table has columns for Actions, Enabled, Name, Condition, and Actions. The table lists various conditions and actions for the IoT Server - Device Conditions.

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Turn the ceiling	Thermostast Temperature ≥ 12.0 °C	Set Ceiling Fan Status to Low
Edit Remove	Yes	Turn off the ceiling fan	Thermostast Temperature ≤ 8.0 °C	Set Ceiling Fan Status to Off
Edit Remove	Yes	Alarm	Smoke Detector Level ≥ 5	Set Siren On to true
Edit Remove	Yes	Fire Sprinkler	Smoke Detector Level ≥ 5.4	Set Fire Sprinkler Status to true
Edit Remove	Yes	Alarm Off	Smoke Detector Level ≤ 1	Set Siren On to false
Edit Remove	Yes	Sprinkler off	Smoke Detector Level ≤ 1	Set Fire Sprinkler Status to false
Edit Remove	Yes	WIndows ON	Thermostast Temperature ≥ 12.0 °C	Set Window On to true
Edit Remove	Yes	Windows OFF	Thermostast Temperature ≤ 7.0 °C	Set Window On to false
Edit Remove	Yes	Garage Door OFF	Siren On is true	Set Garage Door On to true
Edit Remove	Yes	Garage Door ON	Siren On is false	Set Garage Door On to false
Edit Remove	Yes	Turn on Ceiling HIGH	Thermostast Temperature ≥ 15.0 °C	Set Ceiling Fan Status to High

Рисунок 2.3 – Автоматизація керування кліматом

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Також термостат дозволяє вручну керувати приладами. Якщо перемкнути його у режим охолодження (COOL), увімкнеться кондиціонер.

Пристроями можна керувати також віддалено, за допомогою, наприклад, смартфона, що з'єднаний із домашнім шлюзом.

Так, наприклад, можна увімкнути вентилятор, без фізичної взаємодії з ним.

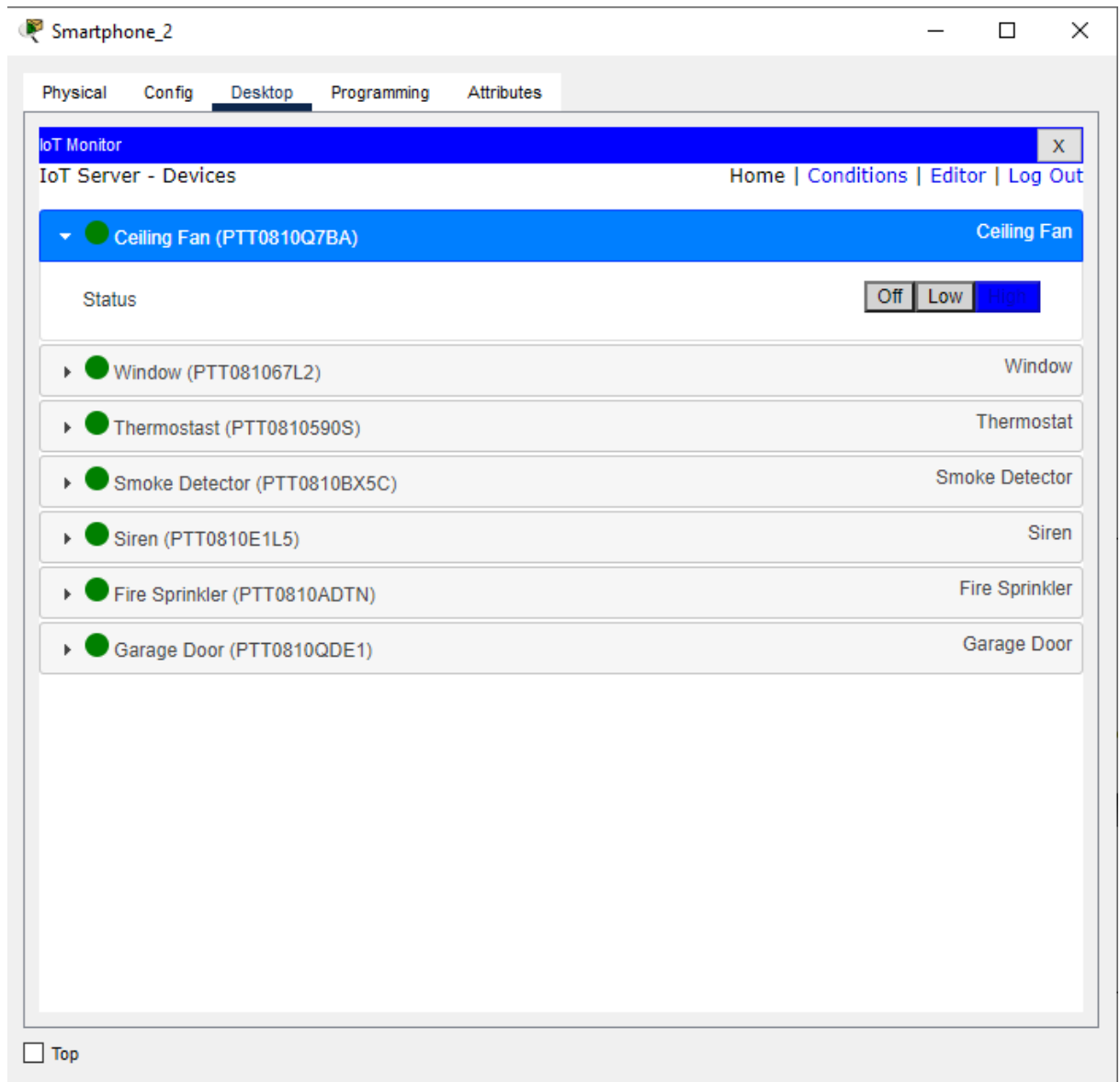


Рисунок 2.4 – Увімкнення вентилятора за допомогою смартфона

Зона №2

Наступною зоною, є зона гаражу. В ньому реалізована система безпеки, що не дозволить скупчення газу, якщо машина була залишена з увімкнутим двигуном на тривалий час.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

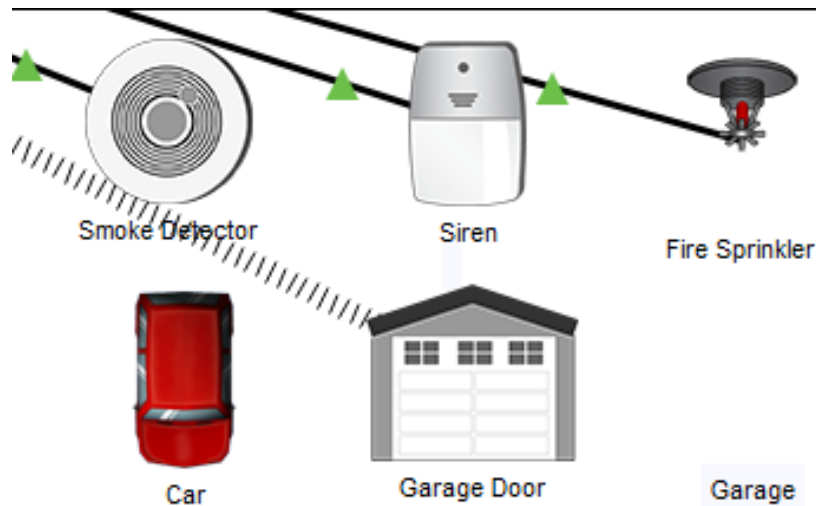


Рисунок 2.5 – Зона гаражу

У цій зоні розташований датчик диму, що при виявленні отруйного газу увімкне сигналізацію, та відкриє ворота гаражу. У випадки сильного задимлення та високої ймовірності пожежі, буде увімкнено оприскувач, який повинен буде загасити її.

