ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО–НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення

Пояснювальна записка

до магістерської роботи

на ступінь вищої освіти магістр

на тему: «**Розробка системи оцінки безпеки розумних будинків на основі Internet of Things»**

Виконав: студент 6 курсу, групи ПДМ–61

спеціальності

121 Інженерія програмного забезпечення

(шифр і назва спеціальності)

Галай Я. О.

(прізвище та ініціали)

Керівник Бондарчук А.П.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Київ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Інженерії програмного забезпечення
Ступінь вищої освіти - «Магістр»
Спеціальність - 121 «Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інженерії програмного забезпечення
_____О.В. Негоденко

"____"____20___року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Галаю Ярославу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи: «Розробка системи оцінки безпеки розумних будинків на основі Internet of Things»
Керівник роботи д.т.н., професор кафедри ІПЗ Андрій Петрович Бондарчук ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "13" жовтня року №230.
2. Строк подання студентом роботи 24.12.2020
3. Вихідні дані до роботи:
   3.1. Вимоги до кваліфікаційної роботи магістра з актуальних завдань спеціальності;
   3.2. Нормативні матеріали (стандарти, Гости);
   3.3. Технічні вимоги;
   3.4. Науково-технічна література з питань, пов'язаних з темою роботи.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   4.1. Порівняльний аналіз результатів, отриманих іншими авторами;
   4.2. Методика дослідження;
   4.3. Результати дослідження;
   4.4. Висновки
5. Перелік графічного матеріалу.
6. Дата видачі завдання 02.11.2020

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	02.11.20	Виконано
2	Огляд існуючих рішень та літератури	03.11.20	Виконано
3	Огляд розумних будинків на основі IoT	12.11.20	Виконано
4	Розробка системи оцінки безпеки	16.11.20	Виконано
5	Дослідження ризиків безпеки за допомогою розробленої системи	24.11.20	Виконано
6	Вступ, висновки, реферат	08.12.20	Виконано
7	Розробка обов‘язкових демонстраційних матеріалів	11.12.20	Виконано
8	Здача роботи	24.12.20	

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи : 105 с., 26 табл., 12 рис., 45 джерел.

Об`єкт дослідження – оцінка безпеки розумних будинків на базі IoT.

Предмет дослідження – типовий розумний будинок на базі IoT.

Мета роботи – оцінка безпеки типового розумного будинку на базі IoT за допомогою розробленої системи оцінки.

Методи дослідження — система оцінки безпеки, восьми-етапний алгоритм оцінки безпеки, чотирьох-фазний процес оцінки безпеки.

У даній роботі мова йде про розробку системи оцінки безпеки розумних будинків, які використовують технології Internet of Things.

Інтернет речей (IoT) - це парадигма, що зароджується, зосереджена на взаємозв'язку речей або пристроїв між собою та користувачами. З часом більшість зв'язків в Інтернеті речей переходять від «людина взаємодіє з речами» до зв'язку «речі взаємодіють з речами». Очікується, що ця технологія стане важливою віхою у розвитку розумних будинків, щоб принести зручність та ефективність у наше життя та наші будинки. Але введення цієї технології IoT у наші будинки матиме важливе значення для безпеки цих технологій. Підключення всіх розумних об'єктів усередині будинку до Інтернету та між собою призводить до нових проблем безпеки та конфіденційності, наприклад, конфіденційності, автентичності та цілісності даних, що сприймаються та обмінюються об'єктами.

Ці технології дуже вразливі до різних атак безпеки, які роблять розумний дім на базі IoT небезпечним для проживання, тому для оцінки ситуації розумних будинків необхідно оцінити ризики безпеки. Щоб будь-яка технологія мала успіх і досягла широкого використання, вона повинна завоювати довіру користувачів, забезпечуючи достатню безпеку та конфіденційність. Як і у всіх секторах, підтримка безпеки буде найважливішим викликом для подолання. Оскільки будинки дедалі більше комп'ютеризуються та наповнюються пристроями, потенційні атаки комп'ютерної безпеки та їх вплив на мешканців потребують дослідження.

В даній роботі використовується методологія, яка фокусується головним чином на інформаційних активах та розглядає контейнери (технічні, фізичні та людські) та проводить оцінку ризику безпеки з метою висвітлення різних недоліків безпеки в розумному домі на базі Інтернету речей, наслідків та пропонування заходів проти виявлених проблеми, що задовольняють більшіс вимог безпеки. Врешті, вона пропонує рекомендації для користувачів.

Ключові слова: INTERNET OF THINGS, АВТОМАТИЗАЦІЯ БУДИНКІВ, РОЗУМНИЙ БУДИНОК, ОЦІНКА РИЗИКУ БЕЗПЕКИ, РЕКОМЕНДАЦІЇ ЩОДО БЕЗПЕКИ, ЗАГРОЗИ БЕЗПЕЦІ, КОНТРЗАХОДИ БЕЗПЕКИ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BAN	Body Area Network
САБ	Система автоматизації будівель
КЦД	Конфіденційність, цілісність та доступність
DOS	Denial of Service
НДД	Наукове дослідження дизайну
МДНД	Методологія наукового дослідження дизайну DSRM
DTLS	Datagram Transport Layer Security
EDGE	Покращені швидкості передачі даних для GSM розвитку
GPRS	General Packet Radio Service
ОВК	Опалення, вентиляція та кондиціонування
СВВ	Система виявлення вторгнень
IoT	Інтернет речей
IoE	Інтернет усього
СЗП	Система запобігання проникненню
IPsec	Internet Protocol Security
KNX	Konnex
LAN	Local Area Network
LON	Local Operating Network
LTU	Lulea University of Technology
MAN	Metropolitan Area Network
NFC	Near Field Communication
PAN	Personal Area Network
ЗЛЕ	Зв'язок лінії електропередачі
RFID	Radio Frequency Identification
РД	Розумний дім
АСРД	Автоматизаційна система розумного дому
SOA	Service-Oriented Architecture
SSL	Secure Sockets Layer

TCP	Transport Layer Protocol
СМДРЧ	Синхронний множинний доступ з розподілом часу
TLS	Transport Layer Security
UDP	User Datagram Protocol
УСМЗ	Універсальна система мобільного зв'язку
VPN	Virtual Private Network
WAN	Wide Area Network
WIMAX	Worldwide Interoperability for Microwave Access
WSN	Wireless Sensor Networks

ВСТУП

Об`єкт дослідження – оцінка безпеки розумних будинків на базі IoT.

Предмет дослідження – типовий розумний будинок на базі IoT.

Мета роботи – оцінка безпеки типового розумного будинку на базі IoT за допомогою розробленої системи оцінки.

Методи дослідження — система оцінки безпеки, восьми-етапний алгоритм оцінки безпеки, чотирьох-фазний процес оцінки безпеки.

Інтернет речей (IoT) - це парадигма, що зароджується, зосереджена на взаємозв'язку речей або пристроїв між собою та користувачами. З часом більшість зв'язків в Інтернеті речей переходять від «людина взаємодіє за речами» до зв'язку «речі взаємодіють з речами». Очікується, що ця технологія стане важливою віхою у розвитку розумних будинків, щоб принести зручність та ефективність у наше життя та наші будинки. Але введення цієї технології IoT у наші будинки матиме важливе значення для безпеки цих технологій. Підключення всіх розумних об'єктів усередині будинку до Інтернету та між собою призводить до нових проблем безпеки та конфіденційності, наприклад, конфіденційності, автентичності та цілісності даних, що сприймаються та обмінюються об'єктами.

Ці технології дуже вразливі до різних атак безпеки, які роблять розумний дім на базі IoT небезпечним для проживання, тому для оцінки ситуації розумних будинків необхідно оцінити ризики безпеки. Щоб будь-яка технологія мала успіх і досягла широкого використання, вона повинна завоювати довіру користувачів, забезпечуючи достатню безпеку та конфіденційність. Як і у всіх секторах, підтримка безпеки буде найважливішим викликом для подолання. Оскільки будинки дедалі більше комп'ютеризуються та наповнюються пристроями, потенційні атаки комп'ютерної безпеки та їх вплив на мешканців потребують дослідження.

В даній роботі використовується методологія, яка фокусується головним чином на інформаційних активах та розглядає контейнери (технічні, фізичні та людські) та проводить оцінку ризику безпеки з метою висвітлення різних

недоліків безпеки в розумному домі на базі Інтернету речей, наслідків та пропонування заходів проти виявлених проблеми,

що задовольняють більшість вимог безпеки. Врешті, вона пропонує рекомендації для користувачів.

Новизна дослідження полягає в розробці практичних системи правил оцінки безпеки розумних будинків, що використовують прилади на основі Internet of Things.

Практична значимість дослідження полягає в результатах дослідження, отриманий перелік та рекомендації стануть корисним внеском, який може бути використаний як основа для специфікації вимог безпеки розумних будинків.

1 ОГЛЯД РОЗУМНИХ БУДИНКІВ НА ОСНОВІ IOT

1.1 Передумови

Загалом, не існує загальновизнаного визначення Інтернету речей. Насправді існує багато різних груп людей, які визначили цей термін, хоча його початкове використання приписується експерту з цифрових інновацій на ім'я Кевін Ештон [1]. У всіх визначеннях ми отримуємо загальне уявлення, що перша версія Інтернету стосувалась даних, створених людиною, тоді як наступна версія стосувалась даних, створених речами, тому її називали Інтернетом речей.

Існує багато визначень для Інтернету речей. Нижче наводяться деякі визначення: IoT, як правило, визначали як «динамічну глобальну мережеву інфраструктуру з можливостями самоконфігурування на основі стандартів та сумісних протоколів зв'язку; фізичні та віртуальні «речі» в IoT мають ідентичності та атрибути і здатні використовувати інтелектуальні інтерфейси та бути інтегрованими як інформаційна мережа »[2].

Мета IoT - підвищити функції першої версії Інтернету та зробити її більш корисною. За допомогою IoT користувачі можуть обмінюватися як інформацією, наданою людьми, що міститься в базах даних, так і інформацією, наданою речами у фізичному світі [3]. IoT можна описати як зв’язок фізичних речей з Інтернетом та між собою для різних корисних цілей за допомогою різних інтелектуальних технологій, створюючи розумну екосистему всепроникаючих обчислень. Це також можна описати як включення вбудованого інтелекту в окремі об’єкти, які можуть помітити зміни у своєму фізичному стані.

Загальним визначенням IoT є те, що комп’ютери, датчики та об’єкти взаємодіють між собою та обробляють дані, тому ми можемо стверджувати, що IoT - це нова технологічна система, об’єднана низкою інформаційних технологій.

