

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 захищеної IoT-системи котеджу»

Виконав студент 4-го курсу, групи ЗКБ-18
спеціальності 125 «Кібербезпека»

 Пулеко К. І.

Керівник, професор кафедри КІ та КБ,

д.т.н., доцент

 Воротніков В. В.

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

 Россінський Ю.М.

Житомир 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри комп'ютерної
інженерії та кібербезпеки

 Сфіменко А. А.

« 01 » березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

студента групи ЗКБ-18

Пулека Костянтина Ігоровича

Тема роботи: Проект захищеної IoT-системи котеджу

затверджена Наказом по університету від « 01 » березня 2022 р. № 128с

Термін здачі студентом закінченої роботи – 10 червня 2022 р.

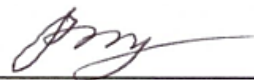
Вихідні дані для роботи:

план котеджа

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Керівник



Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.22	виконано
2	Пошук, огляд та аналіз літературних джерел	14.03.22	виконано
3	Аналіз предметної області та обґрунтування актуальності теми роботи	23.03.22	виконано
4	Розробка проекту захищеної IoT-системи котеджу	30.03.22	виконано
5	Моделювання ризиків для IoT-системи котеджу та розробка рекомендацій по їх усуненню	18.04.22	виконано
6	Перевірка працездатності та ефективності прийнятих рішень	15.05.22	виконано
7	Подача чернетки керівнику для перевірки	26.05.22	виконано
8	Доопрацювання роботи та перевірка керівником	30.05.22	виконано
9	Проведення попереднього захисту	10.06.22	виконано
10	Отримання відгуку керівника	13.06.22	виконано
11	Допуск завідувача кафедри	17.06.22	виконано
12	Подання роботи на рецензування	20.06.22	виконано
13	Захист		

Студент  Пулеко К. І.

Керівник  Воротніков В. В.

РЕФЕРАТ

Випускна кваліфікаційна робота бакалавра направлена на рішення актуального завдання по розробці проекту захищеної IoT-системи котеджу.

Метою роботи є підвищення рівня безпеки IoT-системи на прикладі розробки «розумного будинку» для конкретно заданого котеджу.

Об'єктом дослідження є процес побудови захищених систем IoT.

Предметом дослідження є методи моделювання ризиків, стратегії, заходи та засоби забезпечення кібербезпеки систем IoT.

Наукова новизна дослідження полягає в удосконаленні стратегій кібербезпеки для IoT систем за рахунок поєднання їх з хмарними технологіями та моделюванням ризиків.

Практична значимість роботи. Розроблені в роботі стратегії безпеки при розробці та реалізації IoT-системи котеджу, методики моделювання ризиків для IoT-системи та рекомендацій по їх усуненню можуть бути з успіхом застосовані при розробці інших IoT проектів.

Пояснювальна записка до випускної бакалаврської роботи містить 80 сторінок, 20 рисунків, 4 таблиці 1 додаток. Перелік посилань містить 23 літературних джерел.

КЛЮЧОВІ СЛОВА: Інтернет речей, IoT, захист інформації, кібербезпека, модель ризиків, AZURE, STRIDE, стратегії розробки.

					КБ.КР.Б – 125 – 21 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної IoT-системи котеджу Пояснювальна записка	Літ.	Арк.	Акрушіє	
Розроб.		Пулеко К. І.		20.06.22					
Перевір.		Вороніков В. В.		20.06.22			5	85	
Реценз.		Росієнко В. В.		20.06.22		ФІКТ, гр. ЗКБ-18			
Н. Контр.									
Затверд.		Єфіменко А. А.		20.06.22					

ABSTRACT

Bachelor's degree qualification work is focused on solving an important problem of developing the project of secured IoT system in the cottage.

The purpose of work is to increase the security level of the IoT system on the basis of "smart home" development for specific cottage.

The object of research is the process of creating a secure IoT system.

The subject of the research is risk modeling methods, strategies, measures and tools of cybersecurity of IoT systems.

The scientific novelty of research is improving cybersecurity strategies for IoT systems by combining them with cloud technologies and risk modeling.

Practical relevance of the work. In the research work were developed the security strategies, risk modeling methods for IoT systems and recommendations for their elimination which can be successfully applied in the other IoT projects development.

The explanatory note to the bachelor's thesis contains 80 pages, 24 figures, 4 tables and 1 appendix. The list of references contains 23 literature sources.

KEY WORDS: Internet of things, IoT, information security, cybersecurity, risk model, AZURE, STRIDE, strategies of development.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	8
ВСТУП	9
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ	11
1.1. Обґрунтування актуальності теми роботи	11
1.2. Аналіз існуючих проєктів IoT-систем	15
1.3. Аналіз проблем безпеки IoT-систем «розумних будинків»	24
1.4. Аналіз особливостей та умов рішення поставленого завдання	32
1.5. Постановка завдання	33
Висновки по 1 розділу	35
РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ ІОТ-СИСТЕМИ КОТЕДЖУ	36
2.1. Розробка структурної схеми IoT-системи котеджу	36
2.2. Модель ризиків IoT системи котеджу	42
2.3. Розробка функціональної схеми IoT-системи котеджу	52
2.4. Моделювання ризиків для IoT-системи котеджу та розробка рекомендацій по їх усуненню.....	53
Висновки по 2 розділу	63
РОЗДІЛ 3. ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ТА ЕФЕКТИВНОСТІ ПРИЙНЯТИХ РІШЕНЬ	64
3.1. Розробка моделі IoT-системи котеджу за допомогою Cisco Packet Tracer	64
3.2. Дослідження моделі IoT-системи котеджу за допомогою Cisco Packet Tracer	69
3.3. Рекомендації щодо вдосконалення стратегії безпеки при розробці та реалізації IoT-системи котеджу	73
Висновки по 3 розділу	77
ВИСНОВКИ	78
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	80
ДОДАТКИ	83

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DHCP (англ. Dynamic Host Configuration Protocol) — протокол динамічної конфігурації вузла;

DNS – Domain Name System;

IoT – Інтернет речей (Internet of Things) ;

MCU – модель мікроконтролера в Cisco Packet Tracer;

RFID – Radio-Frequency IDentification;

SBC – модель мікроконтролера в Cisco Packet Tracer;

SDL –Security Development Lifecycle, життєвий цикл розробки безпеки;

STRIDE – модель загроз;

Z-Wave – Бездротовий стандарт автоматизації;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В наш час все більшої популярності набуває концепція Інтернету речей (англ. Internet of Things, IoT). Згідно з найбільш поширеним формулюванням [1], Інтернет речей - концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем, яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій і операцій необхідність участі людини [2].

Одним із напрямків практичного розвитку концепції Internet of Things (IoT, Інтернет речей) є розробка «розумних будинків» (Smart Home). Сучасний «розумний будинок» дозволяє здійснювати управління безпекою, системами клімат-контролю, освітлення, розумними побутовими приладами та лічильниками. По суті «розумний будинок» - це комплексна система, яка працює як єдине ціле для досягнення повного комфорту проживання в будинку. Тому на сьогоднішній день багато компаній надають свої пропозиції для розвитку цього напрямку.

Аналіз сучасного стану розробок «розумних будинків» показав, що на сьогодні ринок пропонує велику кількість пристроїв та систем IoT, що можуть бути використані для рішення завдання. Однак, з того ж аналізу слідує, що питанням забезпечення безпеки IoT систем приділяється значно менше уваги. Разом з тим слід відмітити, що системи IoT мають ряд вразливостей і тому при проектуванні необхідно передбачити заходи та засоби забезпечення кібербезпеки під час функціонування IoT системи котеджу. Тобто, тема роботи, що направлена на розробку проекту захищеної IoT-системи котеджу, є **актуальною**.

Метою дослідження є підвищення рівня безпеки IoT-системи на прикладі розробки «розумного будинку» для конкретно заданого котеджу.

Для досягнення цієї мети в роботі виконані такі завдання:

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

- Обґрунтування актуальності теми роботи та аналіз існуючих проектів IoT-систем.
- Аналіз проблем безпеки IoT-систем «розумних будинків».
- Розробка моделі ризиків, структурної та функціональної схеми IoT-системи котеджу.
- Моделювання ризиків для IoT-системи котеджу та розробка рекомендацій по їх усуненню.
- Перевірка працездатності та ефективності прийнятих рішень шляхом імітаційного моделювання.
- Розробка рекомендацій щодо вдосконалення стратегії безпеки при розробці та реалізації IoT-системи котеджу.

Об'єктом дослідження є процес побудови захищених систем IoT.

Предметом дослідження є методи моделювання ризиків, стратегії, заходи та засоби забезпечення кібербезпеки систем IoT.

Наукова новизна дослідження полягає в удосконаленні стратегій кібербезпеки для IoT систем за рахунок поєднання їх з хмарними технологіями та моделюванням ризиків.

Практична значимість роботи. Розроблені в роботі стратегії безпеки при розробці та реалізації IoT-системи котеджу, методики моделювання ризиків для IoT-системи та рекомендацій по їх усуненню можуть бути з успіхом застосовані при розробці інших IoT проектів.

Методи досліджень. В даній роботі були використані методи: аналізу, моделювання ризиків, імітаційного моделювання.

Публікації. За темою роботи було опубліковано 2 тез доповідей:

Особливості застосування сертифікації X.509 для гарантування безпеки пристроїв Інтернету речей у хмарному середовищі AZURE (2021) [20].

Аналіз напрямків застосування штучного інтелекту в задачах кібербезпеки (2021) [21].

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		10

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ

1.1. Обґрунтування актуальності теми роботи

Важко знайти в наш час людину, нічого не чула про Internet of Things (IoT, Інтернет речей). Згідно з найбільш поширеним формулюванням, Інтернет речей (англ. Internet of Things, IoT) - концепція обчислювальної мережі фізичних предметів («речей»), оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем [1], яка розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси, що виключає з частини дій і операцій необхідність участі людини [2]. Тобто, Internet of things – це підключені до Інтернету пристрої, між якими відбувається обмін даними. Для обробки та передачі інформації IoT обладнання використовує датчики та програмне забезпечення.

Експерти стверджують, що Інтернет речей є однією з найперспективніших технологій останніх років, що вже сьогодні фактично створює сотні нових продуктів і призводить до появи нових компаній на ринку, які диктують свої умови ІТ-гігантам. Ви можете не помічати, але ви самі, ваші друзі чи колеги вже не перший рік користуються такими пристроями кожен день. Більше того, у чималій кількості українських домівок вже встановлені системи "розумного будинку", в які інтегровані десятки датчиків.

Основною концепцією IoT є можливість підключення всіляких об'єктів (речей), які людина може використовувати в повсякденному житті, наприклад, холодильник, кондиціонер, автомобіль, велосипед і навіть кросівки. Всі ці об'єкти (речі) повинні бути оснащені вбудованими датчиками або сенсорами, які мають можливість обробляти інформацію, що надходить з навколишнього середовища, обмінюватися нею і виконувати різні дії в залежності від отриманої інформації. Прикладом впровадження такої

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

концепції є система «розумний будинок» або «розумна ферма». Ця система аналізує дані навколишнього середовища і в залежності від показників регулює температуру в приміщенні. У зимовий період регулюються інтенсивність опалення, а в разі спекотної погоди будинок має механізми відкривання і закривання вікон, завдяки чому провітрюється будинок, і все це відбувається без втручання людини.

Розумний дім (розумний будинок/smart home, digital house) — 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 персонального комп'ютера (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 (обстановку) [3].

Для визначення високотехнологічних особливостей приміщення також вживають терміни: intelligent building, smart-house, digital home.

Розумний дім створюється за допомогою професійного проектування та програмування компаніями, що займаються розробкою проектів smart-home. Програми, що вводяться до алгоритмів multi-room розумного дому, розраховані на певні потреби мешканців та ситуації, пов'язані із зміною середовища або безпекою. Особливістю smart-home є керування за допомогою пульта, на котрому людина може натиснути одну-єдину клавішу для створення певної обстановки. При цьому, сама система мульти-рум аналізує навколишню ситуацію та параметри усередині приміщення, та, керуючись власними висновками, виконує задані користувачем команди із відповідними налаштуваннями. Окрім того, електронні побутові прилади, встановлені у розумному будинку, можуть бути об'єднані у домашню Universal Plug'n'Play — мережу із виходом до Інтернету.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

Основні функції розумного будинку (рис.1.1) [4]



Рисунок 1.1 – Основні функції розумного будинку

- Надійна та проста у користуванні система охорони та відеонагляду.
- Автоматична централізована корекція освітлення у залежності від часу доби та пересування людей по приміщенню (особливо важлива для тих, хто виховує дітей або доглядає за родичами похилого віку).
- Побутові турботи, які, зазвичай, лягають на плечі людини, у розумному будинку узгоджуються з усіма його системами та виконуються найлегшим і найефективнішим способом за допомогою сучасного обладнання. Це, наприклад, може бути полив саду або його накриття від сонця (грози) згідно із вимірами погодних умов; відчинення дверцят о певній годині для виходу домашніх тварин, щоб уранці вони могли вийти на двір без залучення часу хазяїв і т.д.
- Контроль за протіканням води/газу.
- Орієнтація на енергозбереження. Інтелектуальний дім — це не енергоекономна система.

- Домашня автоматика будинку дозволяє покращити умови життя та спростити побутові задачі для користування інвалідів та людей похилого віку.

- Можливість керування інтелектом будинку та побутовими приладами через інтерфейс за допомогою телефонної лінії, мобільного зв'язку або Інтернет. Тобто, можливо робити якісь домашні справи через смартфон або веб-браузер, ще не діставшись самого будинку.

- Усі функції виконуються за допомогою одного пульта-дисплея.

Як і інші пристрої система “Розумний будинок” має переваги, заради яких її варто встановити. Серед них:

Безпека. Система повністю контролює приміщення. Якщо був здійснений незапланований доступ, то вона надішле повідомлення про це. При виникненні надзвичайних подій “Розумний будинок” спробує їх запобігти, в тому числі виникнення пожеж. Він дозволяє спостерігати за тим, що відбувається в будинку з будь-якої точки світу.

Простота у використанні. Вся система управляється єдиним пристроєм. Найчастіше це мобільні телефони.

Гнучкі налаштування. Система дозволяє підлаштовувати пристрої під себе, змінювати їх функції. Так само в неї можна додавати інші прилади в будь-який зручний час.

Економія. «Розумний будинок» знижує витрати за комунальні рахунки. Це пояснюється тим, що система відключає пристрої, які не використовуються в даний момент. Відповідно навантаження на мережу знижується, а разом з нею і споживання електроенергії. Економія на освітленні може досягати 40%, а на опаленні 30%.

Автоматизація. Велика частина побутових предметів може бути підключена до “розумного будинку”. Відповідно це дає можливість управляти ними в автоматичному режимі. Це значно економить час.

Дизайн. Всі елементи системи (кнопки, термостати, датчики, розетки, вимикачі) виглядають сучасно і стильно вписуються в будь-який інтер'єр.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

Можливість дистанційного включення техніки. Виробники розумної техніки створюють спеціальні програми, які потрібно встановити на смартфон для роботи зі смарт-приладом, де б ви не знаходилися.

Голосове управління. Вам навіть не доведеться вставати з дивана, щоб вимкнути світло, приготувати каву або відключити мультиварку.

Автоматичне оновлення. Смарт-пристрої мають модуль Wi-Fi, завдяки чому можуть оновлюватися автоматично, не вимагаючи втручання господарів.

Попередження надзвичайних ситуацій. У разі витoku газу, води або під час пожежі система швидко реагує і відправляє повідомлення на телефон.

Недоліки у «Розумного будинку» теж є. До них відносяться:

Ціна. Незважаючи на те, що побудова системи в основному опирається на примітивні датчики, камери, сенсори, її вартість дуже висока. Щоб окупити «Розумний будинок» потрібно мінімум 5 років.

Обслуговування. Як і будь-яка інша техніка, система може зламатися. У цьому випадку проблему можуть вирішити тільки досвідчені установники, яких поки що не дуже легко знайти. До того ж поломка однієї деталі може вивести з ладу ланцюжок інших пристроїв.

Установка. Система має бути дротова чи бездротова. Дротова вважається безпечнішою, але її потрібно встановлювати або відразу під час ремонту, або робити ремонт під неї.

1.2. Аналіз існуючих проектів IoT-систем

На сьогоднішній день існує досить велика кількість готових комплектів для «розумного будинку». Готові комплекти для «розумного будинку» мають свої переваги. Перевага вибору останнього полягає в тому, що пристрої в наборі ідеально поєднуються між собою. Проектувальнику не доведеться хвилюватися про те, чи будуть прилади злагоджено функціонувати - вони вже протестовані виробником на ефективну безперебійну роботу.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		15

Проектувальнику будуть потрібні лише мінімальні знання при встановленні і програмуванні обладнання. Після цього залишається тільки насолоджуватися затишком, оскільки всі ключові складові вашої домашньої екосистеми будуть повністю автоматизовані [5].

Ціна на комплект для розумного будинку переважно залежить від його комплектації. Залежно від функціональності і кількості пристроїв, які входять в набір, «розумний дім» може взяти на себе:

- управління електроприладами;
- забезпечення безпеки житла;
- попередження та оперативне припинення тривожних ситуацій (пожежа, протікання води і т. д.);
- створення комфортного температурного режиму, вентиляції та освітлення;
- контроль споживання електроенергії та багато іншого.

Початковий комплект «розумного будинку» - це стартовий набір. Як правило, в нього входить:

- контролер - основний інтелектуальний прилад «розумного будинку»: він контролює всі процеси, які відбуваються в житлі;
- різні датчики, які «стежать» за параметрами і ситуацією на певній території, і передають інформацію на контролер;
- розумна розетка – з її допомогою легко дистанційно керувати електроустаткуванням.

При необхідності ви зможете збільшити можливості системи за рахунок доукомплектації детекторами і іншими пристроями.

«Розумні» набори здатні виконувати як звичайні завдання, так і діяти по більш складному запрограмованому плану. Тому перед купівлею необхідно визначитися, для яких цілей необхідний комплект, що у будівлі потрібно вдосконалити і якими процесами інтелектуальна система повинна керувати. Від цього залежить комплектність набору, і, відповідно, його можливості і вартість.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

При великому бюджеті на розробку проєкта доцільно звернути увагу на бренди: Aqara, Sonoff HomeKit, iLoungeMax, Nest, Apple. Вони найбільш популярні серед покупців, які шукають розумний дім, і на протязі багатьох років тримають високий рівень якості.