Smartphone_2

Physical Config **Desktop** Programming Attributes

IoT Monitor X

IoT Server - Device Conditions Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Alarm	Smoke Detector Level >= 5	Set Siren On to true
Edit Remove	Yes	Fire Sprinkler	Smoke Detector Level >= 5.4	Set Fire Sprinkler Status to true
Edit Remove	Yes	Alarm Off	Smoke Detector Level <= 1	Set Siren On to false
Edit Remove	Yes	Sprinkler off	Smoke Detector Level <= 1	Set Fire Sprinkler Status to false
Edit Remove	Yes	Garage Door OFF	Siren On is true	Set Garage Door On to true
Edit Remove	Yes	Garage Door ON	Siren On is false	Set Garage Door On to false

☐ Top

Рисунок 2.6 – Автоматизація системи безпеки

Таким чином, у зоні гаражу запроваджена система, що дозволить уникнути задимлення приміщення, отруєння газами, чи навіть пожежі, що забезпечує додаткової безпеки резиденту розумного будинку.

Пристрої у цій зоні також під'єднані до домашнього шлюзу, що також дозволяє дистанційний моніторинг, або керування ними. Так, наприклад, можна керувати ворітьми гаражу зі свого смартфона, що знову ж таки спрощує життя резидента розумного будинку.

Зона №3

Третьою зоною є зона саду(вулиці). У цій зоні розташовані прилади, незалежні від усієї системи. Це реалізовано завдяки окремому мікроконтролеру SBC0. На ньому зав'язані сенсори, зроблено це на прикладі датчиків руху та вітру.

Завдяки таким мікроконтролерам можна будувати окремі підсистеми, що не будуть пов'язані із основною системою розумного будинку, що є дуже корисним та практичним у певному ряді потреб.

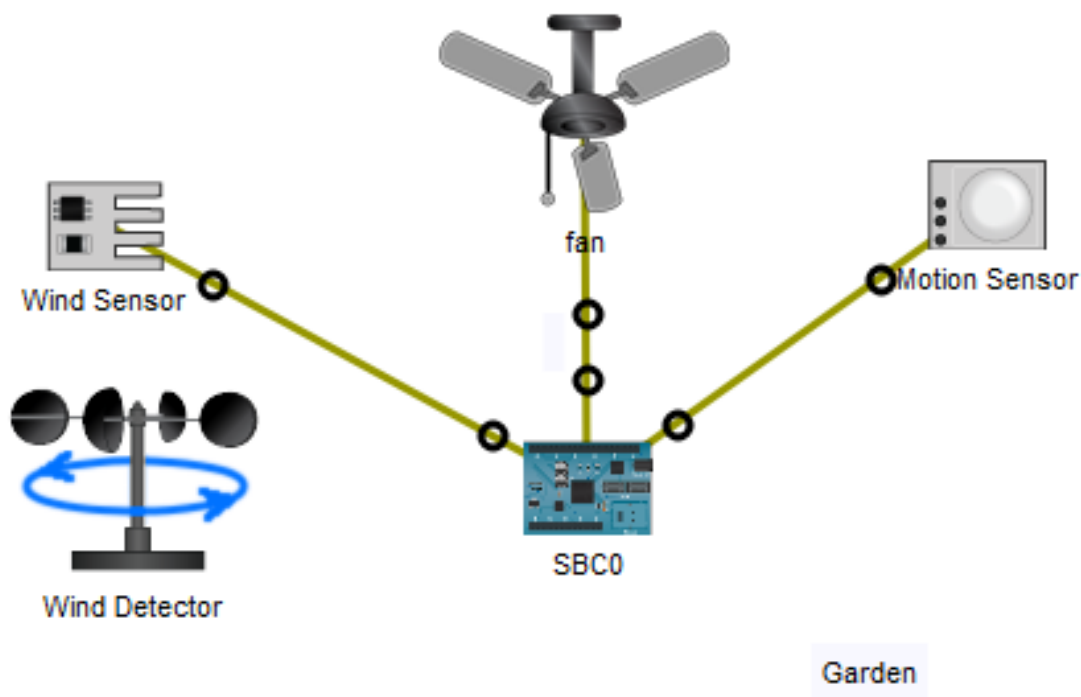


Рисунок 2.7 – Вигляд дворової зони

Використання у системі мікроконтролера дозволяє збільшити гнучкість налаштування пристроїв. За окремої потреби це є дуже корисним. У мікроконтролеру, що використовується в системі зони двору налаштована нестандартна прошивка, що виконує мінімальні функції для демонстрації принципу роботи мікроконтролерів. Інколи ці контроллери використовуються для збільшення точності даних, прискорення швидкодії, процесу кодування чи декодування, встановлення таймерів, виготовлення розумних реле-перемикачів.

Найчастіше вони використовуються у парі з побутовими пристроями. Так, наприклад, можна самостійно зробити розумну кавоварку, чи розумний чайник, використовуючи усього один додатковий мікроконтролер.

Іншим способом використання є пришвидшення швидкодії. Додаючи мікроконтролер до системи, ми значно збільшуємо кількість обчислювальних потужностей у цій системі, що приводить до зменшення затримок у обрахунках, та збільшенні швидкодії.