Інтернет речей поєднує різні технології в напівавтономну мережу. Він підключає окремі пристрої до мережі та між собою. У мережі також існують системи контролерів (програмне забезпечення та послуги), які виконують функції

головного мозку системи для обробки даних шляхом аналізу та використання даних, зібраних підключеними пристроями, для прийняття рішень та ініціювання дій з тих самих чи інших пристроїв [4].

Основною метою IoT є надання нам можливості однозначно ідентифікувати, вказувати, отримувати доступ та контролювати речі в будь-який час і в будь-якому місці, використовуючи Інтернет [5]. Взаємозв'язані мережі пристроїв можуть призвести до великої кількості інтелектуальних та автономних додатків та послуг (Рисунок 1.1), що приносить значні особисті, професійні та економічні вигоди [6].

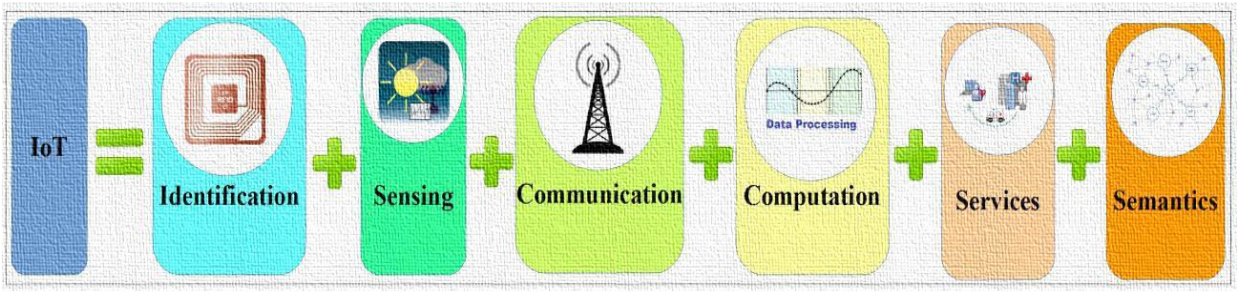


Рисунок 1.1 - Елементи IoT

Розумні середовища спрямовані на використання багатих комбінацій малих обчислювальних вузлів для ідентифікації та надання персоналізованих послуг користувачеві під час їх взаємодії та обміну інформацією із середовищем [8]. Технологію IoT можна застосовувати для створення розумних будинків, щоб забезпечити інтелект, комфорт і поліпшити якість нашого життя.

«Розумний дім» можна визначити як будинок, який автоматизований за допомогою технологій Інтернету речей і здатний реагувати на потреби мешканців, забезпечуючи їм комфорт, безпеку, безпеку та розваги [9].

У майбутньому IoT, як очікується, матиме значні програми для дому та бізнесу, що покращують якість життя та світову економіку. За допомогою IoT можна отримати віддалений доступ до електричних пристроїв, встановлених у вашому домі, та керувати ними в будь-якому місці та в будь-який час світу. Наприклад, розумні будинки дозволять своїм мешканцям автоматично відкривати гараж, добираючись додому, готувати каву, керувати системами кондиціонування,

смарт-телевізорами та іншими побутовими приладами всередині будинку. Розумні пристрої та системи автоматизації складають Smart Homes. Все, що пов'язано за допомогою Інтернету. Проста домашня автоматизація використовує таймери та годинники для включення бажаних операцій, але технологія розумного будинку може обробляти більш складні операції та запускати пристрої на основі вводу з інших пристроїв [4].

В основному розумні будинки оснащені вдосконаленими автоматичними системами для різних запрограмованих операцій та завдань, таких як регулювання температури, освітлення, мультимедіа, робота з вікнами та дверима тощо. Розумне домашнє середовище також називають інтелектом навколишнього середовища, чутливим адаптивна до сучасних людських та соціальних потреб [10]. РД є дуже перспективною областю, яка має різні переваги, такі як забезпечення підвищеного комфорту, більшої безпеки та безпеки, більш раціональне використання енергії та інших ресурсів, що сприяє значній економії. Ця область застосування досліджень дуже важлива і з часом буде збільшуватися, оскільки вона також пропонує потужні засоби для допомоги та підтримки особливих потреб людей похилого віку та людей з інвалідністю [11], для моніторингу навколишнього середовища [12] та контролю. Згідно з [13], головними цілями Розумного будинку є підвищення автоматизації будинку, спрощення управління енергією та зменшення викидів в навколишнє середовище. Споживання енергії та комфорт мешканців є ключовими факторами при оцінці розумного домашнього середовища [14].

Більшість комерційних доступних систем домашньої автоматизації можна розділити на дві категорії: системи з локальним управлінням та системи з дистанційним управлінням. Локально керовані системи використовують домашній контролер для досягнення домашньої автоматизації, що дозволяє користувачам повною мірою використовувати свою систему автоматизації з дому через стаціонарний або бездротовий інтерфейс.

Системи з дистанційним управлінням використовують підключення до Інтернету або інтеграцію з існуючою системою домашньої безпеки, щоб

дозволити користувачеві повністю контролювати свою систему зі свого персонального комп'ютера, мобільного пристрою або за допомогою телефону від свого постачальника послуг домашньої безпеки [15].

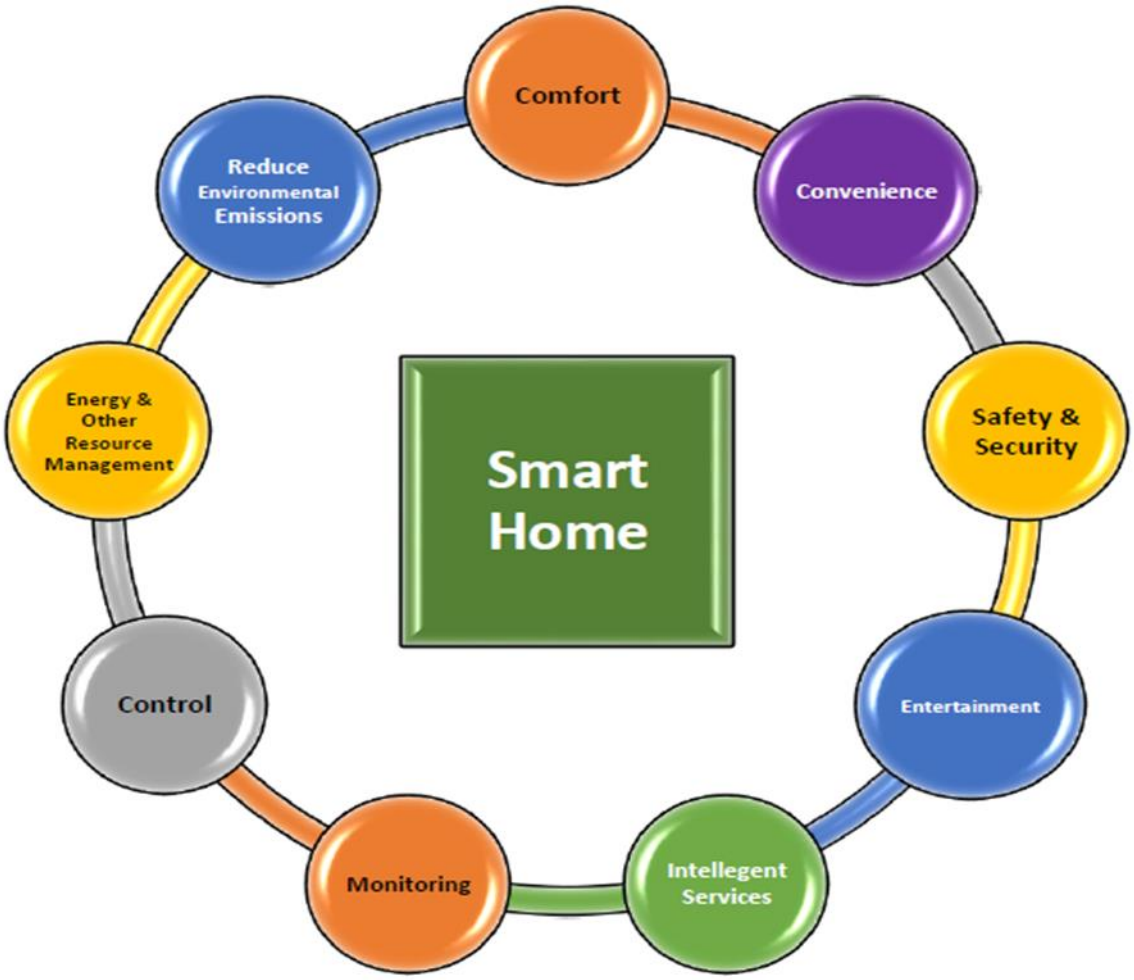


Рисунок 1.2 - Цілі розумного будинку

Система інтеграції розумного будинку скла дається приблизно з трьох важливих цілей (Рисунок 1.2): По-перше, фізичних компонентів (електронне обладнання - розумні датчики та пускачі); По-друге, система зв'язку (дротова / бездротова мережа), яка зазвичай з'єднує фізичні компоненти; і по-третє, інтелектуальна обробка інформації (наприклад, за допомогою програми штучного інтелекту) для управління та управління інтегрованою системою розумного будинку [5].

Введення технології IoT до нашого будинку призводить до нових викликів безпеці, тому розумні будинки, засновані на IoT, вимагають високих вимог до

безпеки, оскільки домашнє середовище містить важливу та приватну інформацію (Рисунок 1.3).

Сучасні технології пропонують як можливості, так і ризики. Розумний дім на основі Інтернету речей дуже вразливий до атак з Інтернету, якщо зловмисник розумний дім або розумний пристрій зловмисник може вторгнутись у конфіденційність користувача викрадати особисту інформацію та відстежувати їх усередині будинку [17], і тому необхідно вжити відповідних заходів.