При обмеженому бюджеті на розробку та встановлення «розумного будинку», як правило застосовують дешевші варіанти. Приклади таких комплектів за доступними цінами наведено нижче.

LifeSmart HomeKit – комплект розумного будинку з контролером управління розумного будинку. До нього приєднуються датчики, прилади для контролю електроживлення, пристрої автоматизації всіх компонентів інфраструктури. Він має оригінальний дизайн та добре впишеться в інтер'єр [7].

Xiaomi Mi Smart Home Set – є повнофункціональним рішенням. У наборі: контролер розетки, бездротовий комутатор, датчики відкриття, закриття дверей, руху [8].

Orvibo Smart Base - комплект розумного будинку з Wi-Fi до розеток, контролює електроживлення побутових приладів. Готовий комплект містить програму для віддаленого контролю розеток, механізм захисту для безпеки, універсальний пульт управління. Управління можливо з усіх смартфонів, підключених до системи [7].

Broadlink "Просунутий +" - комплект розумного будинку - збалансований набір 5 пристроїв лінійки, що дозволяють контролювати електроживлення побутової техніки, світлового обладнання, створювати схеми автоматизації, повідомляти при небажаному русі [7].

Vera Climat Kit - набір для управління розумним будинком з функцією геолокації, що дозволяє підготувати житло до приходу господарів, активувати прилади контролю клімату (включити опалення, кондиціонування), електроприлади. Гнучке регулювання функцій, потужність до 1,7 кВт [9].

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

Щоб зрозуміти їх можливості, розглянемо деякі комплекти більш детально.

Комплект Fibaro Starter Kit - це інтелектуальна електронна система, що дозволяє створювати і налаштовувати автоматизоване управління «розумним будинком» (рис.1.2). Дана автоматизована система управління призначена для підвищення життєвого комфорту і безпеки, а також для зниження витрати енергії в будинку. Система Fibaro Starter Kit автоматично і без участі людини виявляє потенційні загрози для дому та здатна реагувати на ці події, в тому числі і використанням складних запрограмованих сценаріїв для кожної конкретної ситуації. Fibaro Starter Kit також повідомить про тривожному подію повідомленням на мобільний пристрій, щоб домовласники могли оперативно вжити додаткових заходів, якщо це необхідно.



Рисунок 1.2 – Загальний вигляд комплекту Fibaro Starter Kit

До складу комплекту Fibaro Starter Kit входить центральний контролер Fibaro Home Center Lite, керована розетка Fibaro Wall Plug FGWPE- 101, датчик затоплення Fibaro Flood Sensor FGFS-101, датчик руху Fibaro FGMS-001, датчик диму Fibaro Smoke Sensor FGSS-101 і датчик відкриття Fibaro Door/Window Sensor FGK-101. Для роботи пристрою набору Fibaro Starter Kiti використовують просунутий бездротовий стандарт автоматизації Z-Wave [7].

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

Контролер Fibaro Home Center Lite є центром управління «розумним будинком». Завдяки контролеру будинок отримує безліч нових можливостей. На контролері працює спеціальне програмне забезпечення, яке відповідає за функції і сценарії роботи систем «розумного будинку». Контролер дозволяє підключити до 230 інтелектуальних пристроїв Z-Wave. Модульність і розширюваність системи на базі технології Z-Wave дають можливість в майбутньому додавати нові елементи «розумного будинку» в залежності від зростаючих потреб.

Зручний і легкий для освоєння інтерфейс панелі управління контролера дозволяє налаштовувати систему «розумного будинку» не володіючи спеціальними навичками і знаннями з програмування. Завдяки мобільним додаткам користувач може контролювати обстановку в будинку, навіть перебуваючи в автомобілі або робочому офісі. Наприклад, за допомогою смартфона і «розумної» розетки можна вимкнути забуте світло або праску. А під час відсутності домовласників контролер візьме на себе функції охоронної системи: виявить спробу несанкціонованого проникнення в приміщення або злому. Якщо трапиться побутова проблема - витік води, витік газу, загоряння, контролер зніме тривогу і негайно сповістить домовласників.

Керована розетка Fibaro Wall Plug використовується для включення і виключення електричних побутових приладів, а також контролю рівня їх енергоспоживання. Інтелектуальна розетка стежить за інтенсивністю поточного енергоспоживання, попереджаючи про наближення допустимого рівня граничного навантаження. Звіт про фактичне споживання енергії розетка передає по бездротовому протоколу на центральний контролер «розумного будинку», який візуалізує отриману інформацію у вигляді наочних для користувача графіків і діаграм. Це дозволяє виявити найбільш енергоємні електроприлади в будинку і обмежити їх використання.

Бездротовий датчик виявлення протікання води Fibaro Flood Sensor призначений для виявлення затоплень приміщень. Датчик встановлюється на

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

підлогу і при попаданні води на ніжки пристрою відбувається замикання контактів і видається сигнал тривоги. Датчик здатний відправляти сигнал про небезпеку затоплення на блок центрального контролера, включати вбудовану або зовнішню сирену, сигналізувати про позаштатну ситуацію зміною кольору світлодіодного підсвічування. Датчик має водонепроникний корпус. При затопленні приміщення датчик не тоне, а плаває у воді.

Датчик руху Fibaro Motion Sensor призначений для відстеження присутності і пересування людини в приміщенні. Принцип дії датчика заснований на розпізнаванні інфрачервоного випромінювання, що виходить від людей. Якщо в приміщення потрапить будь-якої неживий рухається предмет, наприклад м'яч, датчик не спрацює. Виявляючи присутність людини, датчик може ініціювати певні сценарії поведінки розумного будинку: наприклад, включати світло або музику. Довга відсутність людей в поле зору датчика також можна запрограмувати на якісь корисні дії - наприклад, закриття дверей і постановку будинку на охоронну сигналізацію, якщо в поспіху господарі забули це зробити.

Пожежний датчик Fibaro Smoke Sensor призначений для виявлення загоряння в приміщенні. Датчик дозволяє виявити дим на ранній стадії пожежі, до появи сильного полум'я. Виявивши задимлення, датчик відправить відповідне повідомлення про пожежну тривогу по дроту сигналізації або на контролер Z-Wave. Одночасно з цим активує і вбудовану звукову сирену. Оскільки деякі матеріали горять без виділення диму, в датчик інтегрована паралельна система виявлення пожежі за допомогою вимірювання температури. Датчик визначає температуру навколишнього повітря, і при різкому її підвищенні діагностує загоряння, навіть якщо кількості диму недостатньо для включення сигналу тривоги. Чутливість датчика диму можна регулювати, щоб він не реагував на незначне задимлення, наприклад, під час приготування їжі. Тому цей датчик, на відміну від багатьох інших, можна використовувати на кухні.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

Датчик відкриття дверей/вікна Fibaro Door/Windows Sensor розширює можливості захисту будинку від несанкціонованого проникнення, контролюючи відкриття дверей і вікон, гаражних воріт і т.д. При відкритті дверей або вікна датчик негайно сповіщає про несанкціоноване вторгнення. Також цей датчик може використовуватися в сценаріях автоматичного управління світлом і мікрокліматом в будинку - ці сценарії програмуються за допомогою центрального контролера. Комбінація датчика відкриття і датчика руху дозволяє реалізувати сценарій автоматичного освітлення приміщення при появі там людини - це може бути дуже актуально для освітлення підвалу або комори.

Комплект Fibaro Starter Kit працює по бездротовому протоколу зв'язку Z-Wave. Протокол Z-Wave працює в діапазоні частот 869 МГц. Відстань від датчика до контролера або найближчого пристрою Z-Wave має становити не більше 50 м в умовах прямої видимості і не більше 30 м в приміщенні.

Забезпечується відмінна розширюваність системи «розумного будинку» завдяки можливості поступово додавати функції за рахунок підключення нових пристроїв. Підтримується до 225 додаткових Z-Wave пристроїв «розумного будинку».

Для запобігання нештатних ситуацій Fibaro Starter Kit аналізує інформацію від датчиків диму, витоків газу, протікання води, руху, удару, відкриття дверей, контролю температури і вологості і ін. За сигналом датчика при аварійній ситуації можливе включення пожежної або тривожної сигналізації.

Також гарним типовим варіантом є комплект для розумного будинку Broadlink "Покращений +" (TC2-2) (рис.1.3) [9].

Комплект для «розумного будинку» Broadlink "Покращений +" (TC2-2) - це гармонійно підібране поєднання п'яти пристроїв лінійки Broadlink, що доповнюючи один одного дозволяють дистанційно керувати роботою побутових приладів і світлом, створювати сценарії автоматизації, і бути поінформованим про небажану активність всередині приміщення.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		21



Рисунок 1.3 – Загальний вигляд комплекту Broadlink "Покращений +" (TC2-2)

До нього входить: універсальний пульт управління Broadlink RM-Pro; система датчиків Broadlink e-Air; комплект датчиків Broadlink SmartOne S1C; «розумна Wi-Fi розетка» Broadlink SP Contros і Розумний сенсорний вимикач Broadlink TC2-2.

Одним з основних механізмів комплекту є універсальний пульт управління Broadlink RM-Pro, саме при взаємодії з ним інші комплектуючі, такі як багатофункціональна система з 5 датчиків Broadlink e-Air (A1) і комплект Broadlink SmartOne S1C (підтримує до 16 датчиків) забезпечують дистанційне керування електроприладами в будинку. Наприклад, такими як: телевізор, кондиціонер, DVD, жалюзі, музичний центр, світильник. А розумний сенсорний вимикач Broadlink TC2-2 в зв'язці RM-Pro реалізує індивідуальні сценарії включення або виключення світла в будинку, в залежності від показників системи датчиків e-Air (A1), SmartOne S1C або ж за заданим розкладом.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

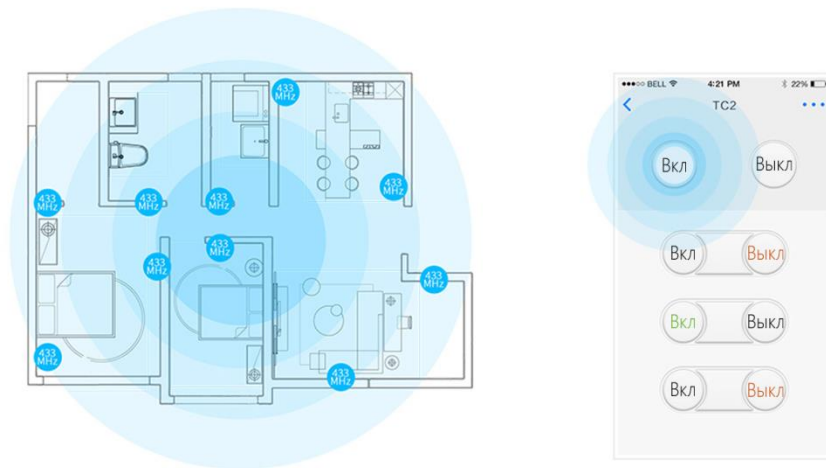


Рисунок 1.4 – Загальний варіант розміщення елементів
та пульт Broadlink RM-Pro

Функціонал універсального пульта дозволяє задавати певний сценарій. Наприклад, при зниженні температури система Broadlink e-Air (A1) подасть сигнал на контролер Broadlink RM Pro, а той в свою чергу включить обігрівач, після досягнення потрібної температури відключить.

У свою чергу, система сигналізації S1C, що включає в себе датчик руху і датчик відкриття, при взаємодії з RM Pro забезпечить три режими роботи пристроїв:

- повний захист;
- частковий захист - частина обраних датчиків будуть зняті з захисту, а інша частина продовжить охороняти приміщення;
- знятий захист - датчики будуть працювати тільки для автоматизації процесів в будинку, без тривоги.

Корисним доповненням комплекту є Розумна Wi-Fi розетка Broadlink SP Contros. Її широкий функціонал з управління будь-яким електроустаткуванням дозволяє створювати власний розклад живлення електроприладів:

- задавати «зворотний відлік» (відключати або включати живлення після закінчення заданого періоду часу);

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

встановити «запланований час» (вмикання/вимикання приладу у встановлений час з можливістю повторення в певні дні тижня);

включити випадковий таймер (вмикання/вимикання електроживлення в випадковий час для створення «ефекту присутності»).

Моделі комплекту виконані у вогнетривкому полікарбонаті з акриловим покриттям та з легкістю впишуться в будь-який дизайн будинку.

Функції та особливості комплекту:

Комплект для Розумного будинку дозволяє дистанційно керувати електроприладами.

Підтримує стандарт Wi-Fi IEEE 802.11 b/g/n (2.4 ГГц).

Настроюється і управляється за допомогою мобільного додатку Broadlink e-Control через Wi-Fi/2 G/3 G.

Дозволяє задавати певні сценарії роботи електроприладів.

Радіочастота сигналу складових комплекту - 433 МГц.

Пульт управління Broadlink RM-Pro підтримує інфрачервоні сигнали (7 ІК випромінювачів, частота сигналу - 38 К, пропускна здатність - 95%), оснащений радіомодулем (частота радіосигналу - 433 МГц).

1.3. Аналіз проблем безпеки IoT-систем «розумних будинків»

Незважаючи на те, що IoT-система «розумного будинку» сама має велику кількість функцій для забезпечення безпеки будинку, вона також має ряд вразливостей і може мати серйозні проблеми з кібербезпекою. Існує велика кількість прикладів, які це демонструють [4].

В 2013 році були оприлюднені результати дослідження невідомим вченим загального стану безпеки в Інтернеті. Дослідження відбувались у 2012 році, дослідник перевіряв відкриті порти на всіх доступних IP-адресах. Через обсяг роботи, яку слід було виконати, дослідник створив комп'ютерного хробака, який шукав пристрої, доступ до яких не був

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		24

захищений паролем, або захищений надзвичайно простим паролем (наприклад, «root» або «admin»). Створений ним ботнет, який отримав ім'я «Carna», зібрав понад 9 ТБ даних, виконав 52 мільйони запитів ICMP ping, 180 мільярдів службових записів, та 2,8 мільярди запитів TCP SYN на 660 мільйонів IP адрес і опитав у сумі 71 мільярд портів. Його хробак спромігся поширитись на понад 400 тисяч пристроїв [5].

В ході досліджень ним був помічений інший хробак, який отримав назву Aidra та був створений для пристроїв під управлінням ОС на основі Linux та процесорної архітектури MIPS. Основним призначенням хробака Aidra було створення ботнету для DDoS-атак. Всього було виявлено 30 тисяч заражених цим хробаком пристроїв[10]. В 2013 році були оприлюднені у вільному доступі початкові коди хробака Aidra (LightAidra) [6].

У вересні 2016 року після публікації статті про угруповання, які продають послуги ботнетів для здійснення DDoS-атак, вебсайт журналіста Брайана Кребса (англ. Brian Krebs) сам став жертвою DDoS-атаки, трафік якої на піку досягав 665 Гб/с, що робить її однією з найпотужніших відомих DDoS-атак. Оскільки хостер сайту відмовився надалі безоплатно надавати свої послуги, сайт довелось на деякий час закрити поки не був знайдений новий хостер. Атака була здійснена ботнетом з інфікованих «розумних» відео-камер (що є підмножиною Інтернету речей). У жовтні того ж року зловмисники оприлюднили початкові тексти використаного шкідливого ПЗ (відоме під назвою Mirai), чим створили ризики неконтрольованого відтворення атак іншими зловмисниками [7].

Ботнет Mirai став можливим завдяки реалізації вразливості, яка полягала у використанні однакового, незмінного, встановленого виробником пароля для доступу до облікового запису адміністратора на «розумних» пристроях. Всього мав відомості про 61 різних комбінацій логін-пароль для отримання доступу до облікового запису методом перебирання[8].

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

Дослідження показали, що значна частина вразливих пристроїв була виготовлена з використанням складових виробництва фірми XiongMai Technologies з офісом в Ханчжоу, та фірми Dahua, Китай. Також дослідження показали, що станом на 23 вересня, коли атака сягнула піку інтенсивності, в Інтернеті можна було знайти понад 560 000 пристроїв вразливих до подібного типу атак[10].

Дослідники загроз із компанії Cisco виявили 224 нових вразливості в продуктах, які не належать Cisco: з них 74 уразливостей з IoT-пристроями. Як розвивається та розширюється IoT, те саме відбувається і з мережами ботів IoT. Та оскільки ці мережі ботів зростають та вдосконалюються, зловмисники використовують їх для запуску DDoS-атак з усе більшою інтенсивністю та масштабністю. Звіт IoT за 2020 рік компанії Gemalto свідчить, що найбільшою проблемою є захист даних, обсяги яких зростають: тільки 60% організацій визнають шифрування цих даних, а 40% залишають їх уразливими; 48% компаній не можуть виявити, який пристрій IoT має порушення.

Таким чином, для управління «розумними будинками» надзвичайно критичною є вимога безпеки IoT-системи, адже успішні атаки означатимуть контроль зловмисника над приладами всередині будинку користувача, що є надзвичайно небезпечним та вкрай небажаним.

Безпека Інтернету речей – це сектор інформаційних технологій, який фокусується на захисті кінцевих пристроїв, мереж та даних, що стосуються Інтернету речей – підключених пристроїв, які не є комп'ютерами, смартфонами або планшетами. По суті, безпека Інтернету речей - це широкий термін, що охоплює стратегії, політики, процеси та технології безпеки, які компанії використовують для захисту своїх пристроїв Інтернету речей від інтелектуальних холодильників та камер відеоспостереження до моніторів на

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

реактивних двигунах або автомобілях та пов'язаних з ними даних, додатків та мережі від злому або іншої шкоди.