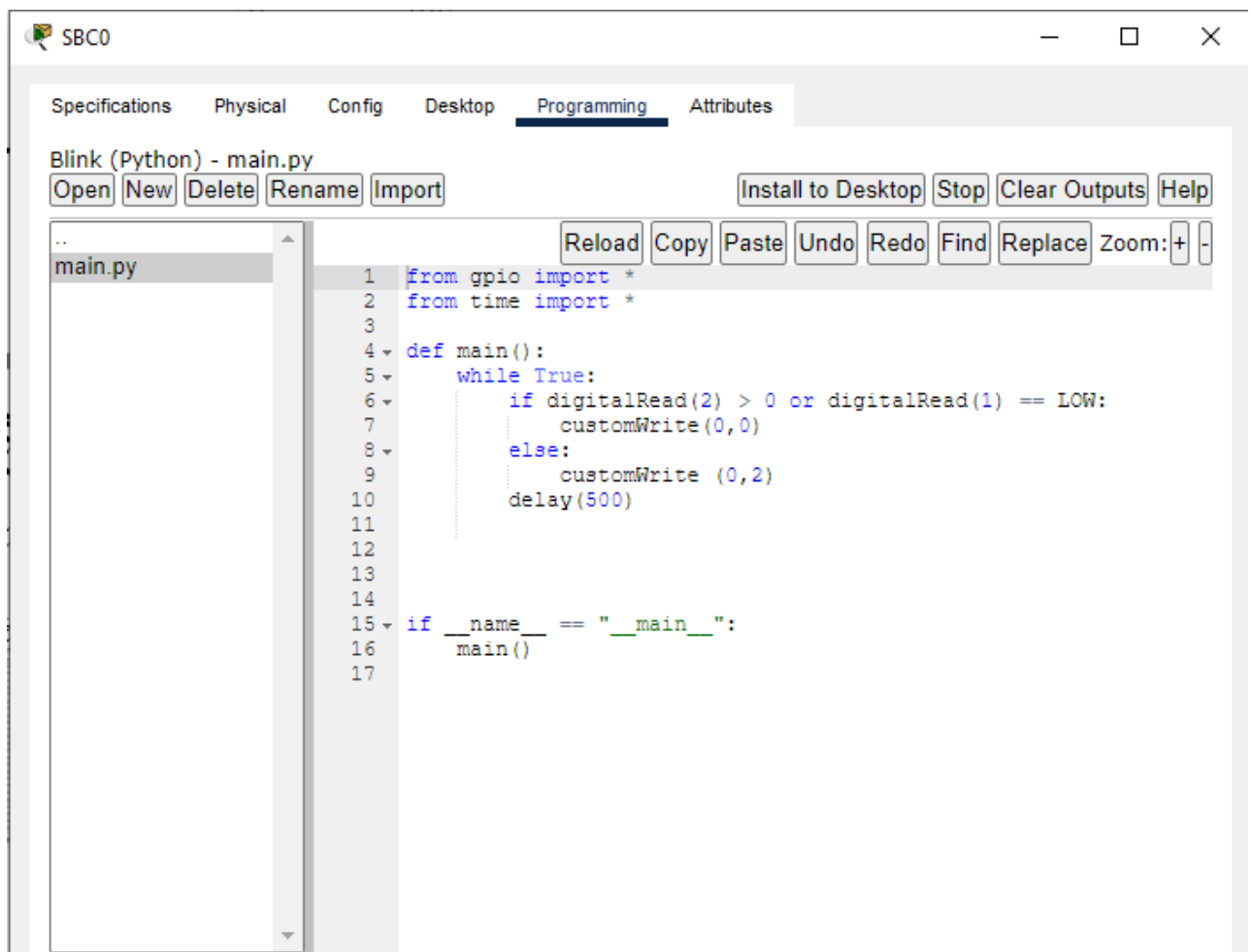


Рисунок 2.8 – Приклад прошивки контроллера

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

2.2 Складання схеми у середовищі Cisco Packet Tracer

Підключення системи до шлюзу

Секція пристроїв розумного будинку трохи відділена від мережі будинку. Якщо оглянути схему, можна побачити, що вся система розумного будинку в основному підключена до домашнього шлюзу. Завдяки ньому відбуваються усі процеси керування розумним будинком.

Підключивши до шлюзу смартфон, отримаємо віддалене керування усіма пристроями та функціоналом системи розумного будинку. Саме через шлюз запити транслюються з смартфона до кінцевих пристроїв. Він виступає маршрутизатором, крім того, маючи у собі певне програмне забезпечення, що дозволяє створювати автоматизації, які полегшують життя резиденту розумного будинку, або підвищують рівень його безпеки.

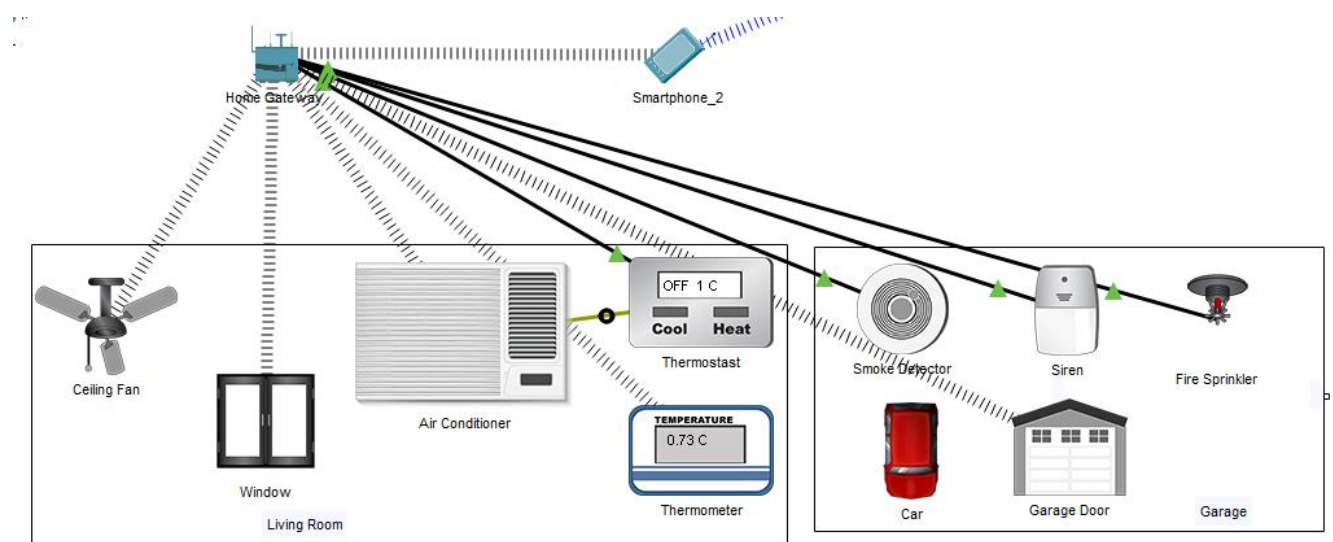


Рисунок 2.9 – Підключення пристроїв розумного дому до шлюзу

Шлюз об'єднує в собі усі елементи системи, дані про них, а також пов'язує їх між собою і відправляє сигнал назовні. В деяких випадках можна придбати окремо шлюз, та доповнити його підключенням до нього інших розумних приладів. В інших випадках, купуючи комплексні набори системи розумного дому, шлюз обов'язково повинен бути до них включений.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Домашня мережа

Окрім елементів розумного будинку, у схемі також присутні і звичайні мережеві пристрої. Мережа складається з чотирьох комп'ютерів, точки доступу, двох смартфонів, комутатора, перетворювача сигналу та IP телефону.

Локальна мережа дому розроблена з використанням протоколу DHCP, що також полегшує життя резиденту дому, дозволяючи забути йому про ручну конфігурацію IP налаштувань пристроїв.

Для локальної мережі дому було використано IP-мережу 192.168.1.0 та маску 255.255.255.0. Крім того, у мережі використовується точка віддаленого доступу, що дозволяє підключатись до мережі за допомогою Wi-Fi.