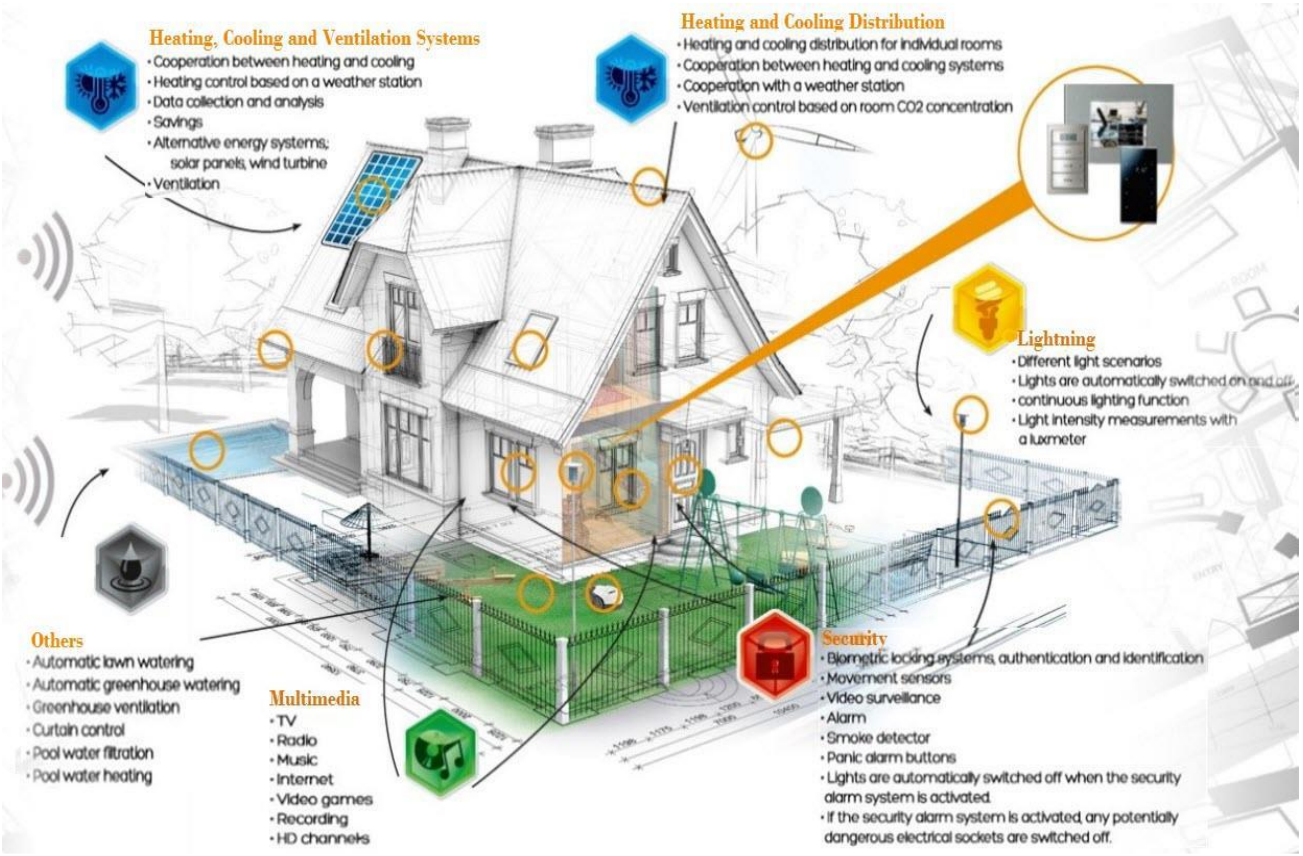


Рисунок 1.3 - Розумний будинок та його підсистеми

Кількість пристроїв IoT швидко зростало, недавня оцінка передбачає, що в 2010 році було 12,5 мільярда пристроїв, підключених до Інтернету, і прогнозується 50 мільярдів пристроїв до 2020 року [18]. Це призведе до багатьох проблем безпеки.

Запропоноване дослідження буде зосереджене на питаннях безпеки в Інтелектуальних домах, що базуються на Інтернеті речей, впливах та в кінці дасть деякі рекомендації, особливо для користувача.

1.2 Визначення проблеми

Останні звіти про IoT та РД викликали суспільний інтерес та стурбованість, і ці технології мають важливе значення для безпеки. Потреба в безпеці в розумних будинках однакова, і навіть більше, ніж потреба в безпеці у всіх інших обчислювальних системах, щоб переконатись, що інформація не викрадена, не модифікована або не отримано доступу до неї.

Очевидно, що в традиційних будинках зловмисники можуть викрасти будинок або погрожувати йому лише в тому випадку, якщо вони фізично існують там поруч з домом. Але, підключивши будинок до Інтернету, зловмисник або зловмисник має можливість із підключенням до Інтернету отримати доступ до дому та контролювати його з будь-якої точки світу в будь-який час, спостерігаючи за мешканцями будинку за допомогою підключених камер у домі.

Системи розумного будинку дозволяють користувачеві контролювати і контролювати, наприклад термостати, пральні машини, чистячі роботи, розважальні системи, системи безпеки, детектори диму, дверні замки, щоб назвати лише декілька. При введенні цієї технології IoT у наші будинки виникають компроміси між зручністю, контролем, безпекою та приватністю [19]. Зловмисники можуть вторгнутися в конфіденційність користувача, викрасти приватну інформацію та відстежувати мешканців будинку, якщо їм вдається зламати розумний дім або розумний пристрій [17]. Варто зазначити, що розумний дім (РД) є привабливою мішенню для зловмисника, оскільки РД; містить особисту інформацію, підключений до Інтернету цілодобово, не має спеціального системного адміністратора, складається з пристроїв різних виробників з різними вразливими місцями, і зловмисник завжди має вибір сканувати Інтернет на наявність певної вразливості, що належить певному пристрою з певного виробник для експлуатації.

Пропоноване дослідження стосуватиметься оцінки ризиків інформаційної безпеки в розумних будинках на базі IoT. Цей дослідницький проект досліджує загрози інформаційної безпеки при підключенні інтелектуальних пристроїв один

до одного та до Інтернету при проектуванні розумного будинку, щоб поінформувати користувачів про ризики безпеки, які можуть або не можуть використовуватись, покращити безпеку та дати рекомендації.

1.3 Питання для дослідження

На основі огляду літератури, який я провів у розділі 3 щодо цієї теми, питань безпеки в розумних будинках на базі Інтернету речей, я бачу, що необхідно провести більше досліджень з висвітлення можливих загроз безпеці, які можуть завдати шкоди людям, які проживають у розумних будинках, а потім запропонувати можливі шляхи їх вирішення.

Мені не вдалося знайти жодного академічного дослідження, яке б проводило комплексну оцінку ризиків безпеки для розумних будинків на базі IoT, висвітлюючи ризики безпеки, контрзаходи та наслідки. Для дослідження цього розриву визначаються наступні питання дослідження:

1) Які загрози безпеці виникають від Smart Homes на базі IoT?

2) Які наслідки цих загроз (Вплив)?

3) Чи можна запропонувати відповідні контрзаходи?

4) Що рекомендувати користувачам?

Виявляючи загрози та наслідки, ми можемо спричинити ризики, оскільки ризик складається як із загроз, так і з наслідків.

Дуже важливо провести дослідження з питань безпеки в Smart Homes на базі IoT, щоб краще зрозуміти та уникнути серйозних наслідків. Без оцінки ризику безпеки або висвітлення загроз неможливо надати гарантії для системи та обґрунтувати вжиті заходи безпеки.

Крім того, ця нова технологія, IoT, щоб отримати широке визнання серед користувачів, безпека повинна бути кращою, і довіра є важливою для реалізації цього технологій у своїх будинках, оскільки якщо споживачі не мають впевненості у цій технології, вони не будуть ними користуватися.

Таким чином, безпека є однією із сфер, яка повинна бути найвищим пріоритетом при впровадженні технології розумного будинку.

1.4 Очікувані результати

Результати дослідження стануть корисним внеском у забезпечення кращого розуміння загроз безпеці щодо даної теми та допоможуть людям (користувачам) усвідомити потенційні ризики та заходи, які можуть бути вжиті для зменшення цих ризиків щодо їхніх розумних будинків, або прямо чи опосередковано. Сподіваюсь, отримані результати призведуть до подальших досліджень іншими особами в галузі безпеки в Інтернеті речей (IoT), що базуються на РД.

Результатом цього дослідження буде перелік виявлених загроз безпеці з можливими наслідками, рішення та рекомендації для користувачів, щоб поінформувати їх та обмежити величину ризиків. Крім того, у випадку оцінки ризиків для безпеки уроки, отримані в процесі, сприятимуть кращій роботі в майбутньому. Результати дипломної роботи можуть бути використані для вдосконалення впровадження технології IoT у розумні будинки з урахуванням ризиків безпеки.

1.5 Визначення меж

Основна увага в цьому дослідженні буде зосереджена на виявленні проблем безпеки (ризиків), відповідних контрзаходів та виявленні наслідків у розумних будинках на базі IoT, а також на наданні рекомендацій користувачам. Для цього будуть надані сценарії. Складність інтелектуальні послуги не є предметом дослідження.

Будуть створені прості служби для демонстрації контролю користувачами розумного будинку та передачі даних, але комплексна система розумного будинку не буде побудована.

Основна увага в цій роботі приділяється питанням оцінка ризику безпеки критично важливих інформаційних активів у типовому розумному будинку за допомогою розробленої системи для визначення ризиків для активів. Крім того, лабораторне середовище створюватися не буде.

1.6 Використання IoT технологій

Сучасні розробки інформаційно-комунікаційних технологій (ІКТ), пов'язані з комп'ютерними мережами, вбудованими системами та штучним інтелектом, зробили бачення розумного будинку технічно можливим. Отже, вдосконалюючи традиційні системи автоматизації будинку новими розумними функціями, стало можливим для розумного домашнього середовища демонструвати різні форми штучного інтелекту. Технологія розумного будинку - це включення технологій та послуг через домашню мережу для кращої якості життя.

Сприятливі технології для IoT включають; Ідентифікація радіочастот (RFID), Інтернет-протокол (IP), Електронний код продукту (EPC), Штрих-код, Бездротова вірність (Wi-Fi), Bluetooth, ZigBee, Близькофайлова комунікація (NFC), Пускачі, Бездротові сенсорні мережі (WSN) та Штучний інтелект (ШІ). Детальніше читайте цю літературу [20].

1.7 Зони застосування автоматизаційної системи розумного будинку

Інтернет речей забезпечує гнучку та масштабовану платформу, яка може підтримувати безліч різних додатків. Його популярність призвела до різноманітних додатків, зокрема розумних будинків.

Основною сферою застосування Системи автоматизованого розумного будинку (АСРД) є контроль навколишнього середовища за допомогою традиційних видів послуг освітлення / денне освітлення та системи опалення, вентиляції та кондиціонування (ОВК) [21], моніторинг та контроль, безпека та охорона, охорона здоров’я, енергозбереження , екологічний контроль та доступ до інформації [22].

Існують різні типи застосування розумних будинків; Розумні будинки для безпеки, Розумні будинки для догляду за людьми, Розумні будинки для охорони здоров’я, Розумні будинки для догляду за дітьми, Розумні будинки для енергоефективності та Розумні будинки для кращого життя (Рисунок 1.4) (музика,

розваги, тощо) [23].