Пристрої з підтримкою Інтернету створюють ряд проблем безпеки. Але хоча Інтернет речей дає можливість підключення до нових пристроїв, загальні проблеми кібербезпеки не є новими (рис. 1.5). [4]

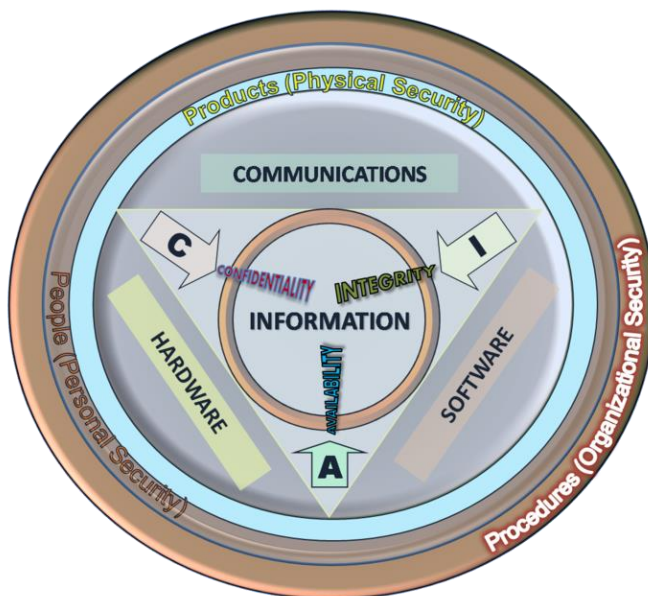


Рисунок 1.5 – Загальні види загроз IoT

Загрозами інформаційної безпеки «розумного будинку» є порушення конфіденційності, цілісності та доступності інформації.

Загрози конфіденційності - це загрози, які призводять до небажаного розкриття конфіденційної інформації. Під загрозами конфіденційній інформації прийнято розуміти потенційні чи реально можливі дії по відношенню до інформаційних ресурсів, що призводять до неправомірного оволодіння даними, які охороняються [9]. Наприклад, порушення конфіденційності в системах домашнього моніторингу можуть привести до ненавмисного розкриття конфіденційних медичних даних. Навіть такі дані, як внутрішня температура будинку, можуть використовуватися для визначення того, зайнятий будинок чи ні. Втрата конфіденційності в таких речах, як ключі та паролі, призведе до несанкціонованих загроз доступу до системи.

Загрози доступу, ймовірно, є найбільшими загрозами. Несанкціонований доступ до системного контролеру, особливо на рівні адміністратора, робить всю систему небезпечною. Це може бути пов'язано з неправильним управлінням паролями і ключами або з неавторизованими пристроями, що підключаються до мережі. Навіть якщо контроль не може бути отриманий, несанкціоноване підключення до мережі може викрасти пропускну здатність мережі або привести до відмови в обслуговуванні законним користувачам. Оскільки багато пристроїв розумного будинку можуть працювати від батареї і мати бездротову мережу з низьким робочим циклом, переповнення мережі запитами може привести до атаки з виснаженням енергії - формі відмови в обслуговуванні.

До загроз доступу відноситься і слабка аутентифікація. Паролі є однією з перших ліній захисту від спроб злому. Але якщо ваш пароль недостатньо надійний, то і пристрій недостатньо захищений. Більшість паролів за замовчуванням є відносно слабкими, оскільки вони призначені для зміни, а в деяких випадках вони можуть бути загальнодоступними або зберігатися у вихідному коді програми (це надзвичайно ризиковано). Кінцеві користувачі також можуть встановити пароль, що легко запам'ятати. Але якщо його легко запам'ятати, то, ймовірно, легко проникнути.

Багато пристроїв IoT мають незначну аутентифікацію або взагалі не мають її. Навіть якщо на самому пристрої немає важливих даних, уразливий пристрій IoT може бути шлюзом до всієї мережі або його можна асимілювати в ботнет, де хакери можуть використовувати його потужність обробки для поширення шкідливого програмного забезпечення та розподіленої відмови в обслуговуванні (DDoS-атаки) [15].

Слабка автентифікація є серйозною проблемою безпеки IoT. Виробники можуть допомогти зробити автентифікацію більш безпечною, вимагаючи кількох кроків, використовуючи надійні паролі за замовчуванням

та встановлюючи параметри, які ведуть до безпечних паролів, створених користувачами.

Суттєвою вразливістю є *доступність мережевої системи*. Оскільки сучасні системи «розумний будинок» підключені до Інтернету, атаки можуть проводитися дистанційно, або за допомогою прямого доступу до мережевих інтерфейсів управління, або шляхом завантаження шкідливих програм на пристрої.

Пристроєм Інтернету речей простіше використовувати ту саму мережу, що й інші пристрої кінцевого користувача, наприклад їхні Wi-Fi або LAN, але це також робить всю мережу більш вразливою. Хтось може зламати пристрій IoT, щоб отримати доступ до більш конфіденційних даних, що зберігаються в мережі чи інших підключених пристроях. Аналогічно, інший пристрій у мережі може бути використаний для злому пристрою IoT. У будь-якому з цих сценаріїв клієнти та виробники вказують один на одного пальцями. Тому в ідеалі кожна система IoT повинна використовувати окрему мережу та/або мати шлюз безпеки або брандмауер, тому, якщо на пристрої є порушення безпеки, він залишається ізольованим від пристрою. (Це одна з переваг стільникового Інтернету речей.) Віртуальна приватна мережа (VPN) допомагає захистити пристрої від зовнішньої мережі, але якщо ваша система має спільне з'єднання з іншими пристроями, вона все ще вразлива для атак з них, якщо вони пошкоджені.

Фізична доступність системи також є проблемою. Як для бездротових технологій, так і для операторів зв'язку по лініях електропередачі, до фізичних мереж можна отримати доступ зовні, навіть якщо сам будинок надійно заблокований [14].

Наступна вразливість - *обмежені системні ресурси*. Контролери пристроїв традиційно представляли собою невеликі 8-розрядні мікроконтролери з дуже обмеженими обчислювальними ресурсами і

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		

ресурсами збереження, що обмежувало їх здатність реалізовувати складні алгоритми безпеки.

Більшість додатків IoT використовують дуже мало даних. Це знижує витрати та подовжує термін служби батареї, але може ускладнити оновлення по повітрю і не дозволяє пристрою використовувати функції кібербезпеки, як-от брандмауери, антивірусні сканери та наскрізне шифрування. Це в кінцевому підсумку робить їх більш вразливими для злому.

Саме тут важливо, щоб сама мережа мала вбудовані функції безпеки.

Системна неоднорідність також є вразливістю. Пристрої поставляються багатьма виробниками з різними мережевими стандартами і різними можливостями оновлення програмного забезпечення. Часто пристрої мають мало або взагалі не мають документації по своєму внутрішньому програмному забезпеченню, операційних системах і встановлених механізмах безпеки.

Фіксована прошивка - ще одна проблема. Існує дуже мало розумних побутових приладів, які надають будь-які регулярні послуги з оновлення програмного забезпечення для виправлення вразливостей.

Ще один з найбільших ризиків безпеки IoT – це якщо пристрої виходять на поле з помилкою, яка створює вразливості. Незалежно від того, чи надходять вони з вашого власного розробленого коду чи третьої сторони, виробникам потрібна можливість випускати оновлення мікропрограми, щоб усунути ці ризики безпеки. В ідеалі це повинно відбуватися віддалено, але це не завжди можливо. Якщо швидкість передачі даних мережі занадто низька або вона має обмежені можливості обміну повідомленнями, можливо, вам доведеться фізично отримати доступ до пристрою, щоб запустити оновлення.

Застарілі пристрої в системі. Якщо система спочатку не була розроблена для підключення до хмари, вона, ймовірно, погано обладнана для боротьби з сучасними кібератаками. Наприклад, старі пристрої можуть бути

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

несумісними з новішими стандартами шифрування. Робити застарілі системи з підтримкою Інтернету, не вносячи суттєвих змін, ризиковано, але це не завжди можливо із застарілими пристроями. Вони з'єднувалися роками (можливо, навіть десятиліттями), що перетворює навіть невеликі покращення безпеки на монументальне починання [16].

Відсутність шифрування. Однією з найбільших загроз для безпеки IoT є відсутність шифрування при регулярних передачах. Багато пристроїв IoT (особливо старих) не шифрують дані, які вони надсилають, а це означає, що якщо хтось проникає в мережу, вони можуть перехопити облікові дані та іншу важливу інформацію, що передається на пристрій і з нього.

Повільне впровадження стандартів – це також вразливість. Що стосується стандартів безпеки, то IoT є відкритий для всіх. Немає універсального стандарту для всієї галузі, а це означає, що всі компанії та ніші виробники повинні розробляти власні протоколи та рекомендації. Відсутність стандартизації ускладнює захист пристроїв Інтернету речей, а також ускладнює можливість міжмашинного зв'язку (M2M) без збільшення ризику.

У той час як деякі пропрієтарні системи, такі як підсистема моніторингу працездатності, можуть мати добре розроблену, відповідаючу стандартам безпеку, більшість сучасних пристроїв розумного будинку реалізують кілька, якщо взагалі застосовують, підходів до безпеки.

Суттєвою вразливістю є *брак професійних спеціалістів з безпеки*, які можуть керувати всіма складовими мережі «розумний будинок». Мало хто з домовласників може дозволити собі професійну допомогу в управлінні домашньої мережею [3]. Замість цього домовласники-любители повинні мати можливість самостійно, безпечно і надійно управляти своїми системами.

1.4. Аналіз особливостей та умов рішення поставленого завдання

Для розробки проекту було надано вхідні данні, які включають загальний вигляд котеджу та його план. Загальний вигляд котеджу подано на рис. 1.5

Котедж одноповерховий та має присадибну ділянку. До основної частини прибудовано гараж для легкового автомобіля.



Рисунок 1.5 – Загальний вигляд котеджу для виконання проекту

План котеджу подано на рис. 1.6.

До складу котеджу входять такі основні елементи:

вітальня;

три спальні кімнати;

їдальня;

кухня;

санітарні вузли – 3 шт;

гардеробні кімнатки – 3 шт;

систему коридорів;

прибудований гараж.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		32



Рисунок 1.6 – План котеджу для виконання проекту

Більшість систем та підсистем «розумного будинку» будуть експлуатуватися в умовах опалювальних приміщень, що визначає умови експлуатації обладнання та покладає на систему IoT вимоги до підтримки заданої температури в приміщеннях, відносної вологості, розміщення мережевого обладнання та елементів IoT, освітлення, часу доби та пори року.

1.5. Постановка завдання

Таким чином, необхідно розробити захищену систему «розумний будинок» для заданого проекту котеджу та провести моделювання прийнятих рішень в Cisco Packet Tracer.

Підставою для виконання роботи є завдання на кваліфікаційну роботу.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		33

1.5.1. Умови експлуатації та параметри навколишнього середовища

Умови експлуатації IoT системи в будинку: температура в приміщенні: 20 - 25 °С; відносна вологість: 40-50%; точка роси: не більше 21 °С; швидкість зміни температури: не більше 5 °С за хв.

1.5.2. Вимоги до технічних характеристик

Основні функції «розумного будинку»:

Контроль та дотримання температурних норм приміщень;

Контроль та дотримання норм вологості в приміщеннях;

Протипожежний захист;

Управління системою освітлення;

Управління дренажною системою.

Надійна та проста у користуванні система охорони та відео-нагляду;

Автоматична централізована корекція освітлення у залежності від години доби та пересування людей по приміщенню (особливо важлива для тих, хто виховує дітей або доглядає за родичами похилого віку);

Контроль за протіканням води/газу;

Орієнтир на енергозбереження;

Можливість керування інтелектом будинку та побутовими приладами через інтерфейс за допомогою телефонної лінії, мобільного зв'язку або Інтернет.

1.5.3. Вимоги до надійності

Система має бути частково резервована, придатна до ремонту, відновлювальна.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		34

1.5.4. Вимоги до захищеності IoT системи

Розробити заходи та засоби забезпечення кібербезпеки під час функціонування IoT системи котеджу.

Висновки по 1 розділу

Актуальною задачею сьогодення є розробка IoT систем, у тому числі і «розумних будинків».

Проведений аналіз показав, що на сьогодні ринок пропонує велику кількість пристроїв та систем IoT, що можуть бути використані для рішення завдання. Однак, слід відмітити, що системи IoT мають ряд вразливостей і тому при проектуванні необхідно передбачити заходи та засоби забезпечення кібербезпеки під час функціонування IoT системи котеджу.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ ІОТ-СИСТЕМИ КОТЕДЖУ

2.1. Розробка структурної схеми ІоТ-системи котеджу

При розробці та впровадженні систем «розумний будинок» можна виділити наступні етапи [17]:

Етап 1. Проектування. Включає узгодження ТЗ, розробку схем розміщення обладнання і прокладання кабельних трас, однолінійну схему і схему автоматизації, а також специфікацію обладнання.

Етап 2. Збірка електрощитів і автоматики. У лабораторії збираються всі щити управління (електрика і автоматика, СКС і серверне обладнання різного призначення).

Етап 3. Програмування та налагодження. Програмується логіка роботи системи. Після цього проводяться стендові випробування і остаточне налагодження устаткування.

Етап 4. Монтаж і пусконаладження. Включає перевірку прокладку кабелів і підключення їх до щитового обладнання розумного будинку. Встановлюється обладнання (кнопки і датчики), перевіряється правильність роботи всієї системи.

Етап 5. Тестова експлуатація. Протягом місяця система знаходиться в робочому режимі. Замовник може висловити свої побажання по підстроювання системи і його побажання враховуються.

Етап 6. Гарантійне обслуговування. Надаються терміни гарантії на все обладнання і ПЗ. Сервісна підтримка протягом усього терміну експлуатації.

У рамках цієї роботи необхідно виконати 1 етап та частково 3 етап. Перевірка працездатності та ефективності буде виконана шляхом імітаційного моделювання за допомогою Cisco Packet Tracer.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		36

Система «розумний будинок» дозволяє узгодити роботу окремих елементів життєзабезпечення, налагодити моніторинг з використанням засобів Інтернету, за допомогою віддаленого відеоспостереження, встановити програмну взаємодію компонентів з урахуванням часу дня, погодних умов, побажань господарів.

Розумний будинок об'єднує і дозволяє здійснювати віддалене управління наступними структурами:

- опалення (радіатори та тепла підлога);
- клімат контроль;
- сигналізації систем охорони і захисту від пожежі;
- спостереження за аварійними ситуаціями;
- відеоспостереження;
- освітлювальні прилади всередині і зовні будівлі;
- відео і аудіопотік;
- енергоспоживання, дотримання лімітів по пікових навантажень;
- полив, каналізаційні, насосні станції;
- шлагбауми, ворота, ролокасети, жалюзі.

Розумний будинок здатний забезпечити дотримання найскладнішого режиму. Господар може підпорядкувати до централізованого контролю всі системи: запрограмоване включення деяких ламп в певний час, кращий обігрів однієї з кімнат в залежності від сезону, включення обігрівача в віддаленому будинку (на дачі). Господар може налаштувати SMS оповіщення про несподіване відключення електроенергії, спрацьовуванні сигналізаційного обладнання.

Для зручності управління будинком, IoT систему в ньому доцільно виділити на декілька підсистем (рис. 2.1): управління освітленням, аудіо та відеоапаратурою, охоронною системою, захистом від надзвичайних ситуацій (протікання води, пожежа і т.д.), кліматичними системами (опаленням, кондиціонуванням) та іншими електроприладами.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		37



Рисунок 2.1 – Основні підсистеми «розумного будинку»

Структурна схема представляє собою набір елементів системи і зв'язків між ними. На основі проаналізованих джерел інформації про аналоги та вимог визначений порядок з'єднання елементів між собою та порядок їх розміщення. Показники пристроїв та датчиків реєструються на центральному сервері, який керує усіма компонентами системи. З серверу можна віддалено управляти усіма процесами, які виконуються у системі. Передбачається розгортання сервера у «хмарі». Виходячи з цих міркувань, сформовано узагальнену структурну схему, яка зображена на рис. 2.2.

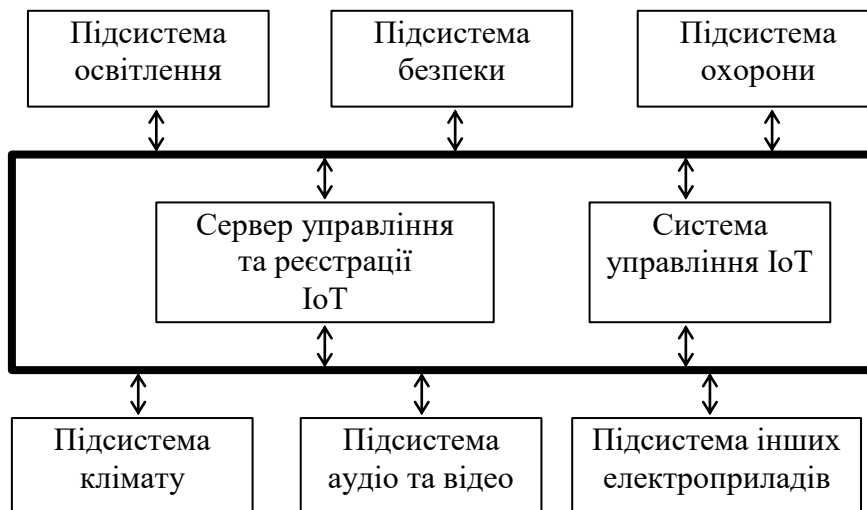


Рисунок 2.2 – Структурна схема IoT-системи для котеджу

Система управління IoT - призначена для формування процесів управління підсистемами та формування і зберігання сценаріїв роботи системи у самому котеджі.

Сервер управління та реєстрації IoT – призначений для віддаленого управління та реєстрації інформації від датчиків, фіксації подій. На сервері реєстрації IoT створюються облікові записи для контролю за всіма елементами в різних приміщеннях житлового будинку. Відповідно до рекомендацій безпеки такий сервер доцільно розгортати у «хмарному» середовищі.

Підсистема освітлення. Управління світлом – це одна з найголовніших переваг системи «розумний будинок» і одна з самих затребуваних її функцій, бо саме світло ми використовуємо переважно у будинку і саме воно є невід’ємною частиною інтер’єру. Підсистема має сама управляти освітленням будинку: за заданим господарем сценарієм вмикаються і вимикаються лампочки та світильники, у визначений час запалюється вечірнє освітлення, вночі будинок сам вимикає світло у всіх кімнатах. Одним натисканням кнопки можна включити або виключити, відрегулювати будь-яке джерело світла в будинку. При цьому господарі можуть перебувати в будь-якій кімнаті будинку або навіть в іншому місті або країні, тому що управляти цією системою можна з мобільного телефону або за допомогою Інтернет.

Можна використати єдину панель управління світлом, що замінює всі вимикачі світла в будинку. Вона також забезпечує доступ до світла у всіх приміщеннях будинку (гараж, коридор, комора тощо), перебуваючи в одній кімнаті можна керувати світлом у всіх інших приміщеннях будинку і в кожному з них окремо.