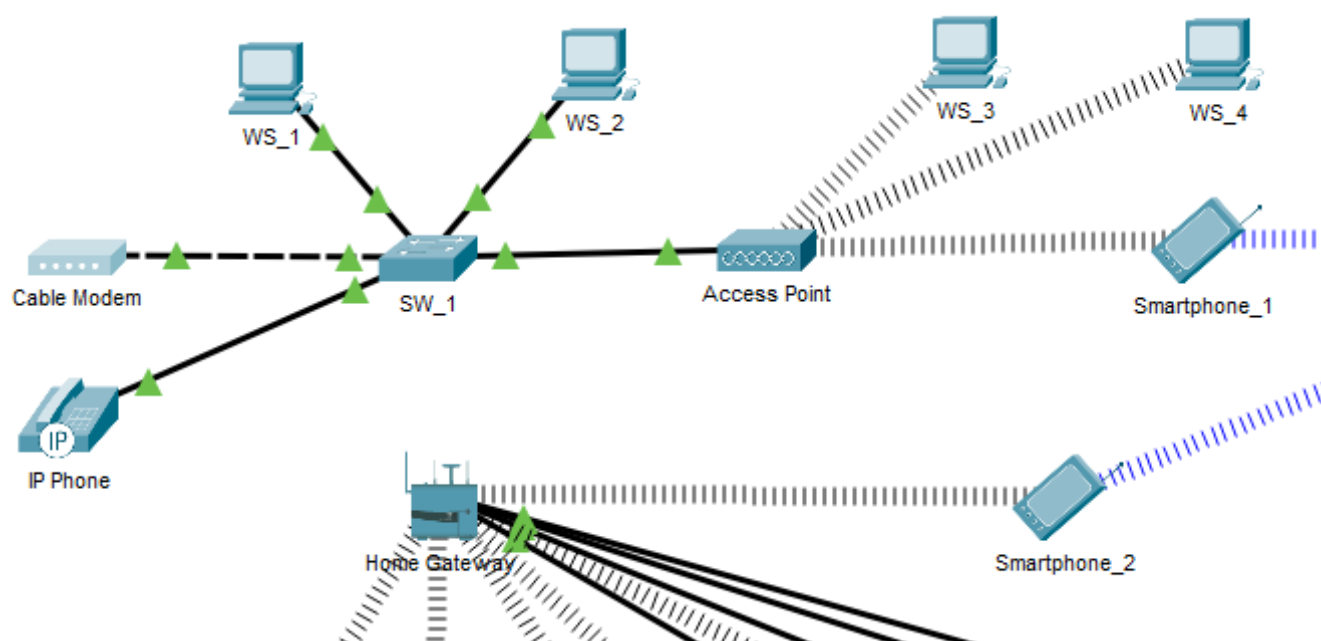


Рисунок 2.10 – Схема мережевих та кінцевих пристроїв системи

Таблиця 2.1 – Параметри IP-адресації мережі

Мережа/ Пристрій	Інтерфейс/Мере жний адаптер/Шлюз	IP-адреса	Маска	/xx
WS_1	Інтерфейс E0/1	192.168.1.2	255.255.255.0	/24
WS_2	Інтерфейс E0/1	192.168.1.3	255.255.255.0	/24
WS_3	Wireless	192.168.1.11	255.255.255.0	/24
WS_4	Wireless	192.168.1.12	255.255.255.0	/24

Продовження таблиці 2.1 – Параметри IP-адресації мережі

Smartphone_1	3G/4G CELL	169.254.67.8	255.255.0.0	/16
Smartphone_2	3G/4G CELL	192.168.5.100	255.255.0.0	/16
	Wireless	192.168.25.109	255.255.255.0	/24
Home Gateway	Wireless	192.168.25.1	255.255.255.0	/24
Бездротові SMART пристрої	Wireless	DHCP	255.255.255.0	/24
Дротові SMART пристрої	FE0	DHCP	255.255.255.0	/24

В цьому розділі було побудовано схему розумного будинку у середовищі Cisco Packet Tracer. Розглянуто основні зони системи, та особливості їх будови, створено автоматизації процесів розумного будинку та налаштовано параметри адресації у мережі. Було налаштовано три зони пристроїв розумного будинку, додавно декілька сценаріїв виконання на домашньому шлюзі, та запрограмовано нестандартну прошивку на контролері третьої зони.

З розділу також можемо зробити висновок, що існує великий асортимент смарт пристроїв, що дозволяє побудувати систему розумного дому майже під будь-які потреби, від збільшення комфорту в домі до додаткових рішень у системах безпеки.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ МЕРЕЖІ РОЗУМНОГО БУДИНКУ

3.1 Перевірка зв'язку у мережі

Після успішної побудови мережі у середовищі Cisco Packet Tracer, необхідно перевірити її працездатність. Окрім перевірки зв'язку між мережевими пристроями, необхідно також перевірити працездатність пристроїв розумного дому.

Перевірка мережевих пристроїв

Почнемо перевірку працездатності з перевірки зв'язку. Для цього виконаємо команду ping на домашньому комп'ютері WS_1, та спробуємо отримати відповідь від інших елементів мережі.

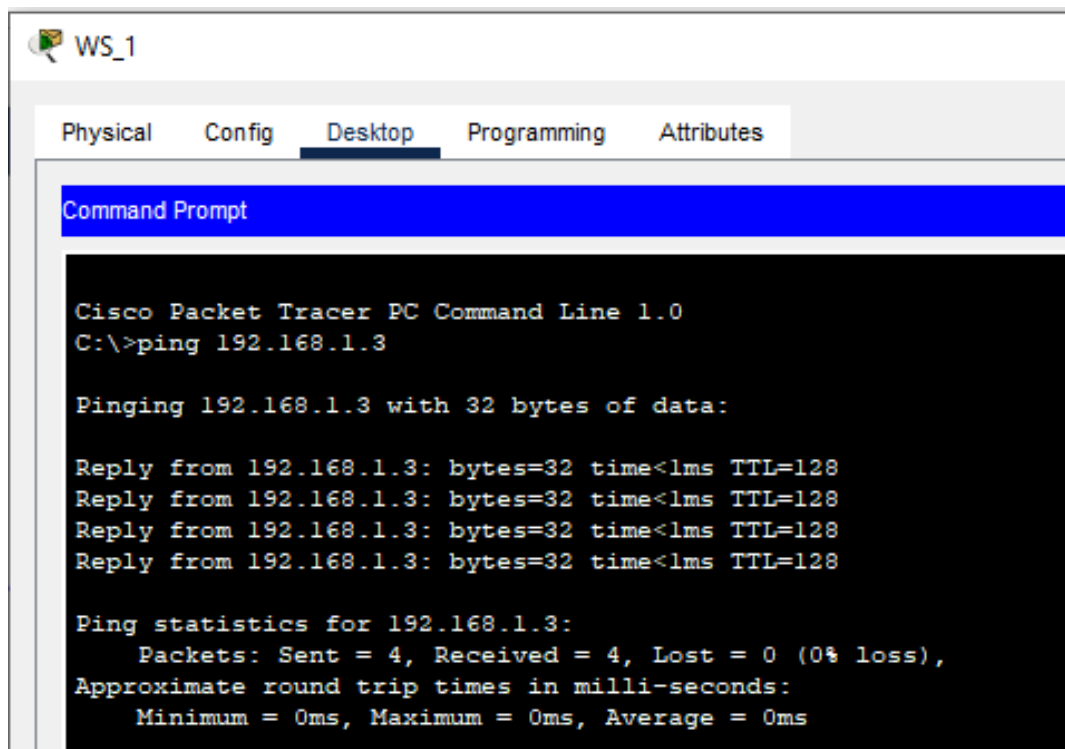


Рисунок 2.1 – Перевірка зв'язку WS_1 з локально підключеним WS_2

Перевіримо також зв'язок із робочими станціями, що підключені до мережі бездротовим методом через точку доступу.