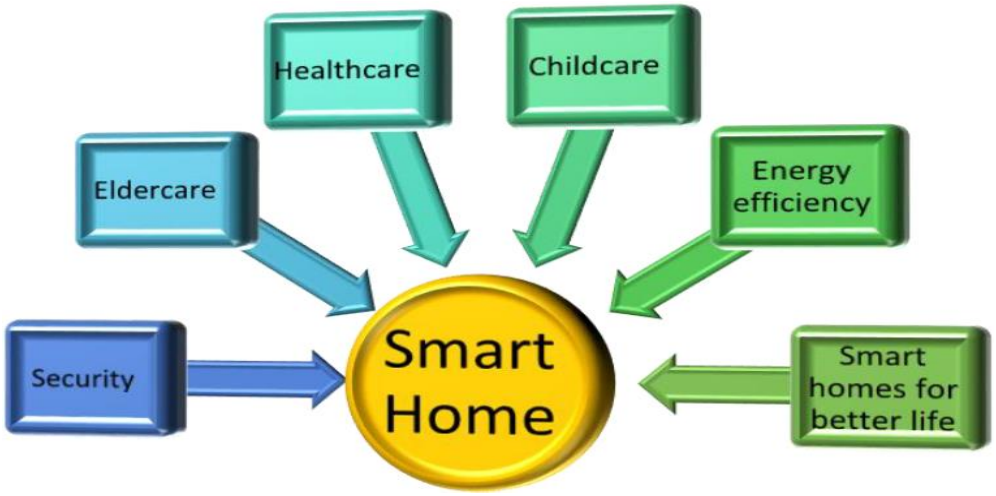


Рисунок 1.4 - Типи застосунків розумного будинку

1.8 Структура

Розумний дім може бути описаний будинком, який обладнаний розумними об'єктами, домашня мережа дозволяє передавати інформацію між об'єктами та житловим шлюзом щоб підключити розумний дім до зовнішнього світу Інтернету. Розумні об'єкти дають можливість взаємодіяти з мешканцями або спостерігати за ними.

Технічно система автоматизації будинку складається з п’яти будівельних блоків [24], які буде розглянути в наступних підрозділах.

1.8.1 Підконтрольні пристрої

Ці пристрої включають усі компоненти, такі як побутову техніку або побутову електроніку, які підключені до системи автоматизації будинку та керуються ними.

Для прямого використання використовуються різні типи технологій підключення, такі як WLAN-, Bluetooth-, Z-Wave-інтерфейси тощо підключення до контрольної мережі.

1.8.2 Сенсори та виконавчі механізми

Датчики можуть бачити і чути в домашній мережі. Існують датчики для широкого спектра використання, наприклад, для вимірювання температури, вологості, світла, рідини та газу та виявлення руху чи шуму. Пускачі - це засіб того, як розумна мережа може насправді робити щось у реальному світі. Існують такі механічні приводи, як насоси та електродвигуни, або електронні приводи, такі як електричні вимикачі. Пристрої IoT, оснащені датчиками, будуть виконувати роль колекторів, а вбудовані в виконавчі механізми - як виконавці. Пристрій з датчиками та виконавчим механізмом сприйме та спрацює.

1.8.3 Підконтрольна мережа

Він забезпечує зв'язок між контрольованими пристроями, датчиками та виконавчими механізмами, з одного боку, та контролером, а також пристроями дистанційного керування (смартфоном, планшетами, ноутбуками та ПК), з іншого. В даний час технології домашньої мережі класифікуються на три основні класи:

- Powerline Communication повторно використовує внутрішню електричну мережу. (наприклад, X.10);
- Бездротова передача (інтерфейси Z-Wave, ZigBee, Bluetooth, Wi-Fi, EnOcean та RFID);
- Кабельна передача (KNX та LON).

Для побутової мережі Ethernet (IEEE802.3), ЗЛЕ та IEEE1394 є найбільш широко використовуваними протоколами дротового зв'язку, а бездротові протоколи, доступні для домашньої мережі, - це бездротова локальна мережа, HomeRF, Bluetooth, UWB, ZigBee тощо [25].

У літературі [26] представлені різні типи мережевих або комунікаційних технологій для підключення інтелектуальних пристроїв в розумному будинку, а саме BAN, PAN, LAN, MAN та WAN.

WAN та MAN використовуються для зовнішнього середовища. Що стосується глобальної мережі, ми знаходимо технології УСМЗ, EDGE, GPRS або супутникові. Ці технології є бездротовими (WWAN: бездротові широкоформатні мережі) і здатні передавати інформацію на відстань до 30 кілометрів. Для MAN

ми знаходимо WIMAX, який здатний передавати інформацію на відстань до 20 кілометрів.

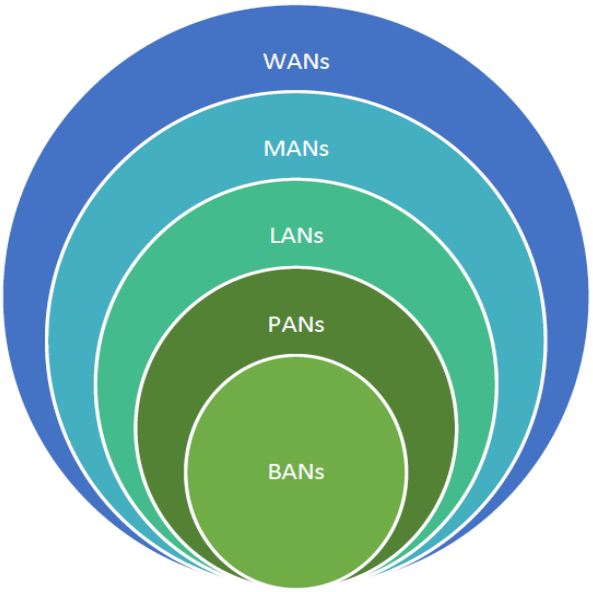


Рисунок 1.5 - Типи мережевих зон

Мережі LAN, PAN і BAN (Рисунок 1.5) використовуються у внутрішньому середовищі. Для локальних мереж Wi-Fi та HyperLan - це переважно бездротові рішення. Ethernet є основним дротовим рішенням.

Для PAN-телефонів Bluetooth, RFID, ZigBee, UWB - це бездротові рішення. CEBus, Convergence, emNET, HAVi, HomePNA, HomePlug, HomeRF, Jini technology, LonWorks, UPnP, VESA, USB та послідовне посилання - це дротові рішення.

Рівень управління складається з інтелектуальних датчиків і виконавчих механізмів, які взаємодіють з навколишнім середовищем та виконують завдання управління.

Вони пов'язані між собою надійною, низькою пропускною здатністю та вартістю ефективна мережа управління.

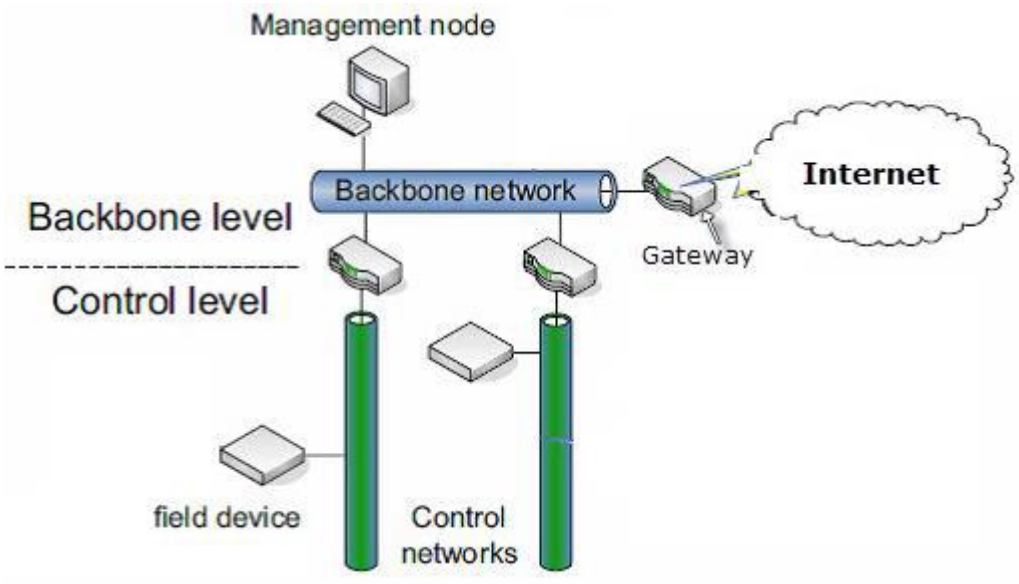


Рисунок 1.6 - Два рівні моделі в САБ [21]

Рівень магістралі з'єднує безліч підмереж управління з високою пропускною здатністю (Рисунок 1.6). Він також забезпечує зв’язок із зовнішнім світом (наприклад, Інтернетом). Вузли управління розташовані на магістралі, оскільки вони вимагають загального огляду всієї БАР.

1.8.4 Контролер, веб-сервер та база даних

Контролер - це комп'ютерна система, яка діє як мозок системи домашньої автоматизації, збирає інформацію за допомогою датчиків і отримує команди через пристрої дистанційного керування.

Він діє на основі команд або набору заздалегідь визначених правил за допомогою виконавчих механізмів або засобів зв'язку, таких як гучномовець, телефон або електронна пошта.

Користувацький інтерфейс підключений до бази даних через веб-сервер. База даних складається з деталей усіх домашніх пристроїв та їх поточного стану. Користувач, який віддалено звертається до свого дому, може запитувати інформацію про стан пристрою з бази даних через веб-сервер. Мікроконтролер керує всіма операціями та зв'язками в домашній мережі.

1.8.5 Пристрої віддаленого користування

Пристрої дистанційного керування, такі як смартфони, планшети,

ноутбуки та ПК, можна використовувати для підключення до програми автоматизації дому на домашньому контролері. Вони роблять це, підключаючись до контролера через саму мережу управління, або через будь-який інший інтерфейс, який надає контролер, наприклад, WLAN, Інтернет або телефонну мережу.

Тому смартфони можна використовувати як домашній пульт дистанційного керування розумним будинком через Інтернет або мобільну телефонну мережу.

На малюнку 7 нижче показані компоненти типової системи автоматизації будинку за допомогою Інтернету.