Велику роль в управлінні освітленням відіграє димер (світлорегулятор). З його допомогою можна управляти яскравістю кожної лампочки: поступове засвічення або затухання, поєднання декількох світлових фонів – можна підсвітити один кут кімнати, а інший заховати в напівтемряві, зробивши інтер’єр кімнати набагато цікавішим.

У разі відсутності господарів, освітлення працює таким чином, що створюється враження, що мешканці знаходяться вдома. Імітація присутності

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		39

господарів – ви самі можете налаштувати систему так, щоб, коли вас немає вдома, вона управляла світлом, створюючи повну імітацію присутності господарів. Це особливо зручно, коли ви у відрядженні, відпустці або в тривалому від'їзду.

Управляти системою освітлення можна за допомогою заздалегідь заданих світлових сценаріїв, які зберігаються в пам'яті системи «розумного будинку».

Підсистема безпеки призначена для забезпечення безпеки будинку та осіб що там проживають. Для захисту від пожежі передбачено датчики диму в кожній кімнаті. При спрацюванні вмикається сирена, відключається електроенергія, крім основних споживачів. Для захисту від газу передбачені датчики газу на кухні та в інших кімнатах. При їх спрацюванні вмикається сирена, перекривається клапан газу в квартирі, вмикається витяжна вентиляція.

Захист від протікання води можна реалізувати таким чином: у ванній та в кухні на підлозі розмістити датчики води. При потраплянні на них води, реле вмикає електромагнітний клапан і він перекриває центральну подачу води в квартирі. Відновлюється подача води в ручну з пульта, панелі, або натиснувши відповідну кнопку в системі управління.

Підсистема охорони. На дверях та вікнах розміщені геркони, які реагують на відкриття дверей. В залі багатофункціональний датчик стежить за рухом. При спрацюванні вмикається сирена, закривається електромагнітний замок на шафі з важливими речами та документами без можливості його відкриття поки будинок під охороною. При відкритті дверей можливе включення веб-камери для фіксації осіб, що входять.

Підсистема клімату призначена для управління кліматом в приміщеннях. Стабільність клімату досягається керуванням електричними теплими підлогами в приміщеннях, вентиляцією та кондиціонуванням. Система управління дозволить встановлювати бажану температуру на будь-яку годину будь-якого дня тижня, а також керувати ними за будь якими

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						40
Змн.	Арк.	№ докум.	Підпис	Дата		

іншими зовнішніми ознаками (відключати при спрацюванні датчика диму, води). Якщо є обмеження на вхідну електричну потужність, то та ж система управління буде контролювати, щоб елементи теплої підлоги вмикались по чергово, а коли вмикається електрочайник – то вимкнуться нагрівальні кабелі підлоги.

Будинок сам круглий рік підтримує в кімнатах комфортну температуру, при якій дихається легко і працюється ефективно, а відпочивається затишно.

Підсистема аудіо та відео призначена для управління мультимедіа в квартирі. Наприклад, багатофункціональний датчик є також інфрачервоним передавачем, з пам'яттю на 255 команд. Тобто він може керувати будь-яким приладом, який керується пультом. В даному випадку керуємо телевізором та музичним центром. Можна з однієї кнопки вмикати телевізор на улюбленому каналі на улюбленій гучності.

Підсистема інших електроприладів дозволяє включати техніку за сценарієм. Можна запрограмувати систему на включення або виключення будь-якого приладу в певний час.

Витяжка в ванній та на кухні, що може налаштовувати затримку часу, ввімкнення за певної умови (наприклад ввімкнути витяжку на 2 хв, після закриття дверей в ванній, ввімкнення після вимкнення світла провітрювання в ночі).

Розетки. Керуючи розетками можна керувати будь-яким приладом, який в неї ввімкнений. Якщо ви ввімкнете в неї опалювальний прилад і відповідно запрограмуєте панель управління, то вона буде підтримувати задану вами температуру в приміщенні.

Електроконтактор в розподільчій коробці. Керуючи ним, ви керуєте всіма споживачами, які до нього під'єднані. Найчастіше до нього під'єднують всі розетки. Він може відключити всі розетки при спрацюванні датчика затоплення, щоб унеможливити потрапляння під дію електричного струму.

Електромагнітний замок – виконує функції безпеки.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		41

Спеціальний електроклапан в ванній по команді, або по таймеру може набрати воду в ванній. Вимикатись пристрій може по датчику води, який розміщується зверху в ванній, або просто по таймеру.

2.2. Модель ризиків IoT системи котеджу

При розробці системи важливо знати загрози, на які вона може наражатися, а після завершення розробки та створення архітектури передбачити належні засоби її захисту. Важливо спланувати стратегію безпеки на початку розробки системи, адже знаючи, як зловмисники можуть скомпрометувати систему, можна спочатку усунути відповідні ризики.

Забезпечення безпеки починається з розгляду моделі ризиків. Оскільки елементом IoT системи виступає «хмарне» середовище Azure, то будемо орієнтуватись на моделі ризиків корпорації Майкрософт. Досвід компанії показує, що крім швидкого з'ясування того, які загрози найсерйозніші, моделювання надає несподівані переваги. Наприклад, можна обговорити загрози з користувачами не з команди розробки, щоб почерпнути нові ідеї та покращити продукт.

Мета моделювання ризиків — зрозуміти, як зловмисники можуть скомпрометувати систему та забезпечити належне усунення ризиків. Завдяки моделюванню ризиків, команда розробників знаходить способи усунення ризиків під час розробки системи, щоб їх не довелося шукати після її розгортання. Це дуже важливо, оскільки модернізація засобів безпеки для безлічі пристроїв у галузі недоцільна, може спричиняти помилки та супроводжується ризиком для клієнтів.

Багато команд успішно встановлюють багатofункціональні вимоги до системи, що надає переваги клієнтам. Проте є складніше завдання — знайти в системі неочевидні вразливості, якими можуть скористатися. Моделювання ризиків допомагає командам розробки зрозуміти, що може зробити зловмисник і чому. У рамках цього структурованого процесу вони

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

обговорюють рішення щодо проектування середовища безпеки в системі, а також вносять зміни до архітектури, пов'язані з безпекою. Хоча модель ризиків є лише документ, це ідеальний спосіб забезпечити безперервну передачу знань та використання отриманого досвіду, що дозволяє новим командам швидко увійти в курс справи. Нарешті, моделювання ризиків дозволяє врахувати інші аспекти безпеки, наприклад, зобов'язання щодо безпеки перед клієнтами. У поєднанні з моделюванням ризиків ці зобов'язання забезпечують поінформованість пристрою під час тестування рішення Інтернету речей (IoT).

Моделювання ризиків – дуже цінна перевага, якщо використовувати її на етапі розробки. При розробці доступні гнучкіші можливості внесення змін для усунення загроз. Таким чином, можна спочатку усунути загрози. Це набагато простіше, ніж додавати засоби усунення ризиків, тестувати їх та підтримувати їхню актуальність. Крім того, не завжди можна все це зробити. З розвитком техніки стає дедалі важче усувати небезпеки. У свою чергу, це потребує більше роботи і жорсткіших компромісів, ніж моделювання ризиків на ранньому етапі розробки.

Під час моделювання ризиків слід розглядати рішення як одне ціле, зосереджуючись на наступних функціях:

забезпечення безпеки та конфіденційності;

функції, збій яких впливає на безпеку;

функції, робота яких пов'язана із кордоном довіри.

Як виконується моделювання ризиків

Моделювання ризиків передбачає такі чотири етапи:

моделювання застосування;

створення списку загроз;

усунення ризиків;

перевірка усунення ризиків.

При побудові моделі ризиків слід керуватися такими рекомендаціями:

- Створити схему з урахуванням еталонної архітектури.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						43
Змн.	Арк.	№ докум.	Підпис	Дата		

- Провести огляд системи. Перш ніж заглибитись у процес, необхідно отримати відомості про систему та сформулювати загальне уявлення. Використання цього підходу, дозволяє зосередитися на потрібних аспектах.
- Не процес повинен керувати розробником, а розробник процесом. Якщо ви виявили проблему на етапі моделювання та хочете вивчити її, одразу ж приступайте. (Не потрібно суворо дотримуватись цих рекомендацій.)

Модель ризиків передбачає такі чотири основні елементи:

- Процеси (наприклад, веб-служби, служби Win32 та керуючі програми *nix). Деякі складні сутності (наприклад, польові шлюзи та датчики) можуть бути абстраговані як процеси, якщо у відповідних областях неможлива технічна деталізація.
- сховища даних (будь-які місця зберігання даних, наприклад файли конфігурації або бази даних);
- потоки даних (у яких дані переміщуються між іншими елементами системи);
- зовнішні сутності (будь-які елементи, які взаємодіють із системою, але не під керівництвом програми, наприклад користувачі та допоміжні веб-канали).

Всі елементи в схемі архітектури схильні до різних загроз. У цій роботі для них використовуватиметься позначення STRIDE (спуфінг, незаконна зміна, відмова, розкриття інформації, відмова в обслуговуванні та несанкціоноване підвищення привілеїв). STRIDE stands for "Spoofing", "Tampering", "Repudiation", "Information disclosure", "Denial of service", and "Elevation of privilege".

Ідея полягає в тому, що можна класифікувати всі свої загрози за однією з 6 категорій STRIDE. Оскільки кожна категорія має певний набір потенційних засобів пом'якшення, після того як ви проаналізуєте загрози та класифікуєте їх, ви повинні знати, як їх пом'якшити.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		44

Слід зауважити, що STRIDE не є суворим механізмом класифікації – існує багато збігів між різними категоріями (наприклад, успішна атака на підвищення привілеїв може призвести до підробки даних). Але це не змінює того факту, що це надзвичайно корисний механізм для аналізу загроз для системи.

Кожна з категорій STRIDE означає наступне:

Підробка (спуфінг). Атака спуфінгу відбувається, коли злоумисник видає себе за когось, ким він не є. Таким чином, злоумисник, який використовує викрадення DNS і видає себе за `www.microsoft.com`, буде прикладом «спуфінгу». Локальні атаки можуть відбуватися. Наприклад, один із механізмів, який фреймворк плагінів Decal впроваджує в процес Asheron's Call, полягає в підробці одного з об'єктів COM, які використовує Asheron's Call.

Фальсифікація. Атаки фальсифікації відбуваються, коли злоумисник змінює дані під час передачі. Злоумисник, який змінив потік TCP, передбачивши порядкові номери, буде маніпулювати цими потоками даних. Очевидно, що сховища даних можуть бути підроблені – саме це відбувається, коли злоумисник записує спеціально створені дані у файл, щоб використати вразливість.

Відмова. Відмова відбувається, коли хтось виконує дію, а потім стверджує, що насправді він цього не робив. В першу чергу це проявляється в таких операціях, як операції з кредитною картою – користувач купує щось, а потім стверджує, що він цього не робив. Інший спосіб, як це відображається, – це в електронній пошті – якщо я отримаю від вас електронний лист, ви можете стверджувати, що ви ніколи його не надсилали.

Розкриття інформації. Загрози розкриття інформації зазвичай досить прості – чи може злоумисник переглядати дані, які він не повинен переглядати? Отже, якщо ви передаєте дані з одного комп'ютера на інший, якщо злоумисник може пронюхати дані на дроті, то ваш компонент піддається загрозі розкриття інформації. Сховища даних також піддаються

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		45

загрозам розкриття інформації – якщо не уповноважена особа може прочитати вміст файлу, це є розголошенням інформації.

Відмова в обслуговуванні. Загрози відмови в обслуговуванні виникають, коли зловмисник може погіршити або відмовити користувачам у наданні послуг. Отже, якщо зловмисник може зламати ваш компонент або перенаправляти пакети в «чорну діру», або перевантажити повністю весь процесор, у вас виникає ситуація «Відмова в обслуговуванні».

Підвищення привілею. Загроза підвищення привілеїв відбувається, коли зловмисник має можливість отримати привілеї, яких він зазвичай не мав. Однією з причин того, що класичні переповнення буфера є настільки важливими, є те, що вони часто дозволяють зловмисникові підвищити рівень своїх привілеїв – наприклад, переповнення буфера в будь-якому компоненті, що працює в Інтернеті, дозволяє зловмиснику підвищити рівень своїх привілеїв з анонімного до локального користувача (або будь-який обліковий запис, на якому розміщено вразливий компонент).

Зрозуміло, що це лише приблизна класифікація загроз (не вразливості). І багато з них не є актуальними за будь-яких обставин. Наприклад, якщо наш компонент схожий на PlaySound, нам не потрібно турбуватися про загрози розкриття інформації для потоків даних між програмою та PlaySound. З іншого боку, якщо ми пишемо сервер електронної пошти, ми абсолютно точно дбаєте про загрози розкриття інформації.

Різні елементи IoT системи схильні до різних загроз STRIDE:

процеси схильні до загроз STRIDE;

потоки даних - загрозам TID;

сховища даних схильні до загроз TID, а іноді і R, якщо дані зберігаються у файлах журналів;

зовнішні сутності схильні до загроз SRD.

Перед підключеними спеціалізованими пристроями відкривається велика кількість можливих зон та шаблонів взаємодії, які необхідно врахувати під час створення інфраструктури безпеки цифрового доступу до

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						46
Змн.	Арк.	№ докум.	Підпис	Дата		

цих пристроїв. Тут термін "цифровий доступ" використовується, щоб відрізнити відповідні операції від тих, що виконуються при прямій взаємодії з пристроєм, коли безпека забезпечується за рахунок фізичного контролю доступу. Наприклад, пристрій знаходиться в кімнаті, двері якої зачинені на замок. Хоча фізичний доступ не можна заборонити за допомогою програмного забезпечення та обладнання, можна вжити заходів, щоб запобігти такому доступу та зменшити ймовірність втручання в інтерфейс системи.

Щоб оптимально використовувати рекомендації щодо безпеки, рекомендується розділити типову архітектуру Інтернету речей на кілька компонентів або зон у рамках моделювання ризиків. Ці зони включають:

- пристрій;
- польовий шлюз;
- хмарні шлюзи;
- додатки.

Поділ на зони - всеосяжний спосіб сегментації рішення. Найчастіше в кожній зоні містяться окремі дані, а також є вимоги до автентифікації та авторизації. За допомогою зони можна ізолювати пошкодження та обмежити вплив зон із низьким рівнем довіри на ті, рівень довіри до яких вищий.

Усі зони поділяються межами довіри. На схемі рис. 2.3 вони позначені червоною пунктирною лінією. Тут зображено перехід даних або даних з одного джерела до іншого. Під час цього переходу дані можуть наражатися на різні загрози STRIDE.

Компоненти в межах кожного кордону також схильні до загроз STRIDE, що дозволяє отримати всеосяжну модель ризиків для вирішення.

Розглянемо стандартні компоненти, які зазвичай знаходяться в цих зонах.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

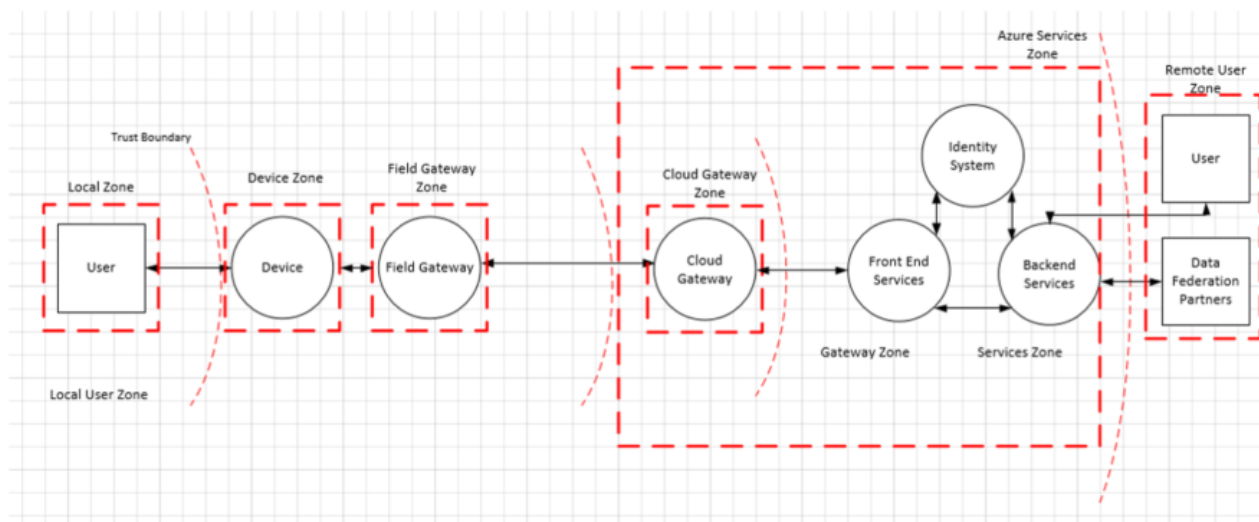


Рисунок 2.3 – Схема еталонної архітектури моделі

Зона пристрою. Середовище пристрою — це фізичний простір навколо пристрою, в межах якого можна отримати фізичний доступ і/або цифровий доступ через однорангову локальну мережу. Під локальною мережею мається на увазі унікально ідентифікована ізольована від загального доступу з Інтернету мережа, до якої можна встановити мережний міст. Нею може бути будь-яка технологія бездротового радіозв'язку ближньої дії, що дозволяє здійснювати одноранговий обмін даними між пристроями. Нею не може бути технологія мережної віртуалізації, яка створює ілюзію локальної мережі, або загальнодоступні операторські мережі, в яких для однорангового обміну даними потрібні два пристрої, що взаємодіють у просторі загальнодоступної мережі.

Зона польового шлюзу. Польовий шлюз — це пристрій, програмне забезпечення або серверне програмне забезпечення загального призначення, яке є засобом реалізації обміну даними, а також, по можливості, системою управління пристроями та центром обробки даних, що отримуються від пристроїв. У зоні польового шлюзу знаходиться сам польовий шлюз та всі підключені до нього пристрої. Як видно із назви, польові шлюзи не використовують виділені засоби обробки даних. Зазвичай вони прив'язані до розташування і можуть зазнавати фізичних атак, а їх оперативна надмірність

обмежена. Простіше кажучи, польовий шлюз - зазвичай саме той об'єкт, на який можуть вплинути або можуть атакувати, так як відомі його функції.