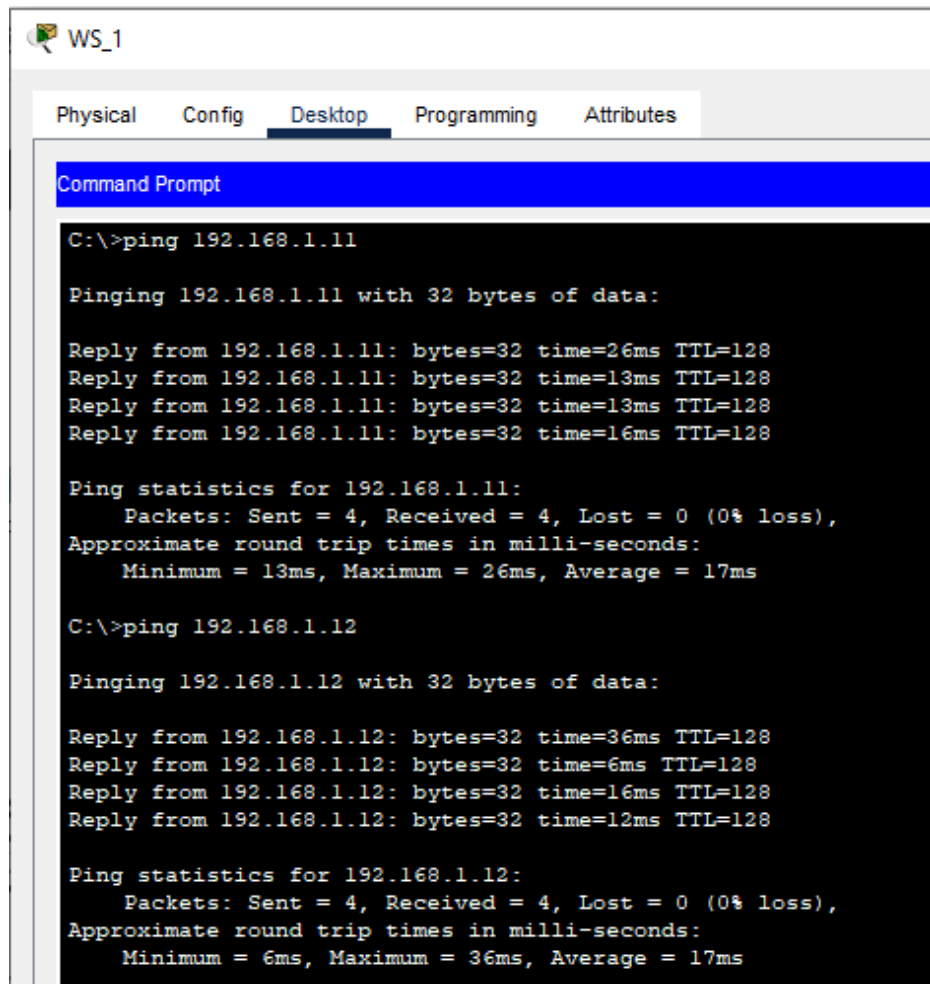


Рисунок 2.2 – Перевірка зв'язку між WS_1 та WS_3,WS_4

Після цього необхідно перевірити зв'язок у підмережі розумного дому.

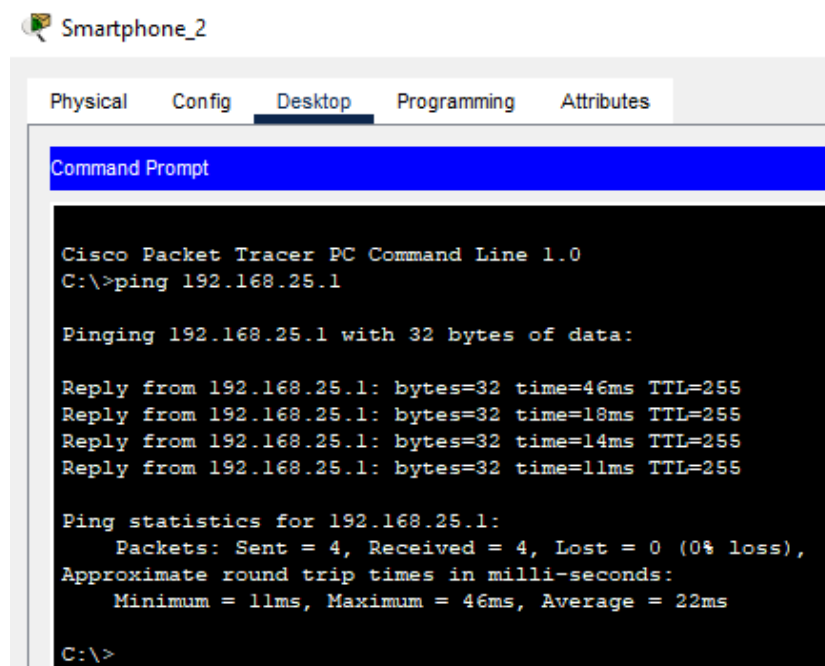


Рисунок 2.3 – Перевірка зв'язку між Smartphone_2 та шлюзом розумного дому

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Також необхідно перевірити комунікацію смартфона та розумних пристроїв.

```

Smartphone_2
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Pinging 192.168.25.102 with 32 bytes of data:

Reply from 192.168.25.102: bytes=32 time=68ms TTL=255
Reply from 192.168.25.102: bytes=32 time=32ms TTL=255

Ping statistics for 192.168.25.102:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 68ms, Average = 50ms

Control-C
^C
C:\>ping 192.168.25.104

Pinging 192.168.25.104 with 32 bytes of data:

Reply from 192.168.25.104: bytes=32 time=39ms TTL=255
Reply from 192.168.25.104: bytes=32 time=15ms TTL=255

Ping statistics for 192.168.25.104:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 39ms, Average = 27ms

Control-C
^C
C:\>ping 192.168.25.105

Pinging 192.168.25.105 with 32 bytes of data:

Reply from 192.168.25.105: bytes=32 time=28ms TTL=255
Reply from 192.168.25.105: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.25.105:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 28ms, Average = 20ms
  
```

Рисунок 2.4 – Перевірка зв’язку Smartphone_2 та SMART пристроїв

3.2 Перевірка працездатності SMART пристроїв та їх автоматизації

Так як у мережі було використано елементи розумного дому та їх автоматизацію, необхідно перевірити правильність їх функціонування, та точність відпрацьовування автоматизацій. Для цього треба проявити активність датчиків. У середовищі Cisco Packet Tracer це можна зробити за допомогою кліку лівої кнопки миші з натиснутою клавішею ALT.

Для початку перевіримо відпрацювання сценарію керування кліматом у зоні жилого приміщення. У сценарій було внесення правило, що вентилятор повинен увімкнутись та відкритись вікно при температурі більше або рівній 12 градусам за Цельсієм.