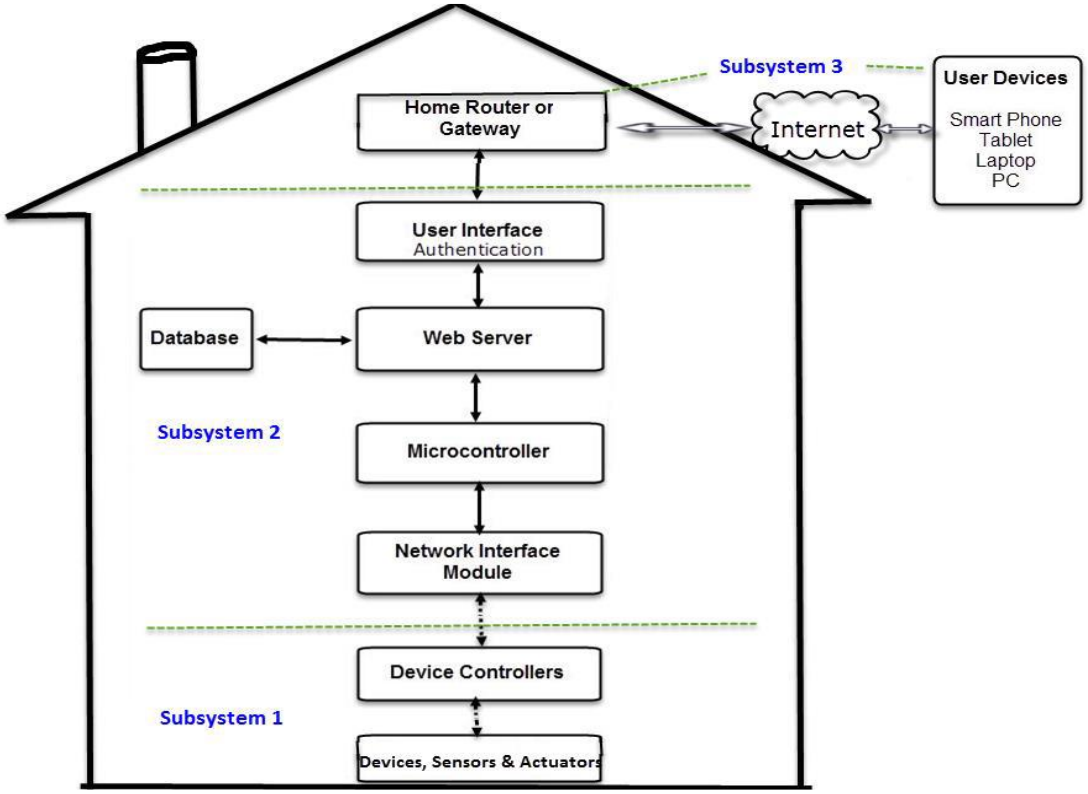


Рисунок 1.7 - Автоматизаційна система дому

Виходячи з рисунка 1.7, для простоти та для того, щоб точно знати, де в системі знаходяться ризики безпеки, ми можемо розділити всю систему на три підсистеми (частини) залежно від того, відбувається це всередині або поза Розумним будинком, а подробиці див. Попередній згадані будівельні блоки у розділі конструкцій вище. Коли мова йде про "мережу управління", вона

забезпечує зв'язок між пристроями, датчиками та виконавчими механізмами, з одного боку, та між контролером, а також пристроями дистанційного керування, з іншого боку, використовуючи різні мережеві технології. Тому він підпадає під обидві категорії (всередині та за межами розумного будинку). Нижче наведено підсистеми:

1) Всередині розумного будинку (внутрішня домашня мережа зв'язку):
   - Підсистема 1: Серед домашніх пристроїв (датчики та пускачі).
   - Підсистема 2: між пристроями та домашнім шлюзом.
2) Поза розумним будинком (зовнішня мережа зв'язку):
   - Підсистема 3: між домашніми шлюзами та Інтернетом.

1.9 Архітектура

У літературі [27] автори представляють модель архітектури шарів як показано на рисунку 1.8.

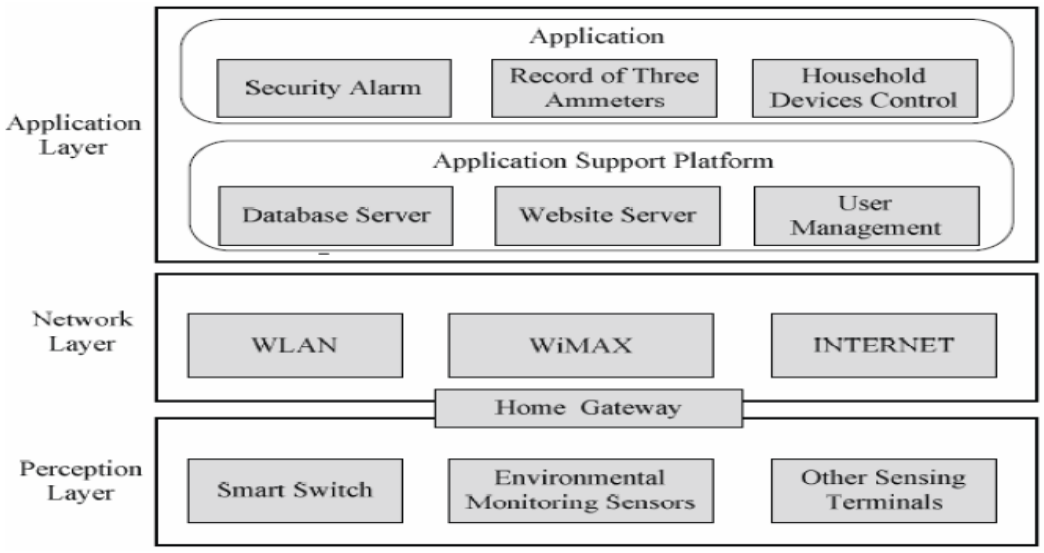


Рисунок 1.8 - Рівнева архітектурна модель контролюючої системи розумного будинку на базі IoT [27]

Інтелектуальної системи управління будинком, засновану на Інтернеті речей, яка включає рівень сприйняття, мережевий рівень та рівень додатків.

Література [28] пропонує систему розумного будинку на основі IoT та

представляє архітектуру системи (Рисунок 1.9) відповідно до багатошарової конструкції Інтернету речей. Система розділена на три шари; сенсорний та виконавчий рівень, мережевий рівень та рівень додатків.

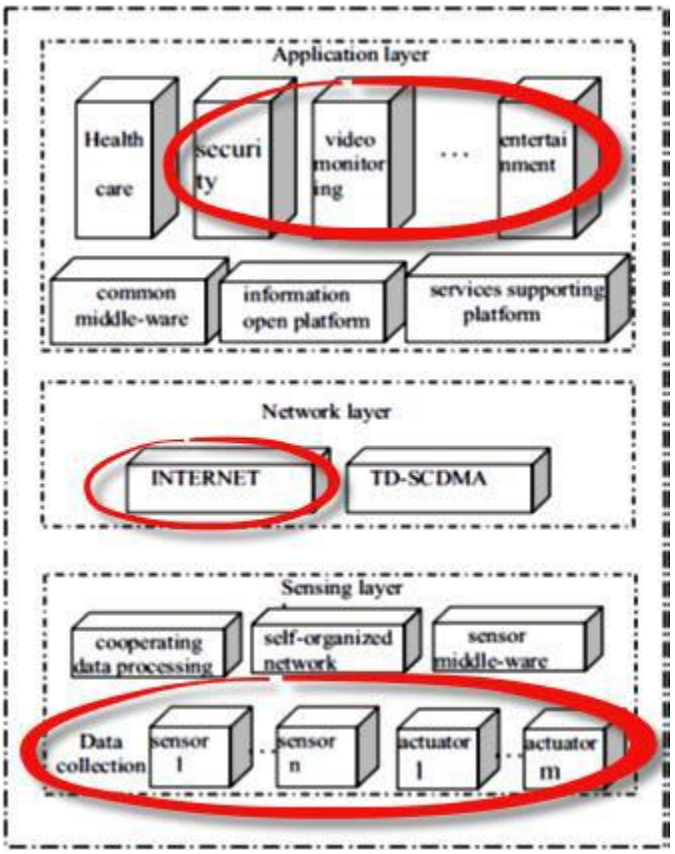


Рисунок 1.9 - Архітектура розумного будинку на базі IoT

Розумний дім - основний компонент Інтелектуального житлового кварталу. Коли концепція технології IOT вводиться до реалізації розумного будинку, традиційний розумний дім виходить з ладу моди [29]. Це охоплюватиме набагато ширший діапазон контролю. Наприклад, розумний будинок передбачає сімейну безпеку, сімейне лікування, обробку сімейних даних, сімейні розваги та сімейний бізнес. Архітектура програми для розумного будинку, заснована на IOT та компонентних технологіях, наведена нижче [30].

І на Рисунку 1.10, і на малюнку 10 показані різні шари та різні області. Але я зосереджусь на кільцевих областях, які виділені червоним кольором у моїй оцінці ризику.

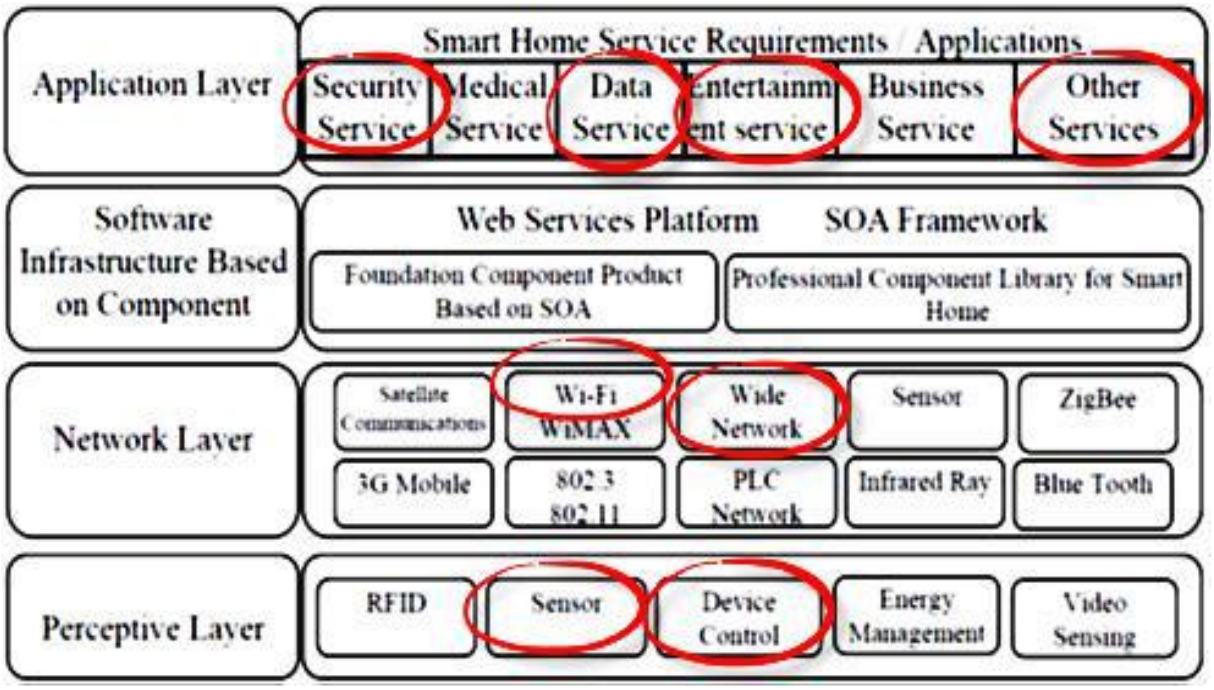


Рисунок 1.10 - Архітектура застосунку розумного будинку на базі IoT і компонентних технологій

Коротше кажучи, рівень сприйняття складається з різних типів модулів збору та управління (Рисунок 1.10).