Польовий шлюз відрізняється від звичайного маршрутизатора трафіку тим, що йому відведено активну роль в управлінні доступом та передачею інформації. Це означає, що він є об'єктом, орієнтованим на додатки, а також терміналом мережевих підключень або сеансів. Пристрої перетворення мережевих адрес і брандмауери, навпаки, не можуть вважатися польовими шлюзами, оскільки вони є явними терміналами підключень чи сеансів. Вони просто маршрутизують (або блокують) підключення чи сеанси, що здійснюються через них. Польовий шлюз має дві окремі контактні зони. Одна з них є внутрішньою частиною зони і взаємодіє з пристроями, підключеними до шлюзу. Інша ж є межею зони і взаємодіє з усіма сторонніми підключеннями.

Зона хмарного шлюзу. Хмарний шлюз — це система, яка забезпечує віддалений обмін даними між пристроями або польовими шлюзами з різних сайтів через простір загальнодоступної мережі. Зазвичай дані передаються у хмарну систему управління та аналізу даних або федерацію таких систем. У деяких випадках хмарний шлюз дозволяє негайно отримати доступ до спеціалізованих пристроїв за допомогою таких терміналів, як планшети або телефони. У цьому контексті «хмара» — виділена система обробки даних, не прив'язана до сайту, що підключені пристрої або польові шлюзи. Крім того, в зоні «хмари» операційні заходи запобігають цільовому фізичному доступу і не завжди доступні в інфраструктурі загальнодоступної хмари.

Хмарний шлюз можна порівняти з накладанням віртуалізації мережі, щоб ізолювати трафік цього шлюзу та всіх пристроїв або польових шлюзів, підключених до нього від мережевого трафіку. Сам хмарний шлюз не є системою керування пристроями чи засобом обробки чи зберігання даних пристроїв. Ці засоби лише взаємодіють із ним. Зона хмарного шлюзу включає сам хмарний шлюз і всі польові шлюзи і пристрої, прямо або

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						49
Змн.	Арк.	№ докум.	Підпис	Дата		

опосередковано підключені до нього. Кордон зони — це окрема контактна зона, з якою взаємодіють всі зовнішні сторони.

Зони служб. У цьому контексті служба – це будь-який програмний компонент або модуль, який взаємодіє з пристроями через польовий або хмарний шлюз, щоб збирати та аналізувати дані, а також забезпечувати управління та контроль. Служби є посередниками. Вони використовують свої посвідчення, щоб взаємодіяти зі шлюзами та іншими підсистемами, зберігають та аналізують дані, автономно виконують команди на пристроях на основі аналізу даних або розкладів, а також надають авторизованим користувачам відомості та можливості керування.

Інформаційні та спеціалізовані пристрої. ПК, телефони та планшети – переважно інтерактивні інформаційні пристрої. Телефони та планшети оптимізовані для збільшення часу роботи від батареї. Вони частково переходять у режим сну, якщо людина не використовує пристрій або такі функції, як відтворення музики або навігація. З погляду системи люди використовують ці інформаційно-технологічні пристрої переважно як проксі. Вони є діючими пристроями, що пропонують дії, та датчиками, які збирають вхідні дані.

Спеціалізовані пристрої (прості датчики температури або складні фабричні вироби), що складаються з тисяч компонентів, мають зовсім інший характер. Це пристрої більш вузького призначення, і навіть за наявності інтерфейсу вони більше орієнтовані на взаємодію з фізичними ресурсами або інтеграцію в них. Вони вимірюють дані навколишнього середовища та створюють звіти про них, включають клапани, контролюють роботу сервосистеми, подають звукові сигнали, перемикають індикатори та виконують безліч інших завдань. Вони дозволяють виконувати ту роботу, для якої інформаційні пристрої надто дорогі, великі, неміцні або не надають необхідні функції. Конкретні цілі застосування дозволяють відразу ж визначити їхню технічну структуру, а доступний бюджет — обсяг роботи та запланований час експлуатації. Разом ці два ключові фактори обмежують

місце і бюджет на споживану енергію, а тому зменшують можливості зберігання, обчислення та забезпечення безпеки.

Проблема з автоматично або віддалено керованими пристроями, наприклад фізичний дефект або помилка в логіці управління, може спричинити навмисне несанкціоноване вторгнення та зміну. Це може знищити партії виробів, спричинити розграбування будівлі або пожежу, а для людей — травми або навіть смерть. Цей тип збитків кардинально відрізняється від перевищення ліміту на вкраденій кредитній картці. Засоби безпеки пристроїв управління, а також для датчиків, які можуть ініціювати команди управління, повинні бути кращими, ніж у будь-якому комерційному чи банківському сценарії.

Взаємодія контролю пристрою та даних пристрою

Перед підключеними спеціалізованими пристроями відкривається велика кількість можливих зон та шаблонів взаємодії, які необхідно врахувати під час створення інфраструктури безпеки цифрового доступу до цих пристроїв. Тут термін "цифровий доступ" використовується, щоб відрізнити відповідні операції від тих, що виконуються при прямій взаємодії з пристроєм, коли безпека забезпечується за рахунок фізичного контролю доступу. Наприклад, пристрій знаходиться в кімнаті, двері якої зачинені на замок. Хоча фізичний доступ не можна заборонити за допомогою програмного забезпечення та обладнання, можна вжити заходів, щоб запобігти такому доступу та зменшити ймовірність втручання в інтерфейс системи.

Досліджуючи шаблони взаємодії, в рамках моделювання приділяється однакова увага контролю пристрою та даних пристрою. Контроль пристрою можна класифікувати як введення будь-яких відомостей, наданих пристрою будь-якою стороною, щоб змінити його поведінку або вплинути на нього, а саме на його стан або стан його середовища. Дані пристроїв можна класифікувати як будь-які відомості про його стан і стан його середовища, які пристрій надає іншій стороні.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		51

2.3. Розробка функціональної схеми IoT-системи котеджу

Проведемо розробку функціональної схеми IoT-системи котеджу. Для цього скористаємося розробленою в підрозділі 2.1 структурною схемою системи та врахуємо особливості моделі запропонованої в підрозділі 2.2.

Типові набори датчиків та виконавчих пристроїв підсистем освітлення, охорони та безпеки розмістимо у кожній кімнаті. Додаткових елементів потребують кухня та гараж, для якого необхідно мати специфічні пристрої (рис. 2.4). Ці елементи та відносяться до зони довіри пристроїв.

Для підвищення рівня безпеки та універсалізації проект розробляється з використанням хмарного середовища Azure. Це дозволить скористатися безпечною еталонною архітектурою Інтернету речей Azure та засобами моделювання ризиків Microsoft. При цьому Система управління IoT у вигляді панелі буде розміщуватися в самому котеджі у вигляді панелі управління, а доступ до неї можна буде здійснити з будь-якого авторизованого пристрою через хмарне середовище.

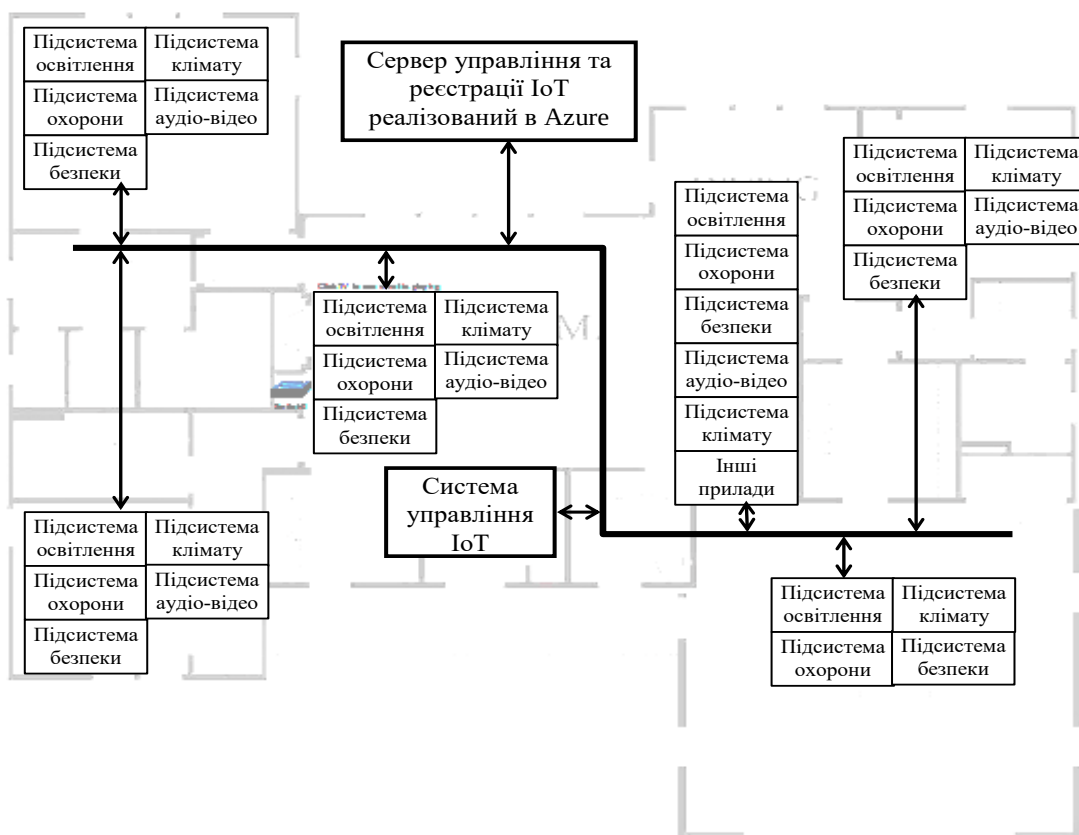


Рисунок 2.4 – Функціональна схема IoT-системи котеджу

Сервер управління та реєстрації IoT реалізується як віртуальний сервер у хмарному середовищі Azure. На сервері створюються облікові записи та віртуальні двійники для контролю за всіма елементами в різних приміщеннях житлового будинку. Кожен підключаємий елемент повинен мати цифровий сертифікат довіри.

У якості кінцевих та проміжних пристроїв можуть використовуватись пристрої будь-якого виробника, якщо вони відповідають вимогам підключення до хмарного середовища Azure. Наприклад, у таблиці 2.1 наведені зображення найпоширеніших компонентів розумного будинку Smart Bus [7].

Для моделювання реальних пристроїв будемо використовувати програмні моделі пристроїв Cisco Packet Tracer, які максимально наближені до реально існуючих аналогів.

В симуляторі Cisco Packet Tracer один IoT-пристрій може бути підключений лише до одного облікового запису, тому керувати одним пристроєм через Local Control або Remote Control можна тільки з одного облікового запису. Відповідно працівники даного об'єкту мають доступ до облікових записів відповідно до прав, які може встановити адміністратор.

Таким чином, розроблено функціональну схему системи, яка ґрунтується на прив'язці до плану будинку та розділена на зони довіри відповідно до моделі ризиків IoT Azure.

2.4. Моделювання ризиків для IoT-системи котеджу та розробка рекомендацій по їх усуненню

Для моделювання будемо використовувати платформу для створення моделей ризиків для Інтернету речей Azure корпорації Майкрософт []. У цьому розділі використовується функціональна схема IoT системи котеджу

Керовані пристрої

Керуючі пристрої

Датчики



ШЛЮЗИ ЗВ'ЯЗКУ

приведена до еталонної архітектури Інтернету речей Azure, щоб провести моделювання ризиків для Інтернету речей, а також усунути знайдені загрози (рис.2.5). Виділено чотири основні області, на яких слід зосередитись: пристрої та джерела даних; передача даних; обробка пристроїв та подій; рівень подання.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		54

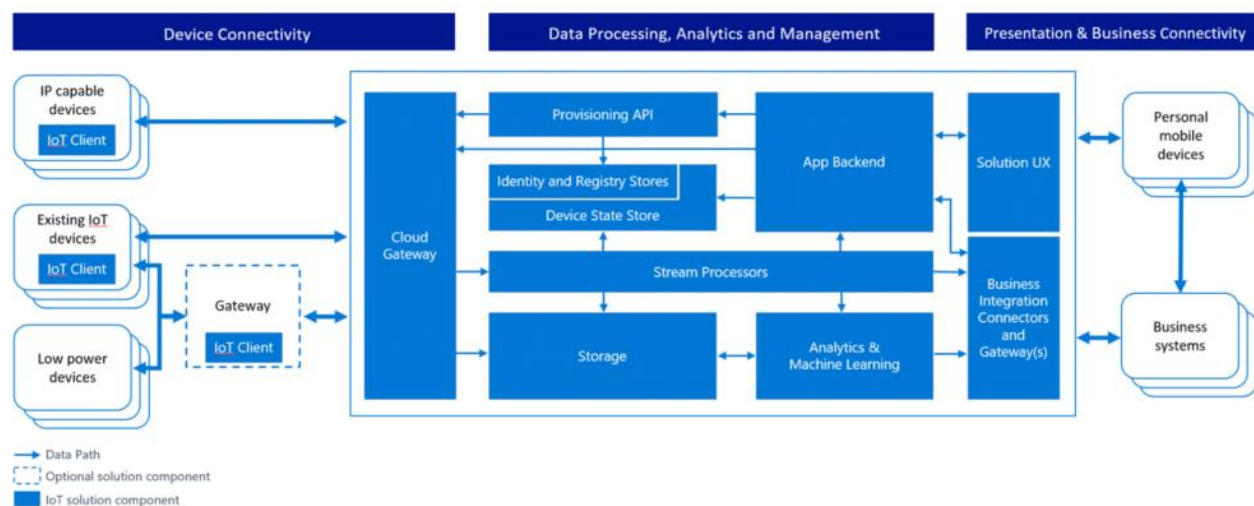


Рисунок 2.5 – Схема моделювання загроз для Azure IoT

Будемо використовувати програмне забезпечення Майкрософт для моделювання ризиків - Microsoft Threat Modeling Tool.

Спрощене представлення архітектури Інтернету речей Майкрософт зі схемою потоків даних, моделлю подано на рис. 2.6.

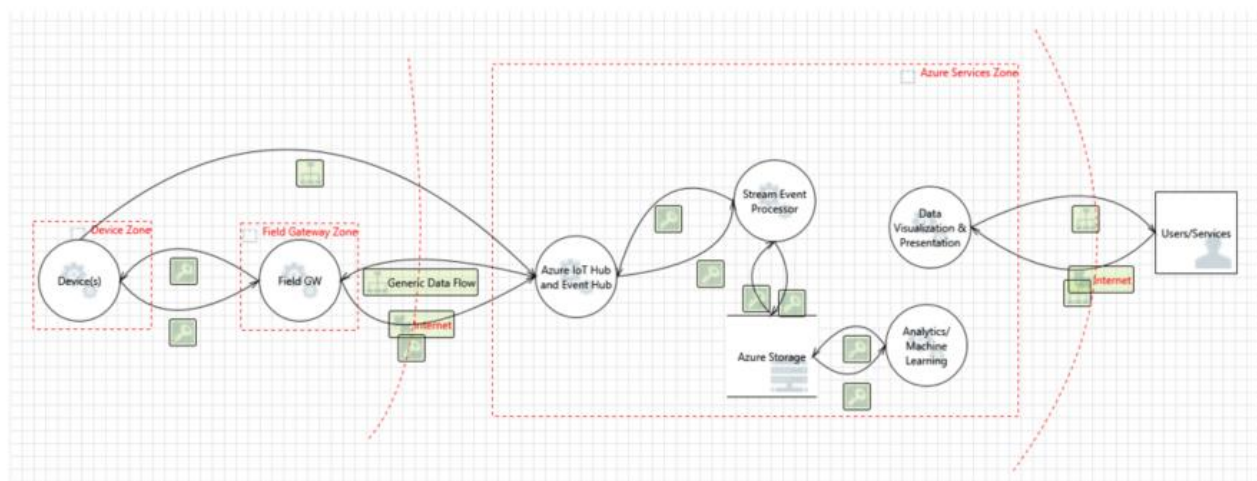


Рисунок 2.6 – Модель для моделювання загроз проекту IoT системи з використанням MS Threat Modeling Tool

Слід зазначити, що у цій архітектурі розділені можливості шлюзу та пристроїв. Такий підхід дозволяє користувачеві використовувати більш безпечні пристрої шлюзу: вони можуть взаємодіяти з хмарним шлюзом за допомогою захищених протоколів, що зазвичай потребує більшого обсягу

обробки, ніж може надати власне пристрій. Передбачається, що у зоні служб Azure хмарний шлюз представлений службою Центру Інтернету речей Azure.

Докладно розглянемо моделювання ризиків раніше розробленої архітектури та наведемо загальні відомості про те, як усунути деякі характерні проблеми. Розглянемо такі основні елементи моделі ризиків:

процеси (підконтрольні та зовнішні);

взаємодія (або потоки даних);

зберігання (або сховища даних).

Процеси. У таблиці 2.2 наведено огляд найпоширеніших ризиків для категорії *процесів* та опис кращих способів їх усунення. Нижче прийняті такі позначення: Спуфінг (Spoofing, далі "S"), Відмова в обслуговуванні (Denial of Service, далі "D"). Незаконна зміна (Tampering, далі "T"). Розкриття інформації (Information Disclosure, далі "I"). Несанкціоноване підвищення привілеїв (Information Disclosure, далі "E").

Таблиця 2.2

Загрози процесам та способи їх усунення

Компонент	Загроза	Виправлення	Ризик	Реалізація
Пристрій	S	Призначити посвідчення пристрою та перевіряти його справжність	Заміна пристрою або його частини іншим пристроєм. Як дізнатися, який із пристроїв справжній?	Перевірка автентичності пристрою за допомогою протоколу TLS або IPSec. Інфраструктура повинна підтримувати спільні ключі для пристроїв, які не виконують повне асиметричне шифрування. Використання Azure AD, OAuth
	TRID	Застосуйте механізми захисту від незаконної зміни до пристрою, щоб запобігти видаленню ключів та інших криптографічних матеріалів з пристрою.	Хтось може незаконно змінити пристрій (фізично втрутитися). Потрібно переконатись, що пристрій не змінили незаконним чином.	Усунути ризики найефективніше дозволяє довірений платформний модуль. Він дозволяє зберігати ключі на спеціальній вбудованій схемі, з якої не можна зчитати ключі, але їх можна використовувати тільки в криптографічних операціях, які передбачають використання ключів без розкриття. Шифрування пам'яті пристрою. Керування ключами пристрою. Підписування коду
	E	Забезпечити контроль	Якщо пристрій дозволяє вико-	Реалізація схеми авторизації для пристрою

Компонент	Загроза	Виправлення	Ризик	Реалізація
		доступу до пристрою. Застосувати схему авторизації	нувати окремі дії за допомогою команд із зовнішнього джерела або навіть зі скомпрометованого датчика, при атаці він дозволяє виконувати операції, які недоступні за інших обставин.	
Польовий шлюз	S	Забезпечити автентифікацію польового шлюзу при доступі до хмарного шлюзу (наприклад, на основі сертифікатів, загальних ключів або тверджень).	Якщо хтось може підробити дані польового шлюзу, він зможе видавати свій пристрій за будь-який інший	TLS RSA/PSK, IPSec, RFC 4279. Щодо тих самих основних проблем зберігання та забезпечення відповідності пристроїв у цілому найкраще рішення – використовувати довірений платформний модуль. Використання розширення 6LowPAN для IPSec, щоб забезпечити підтримку мереж бездротових датчиків
	TRID	Захист поля шлюзу від заміни (TPM)	Якщо спуфінгу, спрямованому на польовий шлюз, зазнає хмарний шлюз, це може спричинити розкриття інформації та незаконну зміну даних	Шифрування пам'яті, довірені платформні модулі, автентифікація
	E	Реалізувати механізм контролю доступу для польового шлюзу		

Приклади загроз, які можуть бути в цій категорії.