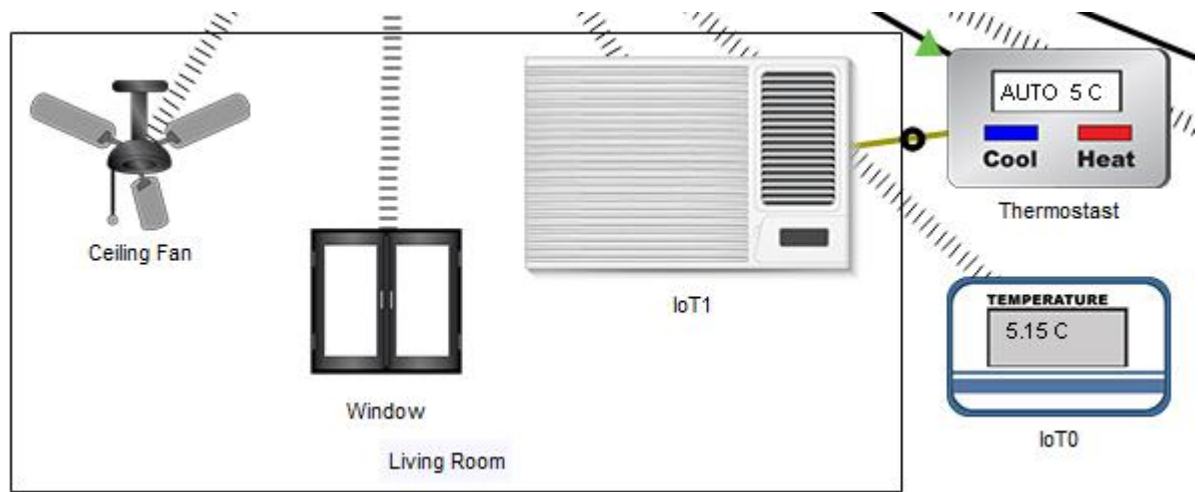


Рисунок 2.5 – Вимкнений вентилятор та закрите вікно при температурі 5 градусів за Цельсієм

Дочекаємось зміни клімату, та перевіримо точність виконання сценарію.

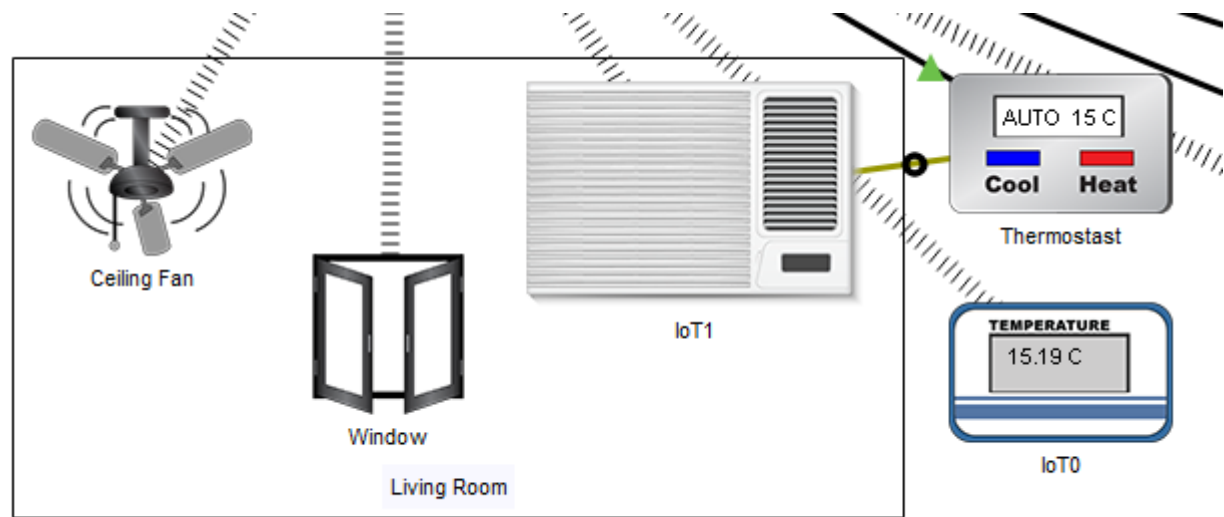


Рисунок 2.6 – При підвищенні температури увімкнувся вентилятор та відчинилось вікно у кімнаті

Далі необхідно перевірити, чи увімкнеться кондиціонер при переведенні термостату у положення COOL.



Рисунок 2.7 – Кондиціонер вимкнений

Переведемо термостат у положення COOL, та перевіримо правильність виконання сценарію. Включення кондиціонеру буде сигналізувати червоний індикатор на його панелі.

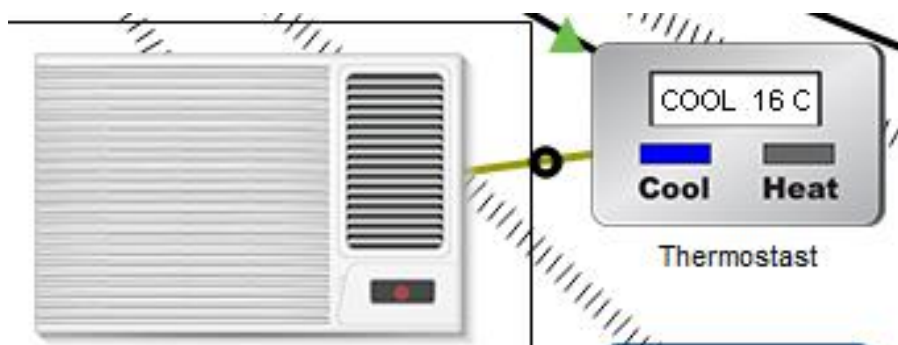


Рисунок 2.8 – Кондиціонер увімкнувся

Перейдемо до зони гаражу. Там запрограмовано відкриття воріт та увімкнення сигналізації зі спринклером коли датчик побачить задимлення.

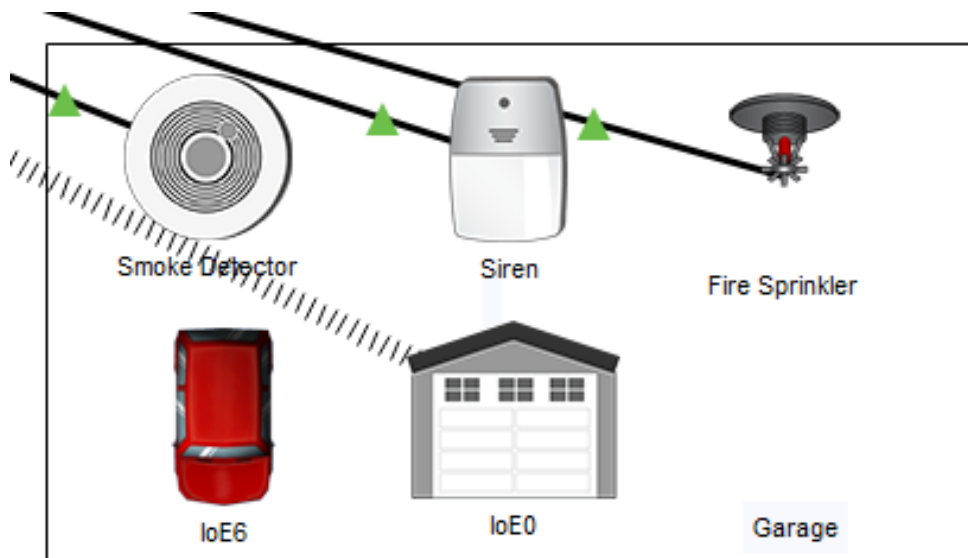


Рисунок 2.9 – Зона гаражу у стані спокою

За допомогою автомобіля зімітуємо задимлення.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