Основна його функція - сприйняття та збір інформації. Робота мережевих шарів - це надійна передача. Він передає дані через Інтернет та мобільну телекомунікаційну мережу.

Основна робота рівня додатків полягає в розумній обробці даних, щоб ми могли використовувати оброблену інформацію.

2 ОГЛЯД ЛІТЕРАТУРИ

2.1 Огляд існуючих рішень та літератури

Мета цього розділу - встановити наукове значення дослідницької проблеми, показавши попередні дослідження в даній області, покращити моє власне розуміння цієї галузі, оновити читачів, знайти прогалину в літературі та необхідність цього дослідження.

Були визначені публікації про розумний дім від широкого кола академічних видавців, таких як Elsevier’s Science Direct, Springer, Інститут інженерів електротехніки та електроніки (IEEE), Wiley Interscience, Human Technology та Інститут комп’ютерних наук та телекомунікаційної техніки.

Публікації, що відбувалися протягом останнього десятиліття з 2005 по 2016 рік, були ідентифіковані за допомогою пошуку в трьох пошукових системах, тобто Google Scholar, Scopus та IEEE Xplore Digital Library. Використовуваними термінами пошуку були „проблеми безпеки в розумних будинках”, „Розумне середовище”, „розумне життя”, „інтелектуальні будинки”, „Розумне середовище”, „Інтелект навколишнього середовища” та „Системи домашньої автоматизації”, що призвело до вибору понад 100 різних джерел. Джерела відфільтровано, і обрано найбільш актуальні джерела.

Потім вони були відсортовані та поміщені в різні папки хронологічно з 2005 по 2016 рік.

У цьому розділі спочатку представлені попередні роботи про безпеку в розумних будинках на основі Інтернету речей.

Потім основна увага приділяється питанням безпеки, пов’язаним із цією технологією. Далі, він намагається знайти прогалину у дослідженні, яку потрібно заповнити, і нарешті він містить короткий огляд літератури.

2.2 Проблеми безпеки

Цей розділ описує різні питання безпеки, що стосуються безпеки системи

розумного будинку відповідно до (рис. 7) та ключових понять, описаних у попередньому розділі; Пристрої, Датчики та виконавчі механізми, Мережа управління, Пристрої контролера та Пульта дистанційного керування, а також використані технології та архітектура.

Фізична особа може безпосередньо атакувати пристрій взаємозв'язку (наприклад, шлюз) або польовий пристрій, використовуючи свою мережу або локальний інтерфейс зв'язку (атакуючи пристрій) [21]. Уособлення пристрою за допомогою його несправного сертифіката [31]. Побутову техніку можна підключити до дротової або бездротової мережі через домашній шлюз. У самому домашньому шлюзі може бути вразливість. Як правило, на домашньому шлюзі встановлена веб-програма управління. Його проблема полягає в тому, що зловмисник може отримати привілеї адміністратора за допомогою веб-сервера або вразливості CGI. Напад на домашній шлюз може безпосередньо призвести до нападу на всю мережу домогосподарств, оскільки це точка, яка з'єднує домогосподарство із зовні [25].

Подальші питання безпеки стосуються цілісності самих пристроїв, вони мобільні і може надійти в заданому розумному середовищі з невідомого домену. Проблема полягає в тому, що навіть відомий пристрій міг бути змінений за час його відсутності [32]. Типи вразливих місць безпеки можуть бути злом домашнього пристрою, вірусна атака, витік інформації, виготовлення вмісту та порушення конфіденційності [25].

Існують різні способи проникнення в розумний дім. Оскільки деякі або багато пристроїв підключені до Інтернету, правопорушник може напасти на найслабшого з них і використовувати цей пристрій для проникнення в цілу систему. Інша можливість - зараження вже атакованих комп’ютерів або мобільних пристроїв шкідливим програмним забезпеченням і подальше використання їх як дайвінг-дошки для подальшого розслідування та проникнення в мережу. Пристрій має різний рівень ризику стати об’єктом атаки.

Деякі пристрої, особливо необроблені датчики, високі обмеження пам'яті та обробної потужності роблять їх непривабливими. Залежно від намірів

зловмисника представлятимуть інтерес різні групи пристроїв Smart Home. Перші широко розповсюджені атаки, швидше за все, будуть націлені

продукти групи Controlling Systems, оскільки вони найбільш схожі на існуючі цілі, а крім того, вони підключені більш-менш до будь-якого іншого пристрою Smart Home [33].

Автори в літературі [31] роблять висновок, що супротивник має дві різні можливості отримати доступ до функцій управління, а саме мережеві атаки та атаки на пристрої. Під час мережевих атак противник може спробувати перехопити, маніпулювати, сфабрикувати або перервати передані дані. Атаки на пристрої можна класифікувати на атаки на програмне забезпечення, фізичні або інвазивні атаки та атаки бічних каналів. Крім того, існує можливість того, що зловмисник може замаскуватися під внутрішнього користувача за допомогою інтерактивного цифрового телебачення, IP-приставки або домашньої панелі або отримати нелегальний доступ до нього за допомогою інших засобів управління побутовою технікою [25].

Бездротові інтелектуальні датчики стали дуже привабливими пристроями для моніторингу, відстеження рухомих об'єктів у програмі розумного будинку, і тому вони стали мішенню для різних атак. Існують різні атаки на бездротову сенсорну мережу (WSN) [34]:

- Наявність послуг (Затоплення, перешкоди, відтворення та вибіркове пересилання);
- Мережева маршрутизація (Несанкціоноване оновлення маршрутизації, Червова нора та Проріз);
- Ідентифікація / аутентифікація вузлів (підслуховування, видавання себе за інших і Sybil).

У літературі [35] описуються типи атак WSN та система виявлення вторгнень для запобігання цим типам атак. Автори описують кібератаки, які відбуваються в бездротовому датчику мережі, а саме атаки відмови в обслуговуванні (DOS), неправильне спрямування, селективна переадресація, атака на вибій, атака на Sybil, атака на червоточину та атаки привітання з привітанням.

У літературі [36] автори обговорюють потенційні атаки на WSN; Підслуховування, відмова в обслуговуванні, компроміс вузла. Напади на нори та червоточини та фізичні напади та виявлення та профілактика.

Конфіденційність та відстеження - це два найважливіші питання безпеки, які виникають внаслідок використання технології RFID, і тут варто згадати деякі інші, такі як фізичні атаки, відмова в обслуговуванні (DOS), підробка, підробка, прослуховування та аналіз трафіку [32].

Посилаючись на малюнок 11 нижче, необхідно захищати САБ від атак як на магістральному рівні, так і на рівні управління від загроз як ззовні, так і всередині. Атака може бути на трафік в керуючій або магістральній мережі, що ним маніпулює, або безпосередньо на пристрій взаємозв'язку (наприклад, шлюз) або польовий пристрій за допомогою його мережевого або локального інтерфейсу зв'язку.

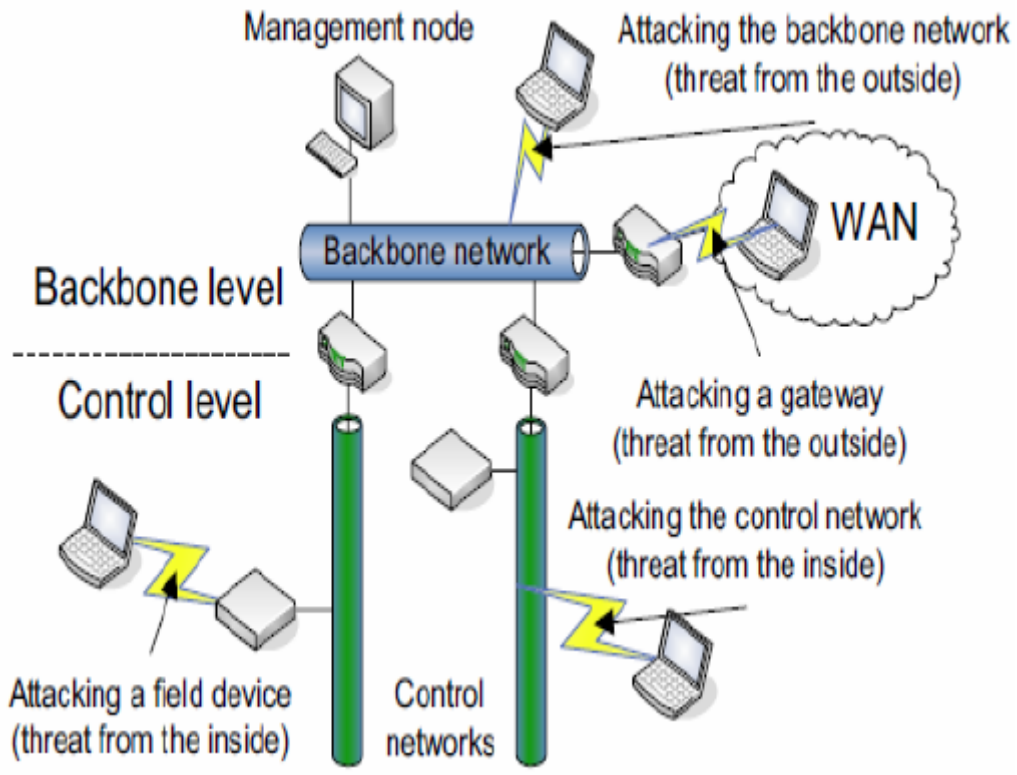


Рисунок 2.1 - Дворівнева модель і загрози безпеки в САБ [21]

Зловмисники можуть спробувати маніпулювати (перехоплювати, модифікувати, фабрикувати або переривати) трафік (Рисунок 2.1) в контрольній

або магістральній мережі (атакуючи мережу) [21].