Спуфінг. Зловмисник може витягти матеріал криптографічного ключа з пристрою, обладнання або програмного забезпечення, а потім отримати доступ до системи за допомогою іншого фізичного або віртуального пристрою, використовуючи посвідчення пристрою, з якого викрав матеріал.

Відмова у обслуговуванні. Пристрій може бути розпізнаний як непрацездатний або нездатний обмінюватися даними через радіочастотні перешкоди або тому, що обрізані дроти. Наприклад, камера відеоспостереження, живлення або підключення якої навмисно вивели з ладу, не може передавати дані.

Незаконна зміна. Зловмисник може частково або повністю замінити програмне забезпечення, яке працює на пристрої, щоб програмне забезпечення могло використовувати посвідчення справжності пристрою, якщо матеріал ключа або засоби шифрування, в яких є матеріали ключів, доступні несанкціонованій програмі.

Незаконна зміна. Щоб камера відеоспостереження не зняла зловмисника, він може налаштувати як показ картинки фотографію порожнього коридору. Димовий або пожежний датчик може передати дані про спалах, якщо хтось тримає біля нього увімкнену запальничку. В обох випадках пристрої повністю технічно справні, але повідомлятимуть системі відомості, отримані в результаті змін.

Незаконна зміна. Зловмисник може використовувати отриманий матеріал ключа, щоб перехопити або вилучити дані з пристрою під час передачі та замінити їх на помилкові дані, а значить аутентифікуватись, використовуючи вкрадений матеріал ключа.

Розкриття інформації. Якщо на пристрої працює змінене програмне забезпечення, можливий витік даних стороннім особам.

Розкриття інформації. Зловмисник може використовувати отриманий матеріал ключа, щоб втрутитися в обмін даними між пристроєм і контролером, польовим або хмарним шлюзом, а потім отримувати інформацію.

Відмова у обслуговуванні. Пристрій може бути вимкнений або увімкнений у режимі, в якому неможливо підтримувати зв'язок (це можуть робити навмисно з багатьма пристроями).

Незаконна зміна. Для пристрою можуть налаштувати інший невідомий системі керування стан (параметри, які не відносяться до еталонних), через що пристрій передаватиме дані, які можна неправильно інтерпретувати.

Несанкціоноване підвищення привілеїв. Це випадок, коли пристрій, який виконує певну функцію, використовується для примусового виконання інших дій. Наприклад, клапан, запрограмований відкриватися наполовину, можуть налаштувати повністю закриватися.

Спуфінг, незаконна зміна даних та відмова. За відсутності захисту (він рідко використовується у споживчих пультах дистанційного керування) зломисник може анонімно змінювати стан пристрою. Хороший приклад: за допомогою пультів дистанційного керування можна увімкнути будь-який телевізор, тому їх часто використовують, щоб пожартувати з когось.

Зв'язок. Тут описані загрози, пов'язані з шляхом обміну даними між пристроями, пристроями та польовими або хмарними шлюзами. У таблиці 2.3 наведено рекомендації щодо використання відкритих портів пристроїв або VPN.

Таблиця 2.3

Загрози зв'язку та способи їх усунення

Компонент	Загроза	Виправлення	Ризик	Реалізація
Пристрій - Центр Інтернету речей	TID	Від D використовувати TLS (для загальних ключів або RSA), щоб шифрувати трафік	Перехоплення даних обміну між пристроєм і шлюзом або втручання в обмін	Забезпечення безпеки на рівні протоколу. При використанні протоколів користувача потрібно з'ясувати, як забезпечити відповідний захист. У більшості випадків пристрій надсилає дані до Центру Інтернету речей (ініціює підключення).
Пристрій — пристрій	TID	Від D використовувати TLS (для загальних ключів або RSA), щоб шифрувати трафік	Зчитування даних при їх передачі між пристроями. Незаконна зміна даних. Перевантаження пристрою новими підключеннями	Безпека на рівні протоколу (HTTP, HTTPS, AMQP, MQTT або CoAP). При використанні протоколів користувача потрібно з'ясувати, як забезпечити відповідний захист. Щоб усунути ризик атаки типу "відмова в обслуговуванні", потрібно встановлювати однорангові підключення пристроїв через польовий або хмарний шлюз,

Компонент	Загроза	Виправлення	Ризик	Реалізація
				щоб вони працювали як клієнти по відношенню до мережі. Піринг може спричинити створення прямого підключення між одноранговими вузлами через шлюз
Зовнішня сутність - пристрій	TID	Надійне підключення зовнішньої сутності до пристрою	Перехоплення підключення до пристрою. Втручання в обмін даними з пристроєм	Забезпечити безпечне підключення зовнішньої сутності до пристрою за допомогою технології Bluetooth з низьким енергоспоживанням або NFC. Забезпечити контроль робочої панелі пристрою (фізичний)
Польовий шлюз - хмарний шлюз	TID	Використовувати TLS (для загальних ключів або RSA), щоб шифрувати трафік	Перехоплення даних обміну між пристроєм та шлюзом або втручання в обмін	Забезпечення безпеки на рівні протоколу (HTTP, HTTPS, AMQP, MQTT або CoAP). При використанні протоколів користувача потрібно з'ясувати, як забезпечити відповідний захист.
Пристрій - хмарний шлюз	TID	Використовувати TLS (для загальних ключів або RSA), щоб шифрувати трафік	Перехоплення даних обміну між пристроєм та шлюзом або втручання в обмін	Забезпечення безпеки на рівні протоколу (HTTP, HTTPS, AMQP, MQTT або CoAP). При використанні протоколів користувача потрібно з'ясувати, як забезпечити відповідний захист.

Нижче наведено деякі приклади загроз, які можуть бути в цій категорії.

Відмова у обслуговуванні. Пристрої з обмеженими функціями зазвичай схильні до загрози атаки типу "відмова в обслуговуванні", якщо активно прослуховують вхідні підключення або небажані датаграми в мережі, оскільки зловмисник може відкрити багато паралельних підключень, не обслуговувати їх або обслуговувати повільно або пристрій може бути перевантажено небажаним трафіком. В обох випадках мережа може розпізнати пристрій як непрацездатний.

Спуфінг, розкриття інформації. Пристрої з обмеженими функціями та спеціалізовані пристрої часто використовують загальні засоби захисту, такі як пароль або PIN-код, або повністю покладаються на довірену мережу. Це означає, що вони надають доступ до даних пристроїв у тій самій мережі, яка часто захищена лише спільним ключем. Отже, при розкритті загального

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		60

секрету пристрою або мережі можна буде керувати цим пристроєм або переглядати дані, які він надсилає.

Підміна: зловмисник може перехопити або частково перевизначити мовлення та підміну ініціатора.

Незаконна зміна. Зловмисник може перехопити або частково перевизначити мовлення та надіслати неправдиві відомості.

Відмова у обслуговуванні. Зловмисник може порушити широкомовний сигнал та відхилити поширення інформації.

Пам'ять (зберігання). Кожен пристрій і польовий шлюз має певну форму сховища (місце тимчасового зберігання черг даних або образів операційних систем). У таблиці 2.4 подані рекомендації щодо зберігання даних.

Таблиця 2.4

Загрози зберігання та способи їх усунення

Компонент	Загроза	Виправлення	Ризик	Реалізація
Сховище пристрою	TRID	Шифрування сховища, підписування журналів	Читання (особистих) даних із сховища, незаконна зміна даних телеметрії. Незаконна зміна даних управління командами, які перебувають у черзі чи кеші. Незаконна зміна пакетів оновлення конфігурації або вбудованого програмного забезпечення, які є в локальній черзі або локальному кеші, може призвести до компрометації операційної системи або її компонентів.	Шифрування, використання коду автентифікації повідомлення або цифрових підписів. Забезпечення суворого контролю доступу до ресурсів за допомогою списків керування доступом (ACL) або дозволів
Образ ОС пристрою	TRID		Незаконна зміна ОС або заміна її компонентів	Секціонування ОС лише для читання, підписування образів ОС, шифрування
Сховище польового шлюзу (для зберігання черг)	TRID	Шифрування сховища, підписування журналів	Читання (особистих) даних зі сховища, незаконна зміна даних телеметрії, а також даних управління командами, що знаходяться у черзі чи кеші. Незаконна зміна пакетів оновлення конфігурації або вбудованого програмного забезпечення (призначених для	BitLocker

Компонент	Загроза	Виправлення	Ризик	Реалізація
даних)			пристроїв або польового шлюзу), які є в локальній черзі або локальному кеші, може призвести до компрометації операційної системи або її компонентів.	
Образ ОС польового шлюзу	TRID		Незаконна зміна ОС або заміна її компонентів	Секціонування ОС лише для читання, підписування образів ОС, шифрування

Обробка пристроїв та подій. Зона хмарного шлюзу

Хмарний шлюз — це система, яка забезпечує віддалений обмін даними між пристроями або польовими шлюзами з різних сайтів через простір загальнодоступної мережі. Зазвичай дані передаються у хмарну систему управління та аналізу даних або федерацію таких систем. У деяких випадках хмарний шлюз дозволяє негайно отримати доступ до спеціалізованих пристроїв за допомогою таких терміналів, як планшети або телефони. У цьому контексті під хмарою мається на увазі виділена система обробки даних, неприв'язана до того ж сайту, що підключені пристрої або польові шлюзи. У хмарі операційні вимірювання запобігають цільовому фізичному доступу і не завжди доступні в інфраструктурі загальнодоступної хмари. Хмарний шлюз можна порівняти з накладанням віртуалізації мережі, щоб ізолювати трафік цього шлюзу та всіх пристроїв або польових шлюзів, підключених до нього від мережевого трафіку. Сам хмарний шлюз не є системою керування пристроями чи засобом обробки чи зберігання даних пристроїв. Ці засоби лише взаємодіють із ним. Зона хмарного шлюзу включає сам хмарний шлюз і всі польові шлюзи і пристрої, прямо або опосередковано підключені до нього.

Хмарний шлюз — це компонент програмного забезпечення, що розробляється користувачами, який працює як служба і надає кінцеві точки для підключення пристроїв і польового шлюзу. Отже, під час його розробки

потрібно спланувати систему безпеки. Під час розробки та створення цієї служби необхідно дотримуватись відповідної процедури для SDL.

Зона служб.

Система контролю (або контролер) — це програмне рішення, яке взаємодіє з пристроєм, польовим або хмарним шлюзом, щоб контролювати один або кілька пристроїв, збирати, зберігати та/або аналізувати їх дані. Вона дозволяє використовувати результати, щоб сформулювати уявлення, або подальшого контролю. Це єдина сутність у цьому обговоренні, яка дає змогу негайно отримати доступ для взаємодії з користувачами. Винятки є проміжні фізичні зони контролю на пристроях, такі як вимикачі. Вони дозволяють вимикати пристрої та змінювати властивості. Іншого такого функціонального пристрою, до якого можна отримати цифровий доступ, немає.

Проміжні фізичні зони контролю — це області, в яких логіки регулювання обмежують функції фізичної зони контролю, щоб запобігти віддаленому керуванню еквівалентними функціями або конфліктам віддаленого введення. Ці проміжні зони по суті підключаються до локальної системи управління, яка використовує ті ж самі базові функції, що будь-яка інша система віддаленого управління, до якої пристрій може бути підключений паралельно.

Висновки по 2 розділу

Розроблена структурна схема IoT системи котеджу орієнтована на розподіл пристроїв по підгрупах та розміщення відповідно до плану котеджу.

При проектуванні систем IoT для забезпечення безпеки важливо правильно змодельовати ризики, щоб виробити рекомендації для їх усунення.

Функціональна схема IoT системи котеджу включає зони пристроїв, зони польового шлюзу та зону хмарного шлюзу. Реалізацію проекту пропонується виконати з використанням хмарного середовища Azure.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		63

РОЗДІЛ 3. ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ТА ЕФЕКТИВНОСТІ ПРИЙНЯТИХ РІШЕНЬ

3.1. Розробка моделі IoT-системи котеджу за допомогою Cisco Packet Tracer

Відповідно до розроблених структурної і функціональної схем та моделі загроз, розробимо програмно-імітаційну модель IoT-системи котеджу за допомогою Cisco Packet Tracer. Використовуючи його можливості проведемо моделювання підключення будинку до всесвітньої мережі Інтернет та хмарного середовища Azure. Для цього здійснимо підключення через модулі ISP Connection до ISP Internet (рис.3.1) [22].

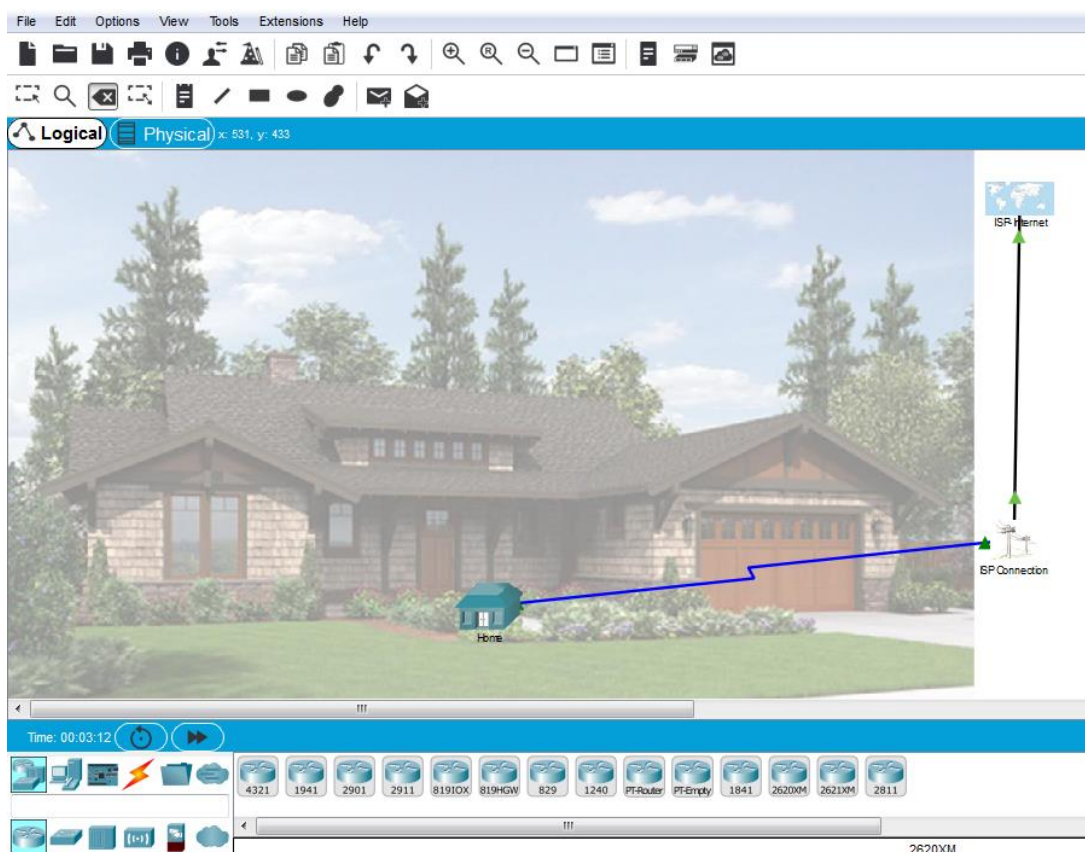


Рисунок 3.1 – Моделювання підключення котеджу до ISP Internet

Скористаємось готовою моделлю ISP Internet. Якщо її відкрити, то побачимо імітацію світового з'єднання (рис.3.2 та додаток В).

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		64

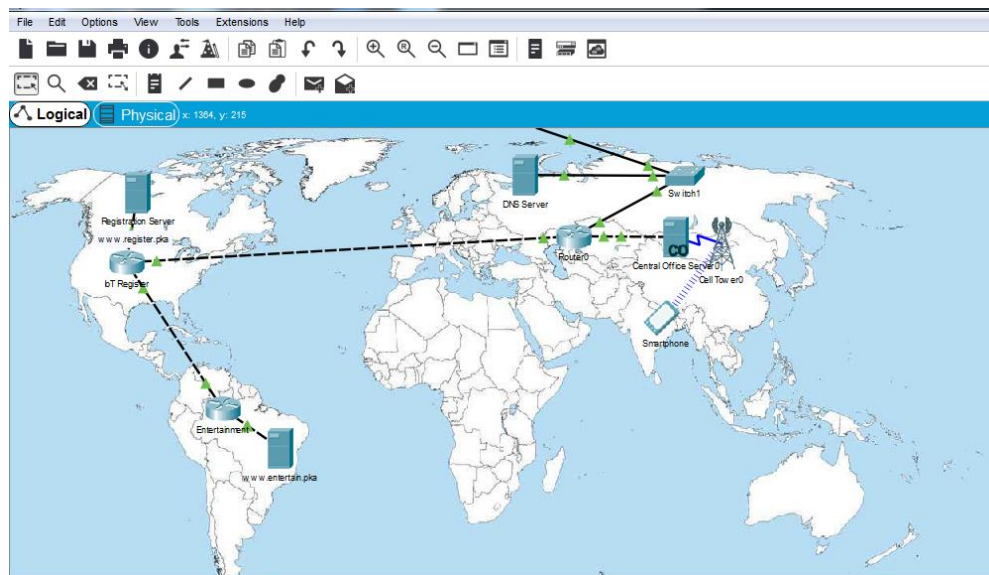


Рисунок 3.2 – Розгортання моделі ISP Internet

Розгортання IoT мережі будинку сплануємо у вигляді окремого кластеру. У якості польового шлюзу у нашій моделі буде виступати пристрій Home Gateway.