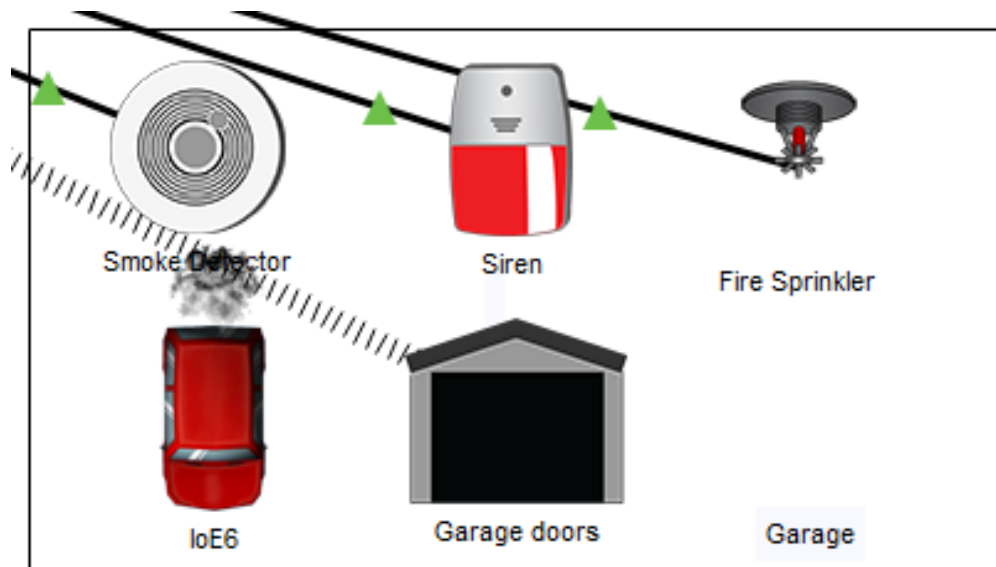


Рисунок 2.10 – Результат відпрацювання сценарію

Як можемо побачити на рисунку 2.10, сценарій відпрацював успішно, перевіримо дали, після тривалого задимлення повинен увімкнутись спринклер.

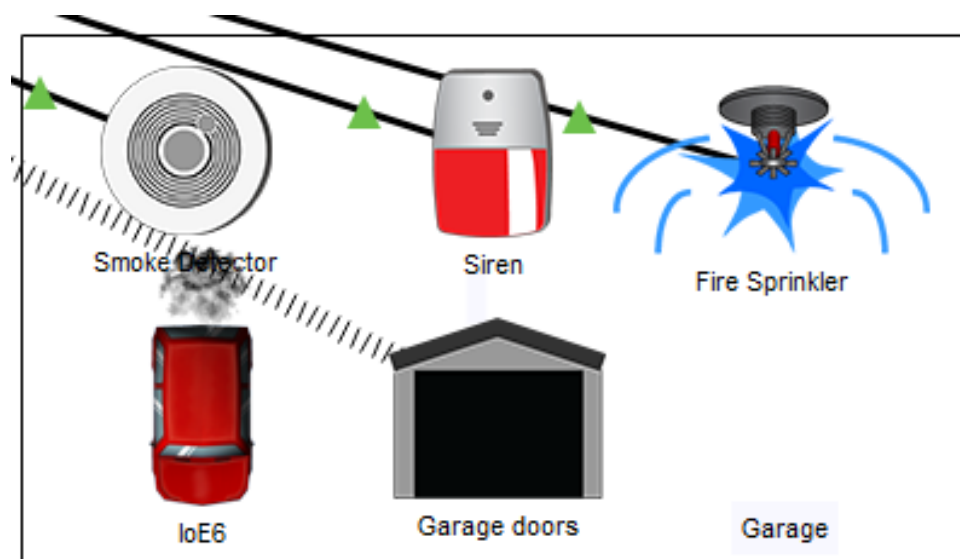


Рисунок 2.11 – Увімкнений спринклер

3.3 Перевірка вразливостей системи

Так як функціонал Cisco Packet Tracer обмежений у плані проведення атак, було використано віртуальну машину для емуляції проведення атаки. Жертвою атаки став мережевий пристрій, що емулює SMART пристрій для вимірювання показників життєвої діяльності. Варто зауважити, що емульований пристрій, скинутий до заводський налаштувань, та без підключених параметрів безпеки. Атаку було вирішено проводити за допомогою віртуальної машини з ОС Kali Linux.

		Вексей О.І.			KIK.KP.B – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Варто також зауважити, що за мережу взято звичайну мережу, без додаткових засобів безпеки та захисту від атак. З атакованого пристрою було знято паролі, та на пристрої було вибрано параметр довіри до мережі. Тому таке дослідження атаки можна вважати неточним.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.202 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::2fce:3748:23a9:4dfb prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:e0:b0:10 txqueuelen 1000 (Ethernet)
    RX packets 23051 bytes 33000487 (31.4 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4006 bytes 270076 (263.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 176 bytes 14796 (14.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 176 bytes 14796 (14.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рисунок 3.1 – Параметри IP-адресації віртуальної машини Kali Linux

Можемо побачити, що мережею є 192.168.43.0/24, використаємо команду nmap, щоб перевірити підключених до мережі клієнтів.

```
root@kali:~# sudo nmap -sn 192.168.43.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-17 10:38 UTC
Nmap scan report for 192.168.43.1
Host is up (0.13s latency).
MAC Address: 0A:C5:E1:B7:C2:32 (Unknown)
Nmap scan report for LAPTOP-V1PLE6BE (192.168.43.165)
Host is up (0.073s latency).
MAC Address: F8:28:19:C6:D3:45 (Liteon Technology)
Nmap scan report for HALMSTA-QVHVBH8P (192.168.43.172)
Host is up (0.00025s latency).
MAC Address: E8:4E:06:32:17:A9 (Edup International (hk))
Nmap scan report for 192.168.43.179
Host is up (0.039s latency).
MAC Address: 00:1E:C0:22:47:FB (Microchip Technology)
Nmap scan report for kali (192.168.43.202)
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 5.53 seconds
```

Рисунок 3.2 – Виконання команди nmap

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

З рисунку 3.2 можемо зробити висновок, що потрібний нам пристрій знаходиться з тегом Microchip Technology. Для ураження цілі було вирішено виконати атаку SYN-flood, для чого потрібно скористатись засобом Metasploit.

```
msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > set RHOST 192.168.43.179
RHOST => 192.168.43.179
msf5 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT => 80
msf5 auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 192.168.43.179:80...
```

Рисунок 3.3 – Процес проведення атаки



Рисунок 3.4 – Результат порушення роботи додатку на пристрої

На рисунку 3.4 чітко видно, що пристрій отримав порушення працездатності, це видно по графіку серцебиття та дихання, що зображені синім та зеленим кольором.

У цьому розділі було проведено перевірку працездатності системи розумного дому та смарт пристроїв. Сценарії автоматизації відпрацювали так як потрібно, мережу було побудовано правильно. Під час атаки на емульований смарт пристрій можна було побачити перешкоди у роботі, але ці дані не є досить точними через доволі широкий спектр факторів.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

ВИСНОВКИ

В даній кваліфікаційній роботі було проведено дослід з побудовою, перевіркою працездатності та спробою атаки системи розумного дому.

Обґрунтування актуальності теми допомогло оцінити важливість розумних будинків у сучасному світі.

Після проведення актуальності та важливості розумних будинків, було спроектовано та побудовано мережу, що імітує процеси розумного будинку.