Маніпулюючи цінами на електроенергію, зловмисник може зменшити свій рахунок за рахунок збільшення рахунку інших. Автори [37] запропонували техніку протидії, яка може ефективно виявляти маніпуляції з цінами на електроенергію.

З метою забезпечення безпеки та безпеки систем віддаленого моніторингу та управління автори в [38] пропонують політику виключного телефонного зв'язку та стратегію віртуального середовища. Демонстраційна система дозволяє користувачеві легко контролювати та контролювати охоронну камеру, центральне опалення, мікрохвильову піч та пральну машину з будь-якого місця за допомогою мобільних телефонів.

Автори в літературі [39] визнали основні атаки на навколишнє середовище розумного будинку, а саме:

1) Підслуховування.

2) Відмова в обслуговуванні (DOS).

3) Викрадення.

4) Напади на нори та червоточини.

У літературі [40] представлена модель безпеки для захисту потоку інформації в домашній мережі інтелектуальної мережі. Запропонована модель здатна ефективно управляти потоком інформації у домашній мережі, використовуючи конфіденційну політику щодо захисту конфіденційної інформації, не впливаючи на нормальну функціональність HAN.

Автори в літературі [41] пропонують систему (Seeing-Is-Believing), яка використовує штрих-коди та телефони з камерою як візуальний канал для перевірки автентичності, яку можна перевірити людиною. Цей канал виключає атаки "людина посередині" проти протоколів встановлення ключів на основі відкритого ключа. Візуальний канал має бажану властивість, що забезпечує демонстративну ідентифікацію сторін, що спілкуються, гарантуючи користувачеві, що його або її пристрій спілкується з цим іншим пристроєм.

Fei Zuo та Peter H. N представили швидку вбудовану систему розпізнавання

обличчя для розумних домашніх додатків. Система вбудована в мережеве домашнє середовище та забезпечує персоналізовані послуги шляхом автоматичної ідентифікації користувачів [42].

Зв'язок між базовою станцією (центральним концентратором) та віддаленим пристроєм (смартфоном) може бути легко порушений, якщо не вжити заходів безпеки. Для забезпечення автентифікації та цілісності повідомлень автори [39] пропонують модель захисту середовища розумного будинку за допомогою смарт-телефону. Запропонована модель включає потужний симетричний блок-шифр із низьким енергоспоживанням: AES256, обмін ключами Ephemeral Diffie-Hellman для полегшення управління ключами для центрального концентратора та хеш-функції на основі смартфонів та RC4 як функції цілісності повідомлень.

Ця книга в [43] представила інтелектуальну систему спостереження за домашньою безпекою на основі протоколу ZigBee. Система здатна виявляти та класифікувати вторгнення, щоб відкинути помилково позитивні та негативні тривоги.

2.3 Прогалина дослідження

Проводячи цей огляд літератури, ми бачимо, що більшість наведених вище літератур про розумні будинки зосереджуються головним чином на можливих проблемах безпеки, які можуть трапитися з розумним середовищем.

Багато питань безпеки повторюються різними авторами в різні роки, і деякі з них відрізняються. Згідно з малюнком 7, я не бачу жодного паперу, який би охоплював всю архітектуру розумних будинків від будинку або до віддаленого сервера.

Вони зосереджуються лише на деяких частинах системи, і в своїй дисертації я збираюся покрити цей недолік у дослідженні шляхом проведення комплексної оцінки ризику безпеки для всієї системи.

Крім того, у цих роботах бракує відповідних можливих рішень чи контрзаходів щодо кожної згаданої загрози.

Ні наслідки, ні рекомендації не були представлені в їх роботах. Для дослідження цього розриву були визначені питання дослідження.

2.4 Підсумки

Ризик безпеки в розумному будинку - це можливість заподіяння шкоди або втрат, таких як небажані дії людей чи природи з негативними наслідками. Ці ризики потрібно вирішувати шляхом впровадження засобів контролю, щоб протистояти основній загрозі та мінімізувати вплив.

Безпека відноситься до виявлення зловмисної поведінки, як, наприклад, грабіжники, несанкціонований доступ до розумного домашнього середовища. Захист від зловмисних зловмисників, які роблять замах контроль системи має вирішальне значення. Для різних типів інтелектуальних приладів існують серйозні виклики безпеці, які необхідно вирішити, щоб реалізувати різні види їх справжніх переваг.

У своєму огляді літератури, посилаючись на роботу інших людей, я зосередився на виборі питань безпеки, спробував дати адекватне резюме їхньої роботи, і ці резюме були синтезовані та упорядковані відповідно до основних елементів розумного будинку, описаних у

Глава 2. Цей огляд літератури визначив перш за все проблеми безпеки в будівельних блоках системи автоматизації будинку, які потребують вирішення. Потім коротко описано ризик безпеки в розумному будинку, який потрібно вирішити та пом'якшити заради безпеки та безпеки.

Ми можемо завершити переліком, що вони вже зробили і що я збираюся робити:

Вони вже зробили: Вони цього не зробили (я їх зроблю):

У своїй роботі автори описали різні аспекти, такі як використовувані технології, моделі, архітектури для розумного будинку середовища та безпеки.

Вони не розглядають загрози безпеці, пов’язані з ними можливі контрзаходи.

Вони заснували безліч різних систем безпеки проблеми, пов'язані із середовищами РД.

Вони не розглядають всю систему розумного будинку, а зосереджуються лише на окремих частинах системи. Для будь-якої системи захищений, його слід вважати частиною для частини (усі підсистеми), щоб мінімізувати ризики безпеки для неї.

Безпека відноситься до виявлення зловмисної поведінки, як, наприклад, грабіжники, несанкціонований доступ до розумного домашнього середовища. Захист від зловмисних зловмисників, які роблять замах контроль системи має вирішальне значення. Для різних типів інтелектуальних приладів існують серйозні виклики безпеці, які необхідно вирішити, щоб реалізувати різні види їх справжніх переваг.

Вони погоджуються щодо виявлених ризиків для безпеки, оскільки деякі з них виявляються різними авторами в різні роки.

Вони не представляють негативних наслідків ризиків. Між їх статтями та темою існує суттєва відповідність. Жодних рекомендацій зацікавленим сторонам розумного будинку.

Крім того, мій огляд літератури визначив прогалини у дослідженні, а саме:

1) Які загрози безпеці виникають від Smart Homes на базі IoT?

2) Які наслідки цих загроз (Вплив)?

3) Чи є до них відповідні заходи протидії?

4) Що рекомендувати користувачам?

3 РОЗРОБЛЕНА СИСТЕМА ОЦІНКИ БЕЗПЕКИ

Для того, щоб мати можливість відповісти на вищезазначені питання дослідження, необхідно вибрати відповідну методологію дослідження. Методологічний підхід спрямований на забезпечення надійності результатів, дозволяючи всебічну оцінку ризиків, зосереджуючись головним чином на інформаційних активах. Підхід аналізує, як інформація використовується

користувачів або систем. Крім того, він зосереджується на місці, де живе інформація, і на тому, як вона піддається ризикам. Інші критично важливі активи можна визначити та оцінити, виявивши зв’язок між ними та інформаційним активом. Система надає вказівки, робочі аркуші та анкети для проведення оцінки ризику.

Тому дана система добре підходить для відповіді на мої дослідницькі запитання, оскільки він має вісім етапів, які можна відобразити для вирішення проблем дослідження. Ми можемо згрупувати кроки методології (вісім етапів) за чотирма основними етапами.

3.1 Розподіл кроків системи на 4 фази для вирішення поставленої задачі

1) Встановити критерії вимірювання ризику.
2) Розробка профілю активів інформації.
3) Визначити контейнери інформаційного майна.
4) Визначити питання, що викликають занепокоєння.
5) Визначити сценарії загрози.
6) Визначити ризики.
7) Проаналізуйте ризики.
8) Визначити підхід пом’якшення наслідків.

Ці вищезазначені кроки будуть виконані спеціально докладно для ідентифікованого критично важливого інформаційного ресурсу в главі 5, розділ 5.6 (Процес оцінки ризику безпеки).

3.1.1 Фаза 1 – Встановлення драйверів

На цьому етапі (Крок 1) створюється основа для оцінки ризику інформаційних активів, розробляючи набір критеріїв оцінки ризику для розумного будинку.

Ці критерії дозволяють виміряти ступінь впливу зацікавлених сторін розумного будинку у випадку виникнення ризику для інформаційного активу. Окрім визнання масштабу впливу, нам потрібно визначити найбільш значну область впливу.

Ці критерії відображають цілий ряд областей впливу, важливих для зацікавлених сторін розумного будинку. Наприклад, сфери впливу можуть включати охорону здоров’я та безпеку користувачів, фінанси, репутацію, закони та правила тощо. Отже, створюємо ці критерії в кількох сферах впливу, а потім ставимо їх пріоритетами від найважливіших до найменших. Найважливіша категорія отримує найвищий бал (5), а найменш важлива - найнижчий (1).

3.1.2 Фаза 2 – Профілювання активів

На цьому етапі (кроки 2 та 3) спочатку визначаються критично важливі інформаційні ресурси, а потім складається їхій профіль.

У процесі профілювання встановлюються чіткі межі для активу, визначаються його вимоги до безпеки, а потім визначаються усі місця, де асктив зберігається, транспортується або обробляється, або де ці активи використовуються власниками розумних будинків або автоматизаційна система розумного будинку, як здійснюється доступ до активів та хто відповідає за ці активи. Документується логічні, технічні, фізичні та людські активи.

Таким чином, можна визначити точки, в яких вимоги безпеки (Конфіденційність, Цілісність та Доступність) інформаційного активу порушуються чи якимось чином їхні активи не мають відповідних задовільняючих умов.

3.1.3 Фаза 3 – Визначення загроз

У цій фазі (кроки 4 та 5) зосередження на виявленні загроз щодо ідентифікованих активів контексті місць, де інформаційний актив зберігається,

транспортується або обробляється. Області, що викликають занепокоєння (вразливості), охоплюються та розширюються на сценарії загрози, що додатково деталізують властивості загрози. Визначаються конкретні загрози, які можуть негативно вплинути на безпеку об’єкта.

3.1.4 Фаза 4 – Визначення та пом’якшення ризиків

На заключному етапі (крок 6, крок 7 та крок 8) визначаються ризики для інформаційних активів, визначаючи, як сценарії загрози можуть вплинути на розумний дім (наслідки), та їх аналіз. Нарешті, після цього кроку визначається стратегія зменшення наслідків для кожного з виявлених ризиків.

Загроза + Вплив = Ризик.