Налаштування польового шлюзу Home Gateway. Необхідно натиснути Home, щоб розгорнути кластер. Далі встановлюємо та налаштовуємо Home Gateway. Переходимо на вкладку Config. Натискаємо Інтернет (Internet). Обираємо DHCP для конфігурації IP. Натискаємо Wireless. Вводимо MyHomeGateway як SSID. Виберіть WPA2-PSK як автентифікацію. Вводимо як пароль PSK – CiscoIoT [23].

Встановлюємо Домашній ПК (Home PC). Натискаємо його Робочий стіл (Desktop). Натискаємо IP Configuration. Обираємо DHCP для конфігурації IP.

Перевіряємо підключення домашнього шлюзу до сервера реєстрації.

а) З домашнього ПК Вводимо `www.register.pka` в веб-браузері. Вводимо ім'я адміністратора `admin` пароль `admin` для входу на сервер дистанційної реєстрації. Це може зайняти кілька хвилин, поки всі пристрої IoT будуть перераховані.

З домашнього ПК (Home PC) Вводимо `192.168.25.1` у веб-браузері. Вводимо `admin` як ім'я адміністратора та як пароль для входу в локальний сервер IoT, розміщений на домашньому шлюзі Home Gateway.

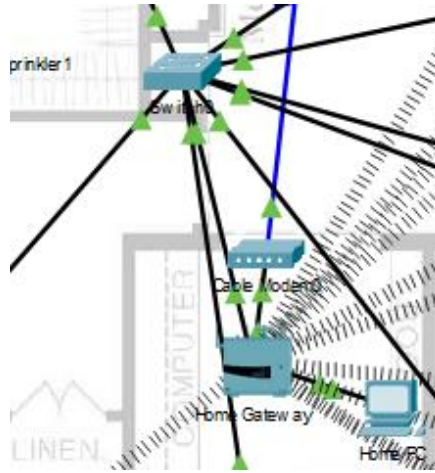


Рисунок 3.3 – Розгортання системи управління IoT котеджу

В Cisco Packet Tracer пристрої IoT мають три види взаємодії: Direct Control (прямий контроль); Local Control (локальний контроль); Remote Control (віддалений контроль).

Direct Control реалізований безпосередньою взаємодією з об'єктом. Local Control використовується за допомогою управління компонентами за допомогою MCU/SBC або через підключення до серверу. Сервер має знаходитись в одній IP-мережі з IoT-пристроєм. Remote Control використовується для підключення та управління пристроєм, який знаходиться в іншій IP-мережі. Оскільки в Cisco Packet Tracer обмежена взаємодія з пристроями IoT з використанням Remote Control, то було обрано взаємодію через Local Control.

Моделювання зони пристроїв.

Двері та вікна IoT. Двері та вікна будинку під'єднуються до комутатора Cisco 2960, який в свою чергу під'єднаний до сервера реєстрації IoT. У підсистемі для управління вікнами та дверима використовується Local Control без MCU/SBC. IoT вікна та двері використовуються в протипожежній системі. Через сервер реєстрації IoT також можна управляти вікнами та дверима.

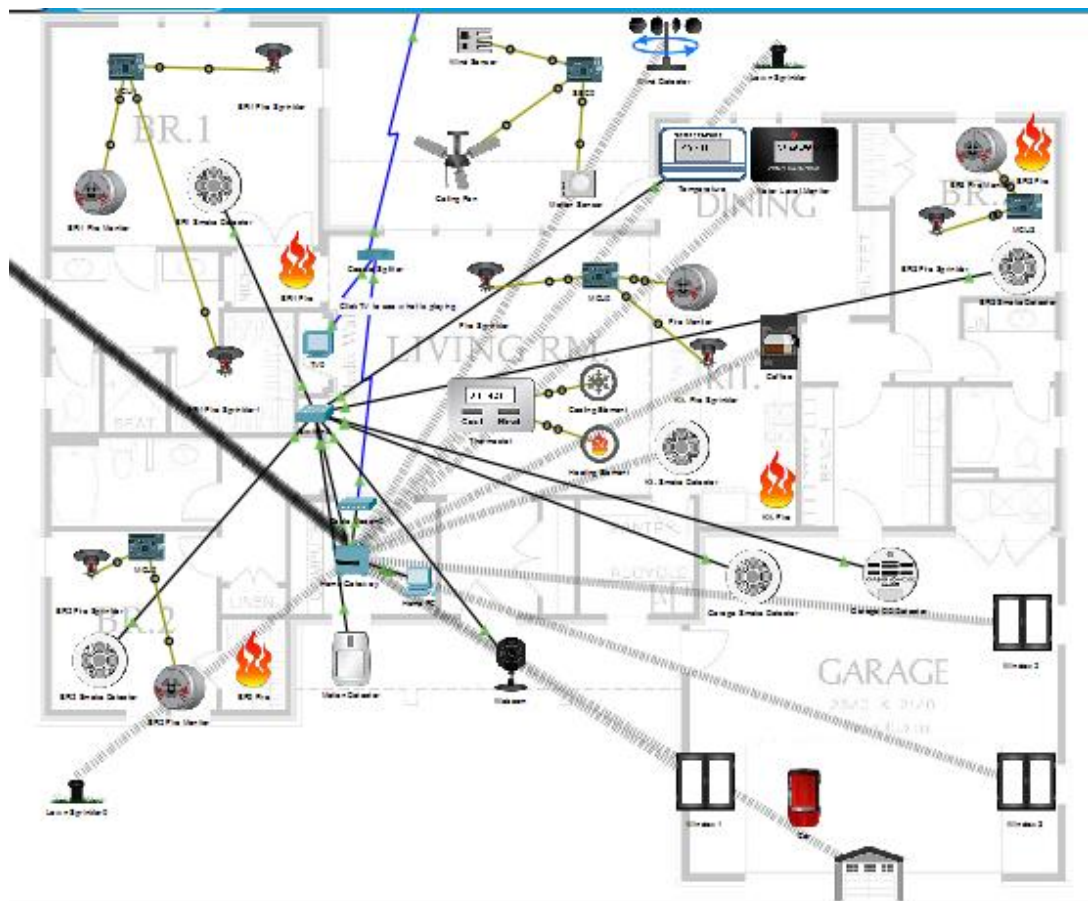


Рисунок 3.4 – Розгортання моделі системи в цілому

Датчики диму входять до протипожежної системи. Датчики передають дані на сервер реєстрації IoT інформацію про рівень задимленості приміщення. Останній вже в свою чергу передає команди управління іншими елементами підсистеми.

Датчики CO та CO₂ входять до протипожежної системи. Датчики передаються інформацію на сервер реєстрації IoT інформацію про рівень CO та CO₂. Останній вже в свою чергу передає команди управління іншим елементами підсистеми.

Термостат входить до системи контролю мікроклімату. Через цифрові входи D1 та D2 до нього можуть під'єднуватися Furnace (нагрівальний елемент) та Air Conditioner (кондиціонер). Термостат може працювати у чотирьох режимах: off (вимкнений); cooling mode (режим охолодження); heating mode (режим нагрівання); auto mode (автоматичний режим).

Управління термостатом доступне як через MCU/SBC, так і через сервер реєстрації (рис.3.5).

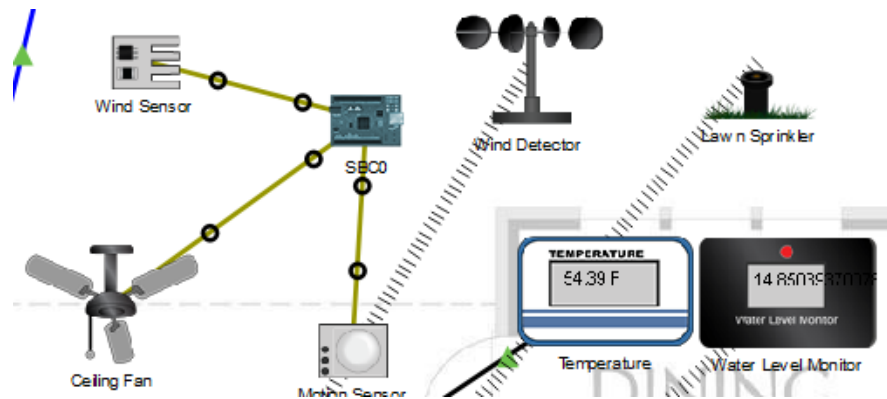


Рисунок 3.5 – Управління вентилятором через термостат

До Smart освітлення входить Photo Sensor (фотодатчик), Light (джерело світлу), MCU та SBC. Photo Sensor приєднаний до SBC, який аналізує дані та відправляє їх на сервер реєстрації IoT. MCU приєднаний до Light і через нього також можна здійснювати контроль елементом, незалежно від сервера реєстрації.

Система контролю вологості повітря включає: Humidity Monitor (датчик вологості), Humidifier (зволожувач повітря), Air Conditioner (кондиціонер). Відповідно датчик вологості аналізує рівень вологості повітря, надсилає дані на сервер реєстрації IoT, та в свою чергу дає команди управління.

Сирени сповіщення та датчики, в яких є вбудовані сирени (рис.3.6). У підсистемі життєзабезпечення виконують роль сповіщення при пожежах чи інших відхиленнях від норм, які задані адміністратором. За необхідності можна налаштувати інші умови спрацювання сповіщень на датчиках та сиренах. Наприклад, сирена може спрацювати на Smoke Detector (датчик диму) та сирена, яка розташована в кімнаті охорони, якщо датчик зафіксує, що рівень диму більше ніж сорок відсотків.



Рисунок 3.6 – Реалізація пожежної сигналізації

До дренажної системи входить Water Level Monitor (датчик рівня води) та Water Drain (стоку). Датчик зчитує рівень води, відправляє дані до серверу реєстрації IoT, на якому налаштовані умови реагування системи.

Живлення IoT-пристроїв можливо реалізувати за допомогою їх підключення до мережевого обладнання з підтримкою PoE/PoE+/UPOE. Power over Ethernet (PoE) — технологія передачі електроенергії за допомогою «витої пари» до периферійних пристроїв, які є елементами мережі Ethernet: пристрої VoIP зв'язку, бездротові мережеві адаптери та точки доступу, веб-камери, тощо [12]. В Cisco Packet Tracer відсутні комутатори з підтримкою PoE/PoE+/UPOE, тому було обрано комутатор Cisco 2960 Catalyst для моделювання.

Для гаража реалізовано систему контролю за наповненням газами та систему відкривання дверей і вікон.

Локальні алгоритми управління реалізовані через проміжні мікроконтролери SBC та MCU. Для них за допомогою мови програмування Python було написано програмне забезпечення.

Реалізувати зону хмарного шлюзу Azure в Cisco Packet Tracer нема можливості, тому тут вона не моделювалась.

3.2. Дослідження моделі IoT-системи котеджу за допомогою Cisco Packet Tracer

Проведемо дослідження працездатності IoT-системи для котеджу по розробленій моделі.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		69

3.2.1. Перевірка керування температурою.

Заходимо з домашнього ПК (Home PC) Вводимо 192.168.25.1 у веб-браузері. Вводимо admin як ім'я адміністратора та як пароль для входу в локальний сервер IoT.

Відкриваємо термостат (Thermostat PTT0810O940).

В даний час термостат (Thermostat) вимкнений. Встановлюємо термостат для автоматичного налаштування потрібної установки.

Розгортаємо панель стану термостату. Натискаємо «Авто». Вводимо потрібну температуру автоматичного нагрівання (61 F) і автоматичного охолодження (86 F) та Натискаємо «Встановити» (Set).

Спостерігаємо за нагрівальним елементом (Heating Element) та охолоджувальним елементом (Cooling Element), коли вони регулюють температуру.

3.2.2. Перевірка стельового вентилятора.

Використовуються такі елементи: Ceiling Fan, Motion Sensor, Wind Sensor, SBC0. Стельовий вентилятор повинен бути налаштований, щоб увімкнути його лише тоді, коли рух було виявлено, а вітер не виявлено. SBC0 з використанням датчиків руху та вітру керує статусом вентилятора. В мікроконтролер SBC0 записуємо програму роботи, що показана на рис. 3.7.

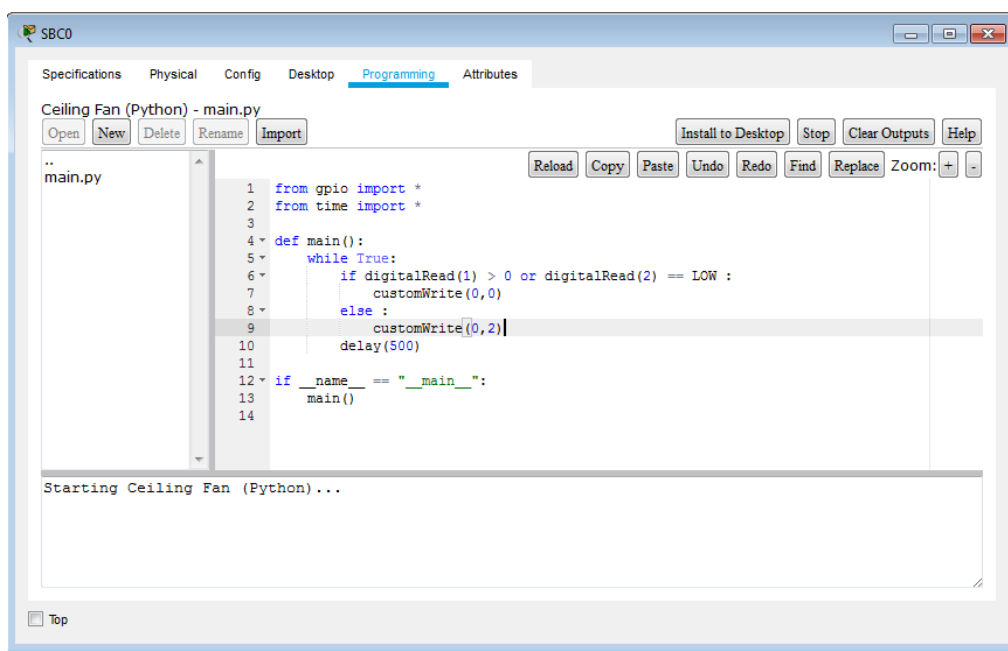


Рисунок 3.7 – Програма роботи мікроконтролера SBC0

Перевіряємо правильність роботи цього блоку.

Натискаємо Alt + Click на датчику руху біля стельового вентилятора. Це дозволить активувати датчик руху. Звертаємо увагу як взаємодіють Wind Detector та Wind Sensor та коли ввімкнувся стельовий вентилятор.

3.2.3. Перевірка поливу газону.

Полив газону може бути дією, що керується умовними виразами, налаштованими на локальному сервері IoT на Home Gateway.

Розгортаємо статус для розбризкувачів води на газоні Lawn Sprinklers, Lawn Sprinklers0 та монітора рівня води Water Level Monitor. Слідкуємо за співвідношенням між рівнем води та станом розбризкувачів.

3.2.4. Автоматизація роботи веб-камери.

Налаштування Веб-камери так, щоб увімкнути її лише тоді, коли спрацював детектор руху. Для цього вводимо відповідні правила (рис. 3.8).

Edit	Remove	Yes	Webcam On	Motion Detector On is true	Set Webcam On to true
Edit	Remove	Yes	Webcam Off	Motion Detector On is false	Set Webcam On to false

Edit Rule

Name Webcam On

Enabled ☒

If:
Match All

+ Condition + Group

Motion Detector On is true

Then set:
Webcam On to true

+ Action

Рисунок 3.8 – Встановлення правил роботи веб-камери на вході

Перевіряємо правильність роботи:

Розгортаємо статус детектора руху (Motion Detector) та веб-камери (Web Camera). Відстежуємо зв'язок між детектором руху та статусом веб-камери.

Натискаємо Alt + Click Motion Detector в топології. Обов'язково натискайте на біля веб-камери.

3.2.5. Перевірка придушення вогню

У кожній спальні та на кухні встановлена система пожежогасіння IoT. У цій демонстрації IoT буде симулюватися вогонь, коли ви знаходитесь далеко

від дому, і ви можете спостерігати за тим, як діє пожежа, використовуючи стан детекторів диму.

Перевіряємо правильність роботи схеми.

Виходимо із Домашнього кластера, натиснувши Назад. Клацаємо на кластері ISP-Internet, щоб вивести його (див. рис.3.2).

З смартфона вводимо `www.register.pk` в веб-браузері. Вводимо `admin` як ім'я адміністратора та пароль для входу в локальний сервер IoT, розміщений на сервері реєстрації.

Розкриваємо всі статуси детекторів диму.

Імітуємо вогонь на кухні. Слідкуємо, що відбувається з датчиками диму.

Почніть моделювання вогню в інших місцях, щоб спостерігати, що відбувається.

3.2.6. Управління відкриттям вікна і дверей в гаражі.

Вважаємо, що стара машина ремонтується в гаражі (переносимо туди значок «старої машини»). Детектор СО, гаражні двері та вікна були встановлені та настроєні таким чином, щоб запобігти отруєнню СО.

Розкриваємо статус усіх вікон, гаражних дверей та гаражного СО-детектора. Для пристрою, який не зв'язаний з мережею, Перевіряємо, чи його налаштовано для підключення до домашнього шлюзу для сервера ІоЕ, та чи ДНСР включений для налаштування ІР-конфігурації.

Запускаємо «старий автомобіль» у гаражі (`Alt+Click the Car`) та спостерігаємо підвищення рівня СО у гаражі.

Натискаємо повторно `Alt + Click the Car`, щоб вимкнути «стару машину».

Перевіряємо, як вікна та двері гаража взаємодіють із рівнем СО в гаражі.

3.2.7. Перевірка особливостей управління

Польовий шлюз та сервер реєстрації (Registration Server) можна використовувати для віддаленого управління пристроями IoT. Можна змінити спосіб доступу цих пристроїв віддалено.

Натискаємо пристрій. На вкладці «Пристрій» Обираємо «Немає», «Головний шлюз» або «Віддалений сервер». Для активності адреса сервера -

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		72

www.register.pka (209.165.201.10) та адміністратор як ім'я користувача та пароль.