Для вирішення задачі побудови мережі було обрано програмне забезпечення Cisco Packet Tracer, та віртуальні машини для емуляції атаки на смарт пристрій. Саме використання цього ПЗ дозволило відтворити систему розумного будинку, та оцінити її переваги та недоліки.

Після ознайомлення з програмним середовищем, було побудовано мережу, налаштовано пристрої, створено автоматизації, що дозволило детальніше вивчити систему розумного будинку.

Було проведено емуляцію атаки на смарт пристрій за допомогою віртуальної машини з ОС Kali Linux. Результати атаки виявились досить спірними через низку факторів, які додали до тестування ймовірностей.

Використання розумних будинків не тільки робить наше життя легшим, але й додає в нього безпечності. З сучасним темпом розвитку технологій, розумні будинки мають величезний потенціал, вони будуть ставати ще безпечнішими, та приносити у життя ще більше комфорту.

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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-potrбно-znati-pro-sistemu-rozumnij-dm/5/>
2. 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/>
3. 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.
4. 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
5. Лутольф Л. "Smart Home concept and the integration of energy meters into a home based system", Сьома Інтернаціональна конференція для Об'єднаних Систем Розумних Будинків, 1992. – С. 17-19
6. Wi-Fi Alliance, "Wi-Fi Alliance" [Електронний ресурс]. – Режим доступу до ресурсу: <http://www.wi-fi.org/>
7. Гудвінс Р. "Next-generation 802.11ax Wi-Fi: Dense, Fast, Delayed" [Електронний ресурс]. – Режим доступу до ресурсу: <https://www.zdnet.com/article/next-generation-802-11-ax-wi-fi-dense-fast-delayed/>

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

8. Національна Агенція Безпеки, "Cyber Security Report - WPA3 Will Enhance Wi-Fi Security", Національна Агенція Безпеки, 2018.
9. Розумний дім. [Електронне джерело]. Режим доступу: http://www.directinfo.net/index.php?option=com_content&view=article&id=139%3A2010-07-06-13-57-09&catid=1%3A2008-11-27-09-05-45&Itemid=84
10. 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.
11. 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/>
12. Granzer W. P. Security in Building Automation Systems / Wolfgang Praus Granzer. Munich: Appress, 2018. – 578 с.
13. Розумне освітлення [Електронний ресурс]. – Режим доступу до ресурсу: <https://milight.com.ua/ua/umnoe-osveshchenie/>
14. Mann William C. The state of the science/Smart technology for aging, disability and independence. — John Wiley and Sons, 2005.
15. Cisco , "IEEE 802.11ax: The Sixth Generation of Wi-Fi", Cisco, 2018
16. Microchip Technology Inc, "Microchip Technology", Microchip Technology Inc, 2019. [Електронний ресурс]. Режим доступу до ресурсу: <https://www.microchip.com>
17. Software Engineering Institute, "TCP SYN Flooding and IP Spoofing Attacks", Carnegie-Mellon University, 1996.
18. Rapid 7, "Metasploit Penetration Testing Software & Pentesting Security," Rapid 7, [Електронний ресурс]. – Режим доступу до ресурсу: <https://www.metasploit.com>
19. Thread Group, "Thread - Press Releases", Thread Group, 15 July 2014. [Електронний ресурс]. – Режим доступу до ресурсу:

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

<https://www.threadgroup.org/news-events/press-releases/ID/20/Introducing-Thread-A-NewWireless-Networking-Protocol-for-the-Home>

20. Thread Group, "Security & Commissioning", Thread Group, 2015.
21. Power Load Event Detection and Classification Based on Edge Symbol Analysis and Support Vector Machine [Електронний ресурс]. – Режим доступу до ресурсу: <https://www.hindawi.com/journals/acisc/2012/742461/>
22. An Overview of Home Automation Systems [Електронний ресурс]. – Режим доступу до ресурсу: <https://ieeexplore.ieee.org/document/7791223/>

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

ДОДАТКИ

		Вексей О.І.			КІК.КР.Б – 125 – 04 – ПЗ	Арк.
		Покотило О.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

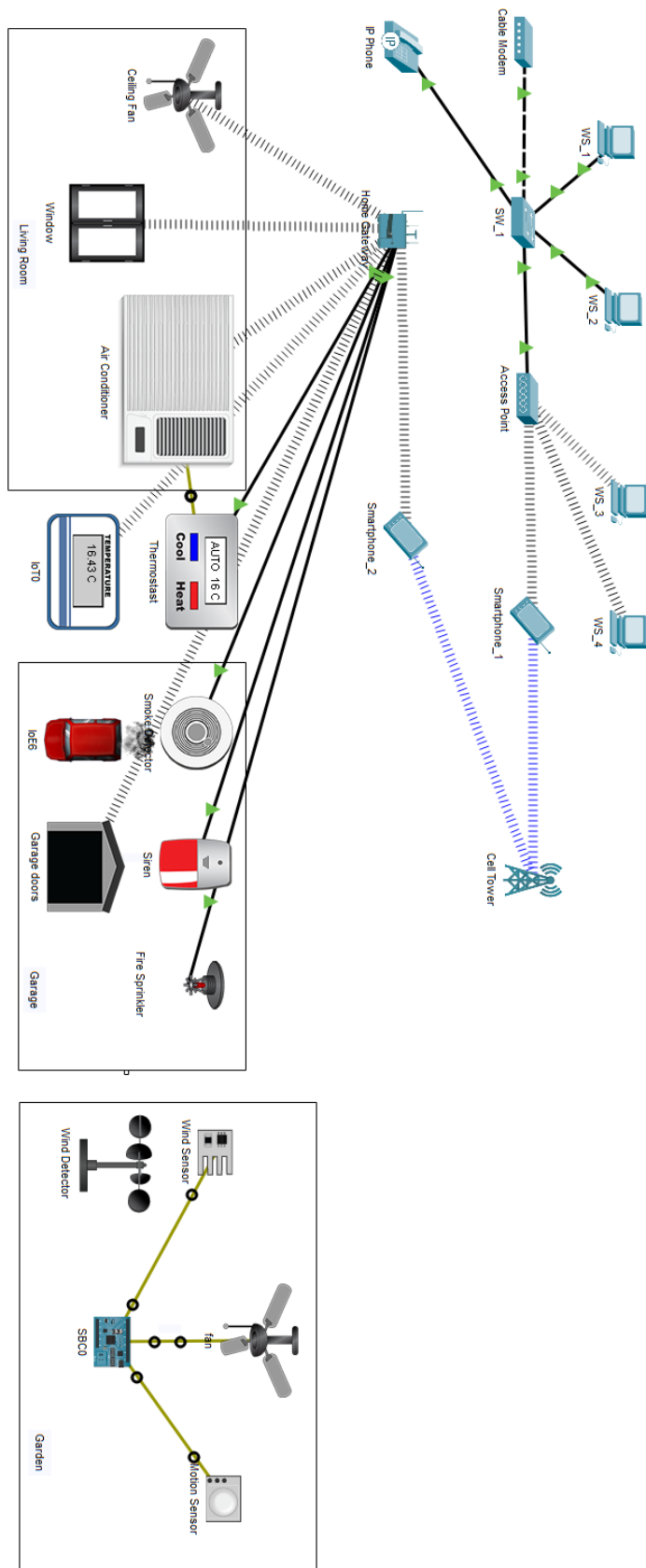


Рисунок А.1 – Топологічна схема мережі