В межах сервера можна додавати умовні вирази для пристроїв, здатних до дійних конфігурацій.

3.3. Рекомендації щодо вдосконалення стратегії безпеки при розробці та реалізації IoT-системи котеджу

Захист інфраструктури IoT котеджу вимагає ретельно продуманої стратегії з погляду безпеки. Відповідно до цієї стратегії необхідно захищати дані у хмарі, забезпечувати цілісність даних у процесі передачі через загальнодоступний Інтернет та безпечно готувати пристрої. Кожен наступний рівень забезпечує гарантії безпеки у всій інфраструктурі.

Таку ретельно продуману стратегію безпеки можна розробити та реалізувати за умови активної участі різних співробітників, які займаються виробництвом, розробкою та розгортанням пристроїв та інфраструктури IoT. Такі працівники та їх ролі описані нижче.

Інтегратор обладнання Інтернету речей. Як правило, це інтегратори обладнання, які збирають обладнання різних виробників, або постачальники обладнання, які надають обладнання для розгортання Інтернету речей, виготовлене або інтегроване іншими постачальниками.

Розробник рішень Інтернет речей. Розробка рішення Інтернету речей зазвичай здійснюється розробником рішень. Цей розробник може входити до команди всередині компанії або системного інтегратора, що спеціалізується на даній діяльності. Розробник рішень IoT може розробляти різні компоненти рішення Інтернету речей з нуля або інтегрувати різні компоненти, які готові до відкриття або з відкритим вихідним кодом.

Фахівець із розгортання рішень Інтернету речей. Розроблене рішення Інтернету речей слід розгорнути у робочому середовищі. При цьому

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		73

розгортається обладнання, налагоджується взаємодія пристроїв та розгортаються рішення на апаратних пристроях або у хмарі.

Оператор рішень Інтернету речей. Після розгортання потрібне рішення Інтернету речей вимагає довгострокового моніторингу, встановлення оновлень та обслуговування. Ці завдання може виконувати команда всередині компанії, до якої входять спеціалісти з інформаційних технологій, групи з експлуатації та обслуговування обладнання, а також спеціалісти у певній галузі, які стежать за роботою усієї інфраструктури IoT.

Нижче розроблені рекомендації щодо розробки, розгортання та експлуатації безпечної інфраструктури IoT для кожного з цих співробітників.

Інтегратор обладнання IoT

Дотримання вимог щодо обладнання. Обладнання має містити мінімум компонентів, необхідних його роботи, і нічого зайвого. Наприклад, додавати USB-порти слід лише якщо вони потрібні для роботи пристрою. Додаткові компоненти відкривають нові напрямки атак на пристрій, яких слід уникати.

Захист обладнання від незаконної зміни. Створіть процедури для виявлення можливостей щодо фізичної незаконної зміни, наприклад кришки пристрою, що відійшла, або вилучення компонента пристрою. Ці сигнали про незаконну зміну можуть передаватися в потоці даних, що надсилаються у хмару, попереджаючи операторів про ці події.

Створення рішення на основі безпечного обладнання. Якщо собівартість придбаних пристроїв дозволяє, створіть функції безпеки, наприклад, безпечне зашифроване сховище, або функції завантаження на основі довіреного платформного модуля (TPM). Ці функції підвищують безпеку пристроїв та допомагають захистити всю інфраструктуру IoT.

Забезпечення безпеки під час оновлення. Вбудоване програмне забезпечення буде оновлюватися протягом усього часу існування пристрою, і це неминуче. Розробка безпечних способів оновлення та криптографічна надійність версій вбудованого ПЗ дозволить забезпечити безпеку пристроїв під час та після оновлення.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						74
Змн.	Арк.	№ докум.	Підпис	Дата		

Розробник рішень IoT

Вибір безпечного способу розробки програмного забезпечення. При розробці захищеного ПЗ необхідно ретельно продумати забезпечення захисту на всіх етапах - від створення проекту аж до його реалізації, тестування та розгортання. Від цього методу залежить вибір платформ, мов та інструментів. Життєвий цикл розробки захищених програм надає поетапний спосіб створення захищеного програмного забезпечення.

Обережність під час вибору програмного забезпечення з відкритим кодом. Програмне забезпечення з відкритим кодом дає змогу прискорити розробку рішень. Під час його вибору слід враховувати рівень активності спільноти щодо кожного такого компонента. Якщо спільнота активна, це гарантує підтримку програмного забезпечення, а також виявлення та усунення проблем. І навпаки, якщо використовується проект маловідомого неактивного програмного забезпечення з відкритим кодом, то підтримка не надаватиметься, а проблеми, швидше за все, не виявлятимуться.

Обережність під час інтеграції. Багато проломів у системі захисту ПЗ виявляються на межі інтерфейсів API та бібліотек. Функціональна можливість, яка не потрібна для поточного розгортання, може бути доступною на рівні API. Для забезпечення загальної безпеки обов'язково перевірте всі інтерфейси компонентів, що інтегруються, на наявність вразливостей.

Фахівець із розгортання рішень IoT

Безпечне розгортання обладнання. Може знадобитися розгорнути пристрої Інтернету речей в незахищених місцях, наприклад, у громадських приміщеннях або неконтрольованих місцях розташуваннях. У цьому випадку слід забезпечити максимальний захист обладнання, що розгортається, від незаконної зміни. Якщо в пристрої встановлено USB-порти або інші порти, переконайтеся, що вони надійно прикриті. Їх можна використовувати як точки входу для атаки.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
						75
Змн.	Арк.	№ докум.	Підпис	Дата		

Безпечно зберігання ключів автентифікації. При розгортанні кожного пристрою потрібні коди та пов'язані з ними ключі автентифікації, створені хмарною службою. Ці ключі слід зберігати у фізично безпечному місці навіть після розгортання. Шкідливий пристрій може використовувати будь-який компрометований ключ для маскуванню під існуючий пристрій.

Оператор рішень IoT

Оновлення системи. Операційна система та всі драйвери пристрою мають бути оновлені до останньої версії. Постійне оновлення операційних систем, наприклад Windows чи Linux, дозволяє захистити їх від атак зловмисників.

Захист від шкідливих процесів. По можливості додавайте нові антивірусні та антишкідливі програми в операційну систему кожного пристрою. Це допоможе усунути більшість зовнішніх загроз. Можна захистити більшість сучасних операційних систем від загроз, вживши відповідних заходів.

Часте проведення аудиту. Для реагування на проблеми з безпекою слід перш за все виконувати аудит інфраструктури Інтернету речей на наявність інцидентів безпеки. Більшість операційних систем має вбудовані засоби ведення журналу подій. Їх слід часто переглядати, щоб переконатися у відсутності проломів у системі безпеки. Дані аудиту можна надіслати як окремий потік даних телеметрії до хмарної служби для аналізу.

Фізичний захист інфраструктури Інтернету речей. Найсерйозніші атаки на систему безпеки інфраструктури Інтернету речей здійснюються у вигляді фізичного доступу до пристроїв. Дуже важливо забезпечити захист USB-портів та інших фізично доступних компонентів від атак зловмисників. Одним із ключів для виявлення проломів є ведення журналів фізичного доступу, наприклад використання USB-портів. Наприклад, у Windows 10 (IoT та інші SKU) доступна можливість докладного ведення журналу таких подій.

Захист облікових даних хмари. За допомогою облікових даних для автентифікації у хмарі, що використовуються для налаштування розгортання

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		76

інфраструктури Інтернету речей та роботи з нею, можливо, найпростіше отримати доступ до системи Інтернету речей та скомпрометувати її. Щоб захистити облікові дані, слід часто змінювати паролі та не використовувати їх на загальнодоступних комп'ютерах.

Можливості різних пристроїв IoT різняться. Деякі пристрої можуть бути комп'ютерами зі стандартною операційною системою настільного комп'ютера. А на деяких пристроях може бути встановлена дуже спрощена операційна система. Описані вище рекомендації з безпеки можуть застосовуватися до цих пристроїв по-різному. Слід використовувати додаткові рекомендації щодо розгортання та безпеки, що надаються виробником пристроїв (якщо є).

Деякі застарілі та обмежені пристрої можуть бути не призначені для розгортання IoT. У них може бути відсутня можливість шифрування даних, підключення до Інтернету або надання розширених засобів аудиту. Щоб забезпечити безпеку, необхідну для підключення таких пристроїв до Інтернету, при об'єднанні даних застарілих пристроїв потрібно використовувати польові шлюзи. Польовий шлюз забезпечує безпечну автентифікацію, узгодження зашифрованих сеансів, отримання команд із хмар та інші функції безпеки.

Висновки по 3 розділу

На основі можливостей програмного комплексу Cisco Packet Tracer розроблено імітаційну модель IoT системи котеджу.

Здійснено моделювання та перевірку правильності прийнятих у проекті рішень.

Розроблено рекомендації щодо вдосконалення стратегії безпеки при розробці та реалізації IoT-системи котеджу.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		77

ВИСНОВКИ

У випускній кваліфікаційній роботі бакалавра вирішене актуальне завдання по розробці проекту захищеної IoT-системи котеджу.

Проведений аналіз літературних джерел виявив велику кількість публікацій, що стосується розробок різних рішень «розумних будинків», що підтверджує актуальність теми роботи.

Аналіз сучасного стану розробок «розумних будинків» показав, що на сьогодні ринок пропонує велику кількість пристроїв та систем IoT, що можуть бути використані для рішення завдання. Однак, з того ж аналізу слідує, що питанням забезпечення безпеки IoT систем приділяється значно менше уваги. Разом з тим слід відмітити, що системи IoT мають ряд вразливостей і тому при проектуванні необхідно передбачити заходи та засоби забезпечення кібербезпеки під час функціонування IoT системи котеджу.

Для рішення задачі була розроблена структурна схема IoT системи котеджу орієнтована на розподіл пристроїв по підгрупах та розміщення їх у кімнатах, відповідно до плану котеджу.

Для забезпечення безпеки важливо правильно змодельовати ризики, щоб виробити рекомендації для їх усунення. Тому моделювання ризиків передбачає такі чотири етапи: моделювання застосування; створення списку загроз; усунення ризиків; перевірка усунення ризиків.

У роботі використана модель загроз STRIDE (спуфінг, незаконна зміна, відмова, розкриття інформації, відмова в обслуговуванні та несанкціоноване підвищення привілеїв).

Функціональна схема IoT системи котеджу включає зони пристроїв, зони польового шлюзу та зону хмарного шлюзу. Реалізацію проекту пропонується виконати з використанням хмарного середовища Azure.

Моделювання ризиків виконано за допомогою середовища MS Threat Modeling Tool. Докладно розглянуто моделювання ризиків для таких

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		78

елементів як: процеси (підконтрольні та зовнішні); взаємодія (або потоки даних); зберігання (або сховища даних).

Розроблені рекомендації по усуненню кожного виду ризиків.

На основі можливостей програмного комплексу Cisco Packet Tracer розроблено імітаційну модель IoT системи котеджу, у якій виділяються зони безпеки: пристроїв, польового шлюзу, хмарного шлюзу.

Проведені моделювання та перевірка правильності прийнятих у проекті рішень на основі моделі. Результати моделювання підтвердили працездатність та ефективність прийнятих рішень.

На основі розподілу функцій між виконавцями проекту, розроблено рекомендації щодо вдосконалення стратегії безпеки при розробці та реалізації IoT-системи котеджу.

Таким чином, завдання на випускню кваліфікаційну роботу бакалавра виконано у повному обсязі.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		79

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Интернет речей. [Электронный ресурс] – Режим доступа: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D1%80%D0%B5%D1%87%D0%B5%D0%B9
2. Internet of things : challenges, advances, and applications. — Boca Raton, 2018. — 1 online resource (xvii, 418 pages) с. — ISBN 978-1-315-15500-5, 1-315-15500-1, 978-1-4987-7853-4, 1-4987-7853-4, 978-1-351-65105-9, 1-351-65105-6
3. Abhik Chaudhuri. Internet of things, for things, and by things. — Boca Raton, FL, 2019. — 1 online resource (xxvii, 257 pages) с. — ISBN 978-1-315-20064-4, 978-1-351-77968-5, 1-315-20064-3, 1-351-77968-0
4. Безпека Інтернету речей. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0_%D1%96%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D1%83_%D1%80%D0%B5%D1%87%D0%B5%D0%B9
5. Соколов М.Н., Смолянинова К.А., Якушина Н.А. Проблемы безопасности интернета вещей: обзор. — Вопросы кибербезопасности : журнал.— 2015. — № 5(13). — 34 с.
6. Loukas, George (June 2015). Cyber-Physical Attacks A growing invisible threat. Butterworh-Heinemann (Elsevier). с. 65. ISBN 9780128012901.
7. КОМПЛЕКТ ДЛЯ РОЗУМНОГО БУДИНКУ FIBARO STARTER KIT <https://secur.ua/ua/komplekt-dlja-umnogo-doma-fibaro-starter-kit.html>
8. Комплекты для розумного будинку. [Електронний ресурс] – Режим доступу: <https://worldvision.com.ua/komplekty-dlya-umnogo-doma/>
9. Ли П. Архитектура интернета вещей / пер. с англ. М. А. Райтмана. – М.: ДМК Пресс, 2019. – 454 с.: ил.
10. Грингард С. Интернет вещей. Будущее уже здесь / С. Грингард. – Альпина Паблишер – 2017. – 188 с.

					КБ.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		80

11. Росляков А. В., Ваянин С. В., Гребешков А. Ю. Интернет вещей: учеб. пособ. /А. В. Росляков, С. В. Ваянин, А. Ю. Гребешков. – Самара. 2015. – 136 с.
12. Шаньгин В. Защита информации в компьютерных системах и сетях / В. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.
13. Интернет вещей. Исследования и область применения: монография / Е.П. Зараменских, И.Е. Артемьев. - М.: НИЦ ИНФРА-М, 2015. - 200 с.: 60х90 1/16. <http://znanium.com/catalog.php?bookinfo=526946>
14. Брайчевський, С. М. (2019). Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. Інформація і право 4 (31). doi:10.37750/2616-6798.2019.4(31).194348
15. Лукацкий А.С. Криптография в "Интернете вещей" // www.slideshare.net : сайт. — 2016. — 23 марта
16. Баранов О.А. Интернет речей (IoT): огляд правових проблем // Інтернет речей: проблеми правового регулювання та впровадження: Матеріали науково-практичної конференції. 24 жовтня 2017 р., м. Київ. / Упоряд. В. М. Фурашев, С. Ю. Петряєв. – К.: НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. http://ipp.kpi.ua/wp-content/uploads/2017/-_14.11.2017.pdf
17. Общие сведения о функциях средства моделирования угроз [Электронный ресурс] – Режим доступа: <https://docs.microsoft.com/ru-ru/azure/security/develop/threat-modeling-tool-feature-overview>
18. Архитектура безопасности Интернета вещей. [Электронный ресурс] – Режим доступа: <https://docs.microsoft.com/ru-ru/azure/iot-fundamentals/iot-security-architecture#security-starts-with-a-threat-model>
19. S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques", Computer Science, vol. 60, pp. 708-713, 2015.

20. Пулеко І. В., Пулеко К.І. Особливості застосування сертифікації Х.509 для гарантування безпеки пристроїв Інтернету речей у хмарному середовищі AZURE. Тези Всеукраїнської науково-практичної online конференції аспірантів, молодих учених та студентів, присвяченої Дню науки. – Житомир : «Житомирська політехніка», 2021. – 646 с. 11-15 травня 2021 року. С. 137-138.

21. Пулеко К. І., Поліщук Ю. Я. Аналіз напрямків застосування штучного інтелекту в задачах кібербезпеки. Тези доповідей IV Всеукраїнської науково-практичної інтернет-конференції здобувачів вищої освіти і молодих учених «Інформаційно-комп'ютерні технології: стан, досягнення та перспективи розвитку», м. Житомир, 25 – 26 листопада 2021 р. – Житомир: Житомирська політехніка, 2021. – 186 с. Стор.62-63. ISBN 978-966-683-592-8

22. Пулеко І. В. Методичні рекомендації для проведення лабораторних робіт з навчальної дисципліни «Архітектура та технології IoT» для студентів освітнього рівня «бакалавр». Частина 1/ підг. І. В. Пулеко. – Житомир : ЖДТУ, 2019. – 68 с.

23. Методичні рекомендації для проведення лабораторних робіт з навчальної дисципліни "Архітектура та технології IoT" для студентів ОР "бакалавр". Частина 2. / Пулеко І.В., Сугоняк І.І. Свінцицька О.М. - Житомир: Державний університет "Житомирська політехніка", 2020. - 90 с.

ДОДАТКИ

Програмне забезпечення мікроконтролерів проекту

Програма для MCU0

```
from gpio import *
from time import *

def handleSensorData():
    value = digitalRead(0)
    if value == 0:
        customWrite(1, '0')
        customWrite(2, '0')
    else:
        customWrite(1, '1')
        customWrite(2, '1')

def main():
    add_event_detect(0, handleSensorData)

    while True:
        delay(1000)

if __name__ == "__main__":
    main()
```

Програма для MCU1

```
from gpio import *
from time import *

def handleSensorData():
    value = digitalRead(0)
    if value == 0:
        customWrite(1, '0')
        customWrite(2, '0')
    else:
        customWrite(1, '1')
        customWrite(2, '1')

def main():
    add_event_detect(0, handleSensorData)

    while True:
```

```
        delay(1000)

if __name__ == "__main__":
    main()
```

Програма для MCU2

```
from gpio import *
from time import *

def handleSensorData():
    value = digitalRead(0)
    if value == 0:
        customWrite(1, '0')
    else:
        customWrite(1, '1')

def main():
    add_event_detect(0, handleSensorData)

    while True:
        delay(1000)

if __name__ == "__main__":
    main()
```

Програма для MCU3

```
from gpio import *
from time import *

def handleSensorData():
    value = digitalRead(0)
    if value == 0:
        customWrite(1, '0')
    else:
        customWrite(1, '1')

def main():
    add_event_detect(0, handleSensorData)

    while True:
        delay(1000)

if __name__ == "__main__":
```

```
main()
```

Програма для SBC0

```
from gpio import *
from time import *

def main():
    while True:
        if digitalRead(1) > 0 or digitalRead(2) == LOW :
            customWrite(0,0)
        else :
            customWrite(0,2)
        delay(500)

if __name__ == "__main__":
    main()
```