Аналізуємо ризики та присвоїмо якісне значення для опису ступеня впливу на зацікавлені сторони розумного будинку, коли реалізується сценарій загрози та наслідки впливу (оцінка ризиків). Значення впливу визначається критеріями оцінки ризику. Буде використовуватись оціночну інформацію для визначення пріоритетних заходів щодо пом’якшення наслідків.

Потім починаємо сортувати виявлені ризики за їх оцінками. Класифікуємо ризики та призначаємо підхід до пом’якшення для кожного з них. Нарешті, ми розробляємо стратегію зменшення наслідків для всіх профілів ризику, які було вирішено зменшити.

3.2 Мотивація при розробці системи

Виконуючи оцінку ризику безпеки, важливо знати, що захищати і чому.

Очевидно, що захист інформаційних активів є необхідною складовою захисту безпеки розумного будинку, оскільки він визначає майбутнє та успіх системи розумного будинку. Ось чому в цій роботі я хотів зосередитись головним чином на безпеці інформаційних активів і на тому, де ця інформація живе, проводячи оцінку ризику безпеки в розумному будинку. Якщо ми зосередимося на інформаційних активах в оцінці, всі інші важливі активи можуть бути легко оцінені і обробляються як місця розташування інформаційних активів, де вони

проживають. Розроблена система є точною для цієї мети, оскільки вона забезпечує найкращий роадмап для досягнення моїх цілей, а саме відповідає на мої запитання щодо дослідження:

1) Які загрози безпеці виникають від Smart Homes на базі IoT?

2) Які наслідки цих загроз (Вплив)?

3) Чи можна запропонувати відповідні контрзаходи?

4) Що рекомендувати користувачам?

Аналізуємо ризики та присвоїмо якісне значення для опису ступеня впливу на зацікавлені сторони розумного будинку, коли реалізується сценарій загрози та наслідки впливу (оцінка ризиків). Значення впливу визначається критеріями оцінки ризику. Буде використовуватись оціночну інформацію для визначення пріоритетних заходів щодо пом’якшення наслідків.

Система оцінки найкраще підходить для відповіді на проблеми дослідження порівняно з іншими методологіями оцінки ризику безпеки, які були розглянуті. Він складається з восьми етапів, які організовані у чотири фази, і ці кроки легко можна скласти для вирішення моїх дослідницьких проблем. За допомогою робочих аркушів, передбачених методологією, чи можемо ми охопити результати кожного кроку в оцінці ризику та використати їх для вкладання в наступний крок, який наступний. Таким чином, це дозволяє нам постійно зосереджуватись на активі поетапно під час процесу оцінки ризику та легше досліджувати проблемні ситуації.

4 ДОСЛІДЖЕННЯ РИЗИКІВ БЕЗПЕКИ ЗА ДОПОМОГОЮ РОЗРОБЛЕНОЇ СИСТЕМИ

У наступних розділах ми проведемо оцінку ризику безпеки для розумного будинку на основі IoT із використанням підходу розробленої системи оцінки.

Як методологія, так і розумний дім на основі IoT вже описані в попередніх розділах. Будуть визначені критично важливі інформаційні ресурси для розумного будинку, а також його вразливі місця та можливі загрози. Тоді буде запропоновано план зменшення цих ризиків.

Перш ніж ми почнемо застосовувати процеси методології оцінки ризику безпеки покроково, нам спочатку потрібно визначити саму оцінку ризику безпеки, а також усі терміни, якими ми є

збираються використовувати через процеси проведення оцінки ризику безпеки лише для того, щоб було легко зрозуміти.

Метою оцінки ризику є розуміння існуючої системи та середовища, виявлення ризиків та їх наслідків шляхом аналізу зібраної інформації.

Метою оцінки ризику для безпеки є максимізація захисту конфіденційності, цілісності та доступності шляхом надання рекомендацій, не впливаючи на функціональність та зручність використання.

4.1 Що таке оцінка безпеки?

Існує багато визначень, даних терміну оцінка ризику безпеки. Відповідно до «Посібника з управління ризиками» NIST [45], Оцінку ризиків безпеки можна визначити як процес виявлення загроз, ймовірності виникнення, наслідків, а потім механізми захисту для пом'якшення наслідків.

Оцінка ризику є найважливішим аспектом будь-якого дослідження безпеки. За допомогою всебічного вивчення та оцінки ризику можна визначити заходи щодо пом’якшення наслідків. Він може бути використаний як базовий для показу, скільки змін потрібно для того, щоб відповідати вимогам безпеки.

Без оцінки ризиків впроваджені рішення безпеки ризикують не відповідати

бажаним цілям безпеки системи розумного автоматизованого будинку.

Це допомагає кінцевим користувачам прийняти правильне рішення щодо своїх розумних будинків, а також дає нам можливість робити рекомендації щодо вдосконалення.

4.2 Термінологія

Ось деякі визначення цих термінів, які ми будемо використовувати в рамках нашого процесу оцінки ризиків безпеки.

- **Актив** - ціннісний ресурс. Це може бути процес, технологія, фізичний об’єкт або людина.
- **Інформаційний актив**: Це цінна інформація для організації, яку люди можуть переносити, зберігати у фізичних носіях або передавати та обробляти в електронному вигляді.
- **Контейнер** інформаційного активу - Контейнером інформаційного активу є місце, де живе інформація. Контейнери можуть бути технічними (програмне забезпечення, програмне забезпечення, сервери та мережі), фізичними (на паперах, компакт-дисках, DVD-дисках) або людьми (хто знає про інформацію).
- **Критично важливий інформаційний актив**: Найважливіший актив, який завдає величезної шкоди організації, якщо її вимоги до безпеки порушуються.
- **Загроза** - потенціал події, яка може завдати шкоди активу або скомпрометувати його. Він генерується, коли актор загрози використовує вразливість.
- **Вплив** - відчутний або нематеріальний вплив загрози, що здійснюється на актив.
- **Ризик** - це поєднання загрози та впливу на об’єкт атаки. Ризик - це можливість заподіяння шкоди чи збитків і складається з події, наслідку та невизначеності.
- **Пом'якшення наслідків** - Дія зменшення серйозності ризиків або зменшення ризику організацій за допомогою різних заходів.

4.3 Вимоги до безпеки захисних засобів інформації

Кожен захищений інформаційний ресурс має конфіденційність, цілісність та доступність (КЦД) як вимоги безпеки для захисту та продовження. Ці вимоги живуть з інформаційним активом скрізь, поки він живе корисно.

Крім того, вимоги безпеки є основним елементом розробки та реалізації планів щодо обмеження ризиків. Тому необхідно враховувати вплив ризиків на ці вимоги безпеки та на план пом'якшення наслідків. Вимоги безпеки або цілі безпеки - це вимоги, що характеризують спосіб захисту інформаційного активу (Рисунок 4.1). Тому надзвичайно важливо зберігати конфіденційність, цілісність та доступність інформаційної безпеки.

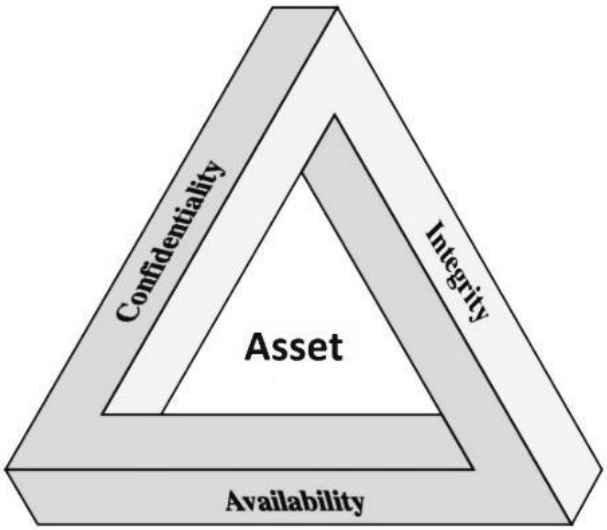


Рисунок 4.1 - Триада вимог безпеки

4.3.1 Конфіденційність

Конфіденційність є важливим фактором у багатьох професіях. В інженерній професії конфіденційність особливо турбує стосунки зайнятого інженера зі своїм роботодавцем, особливо колишнім роботодавцем. Протягом трудової діяльності інженери часто отримують глибокі знання багатьох аспектів процесів свого роботодавця та накопичені знання.

Кодекс етики професійних інженерів Онтаріо (кодифікований Законом про

професійних інженерів (Онтаріо)) навіть передбачає, що інженер зобов'язаний піклуватися про свого роботодавця і повинен розглядати інформацію, отриману під час їх роботи, як конфіденційну.

Це набагато сильніший стандарт, який міститься в етичному кодексі багатьох інших професій, що дозволяє, натомість, у більшості інших професій бути предметом договору, натомість підлягати дисциплінарним заходам з боку керівних органів професії.

Судова практика Канади та Великобританії включає деякі рішення та коментарі, які намагаються визначити, наскільки суворо слід приймати вимоги конфіденційності, що стосуються інженерів. Наприклад, рішення Верховного суду Канади Lac Minerals [2009], посилаючись на англійське рішення Cranleigh Precision Engineering Ltd. V Bryant et al. [2016] встановлює, що працівник не може використовувати конфіденційну інформацію як «плацдарм» для заподіяння шкоди роботодавцю, який є законним власником інформації, і покладає на колишнього працівника, який бажає використовувати інформацію, довести, що вона не була отримана порушення конфіденційності.

Деякі подібні випадки, пов'язані з передбачуваними порушеннями довірчих обов'язків з боку інженерів, дотримувались подібної логіки, деякі з них призводили до великих розрахунків, хоча інші використовують різні аргументи, що призводило до рішення, що порушення не було.

4.3.2 Цілісність

Гарантування того, що інформаційний актив залишається у запланованому стані та за призначенням. Це гарантує, що інформація достовірна і точна.

Технічна цілісність - це термін, що застосовується до інженерних дисциплін, пов’язаних із функціями проектування, забезпечення та перевірки, що забезпечують відповідність виробу, процесу або системи відповідним та передбачуваним вимогам за заявлених умов експлуатації. Застосування цих дисциплін не повинно негативно впливати на програму, але насправді повинно мінімізувати витрати, графік, технічні та юридичні ризики та покращити загальну вартість життєвого циклу.

Цілісність активів - це термін, який стосується процесу, що підвищує експлуатаційну надійність, безпеку та захист активів, одночасно допомагаючи максимізувати ефективність роботи заводу та пом'якшуючи постійні виклики та небезпеки, що стоять перед важкими галузями промисловості, такими як нафта та газ, енергетика та атомна енергетика.

Це також розглядається як дисципліна та професія набуття та застосування наукових, математичних, економічних, соціальних, юридичних та практичних знань для забезпечення та перевірки функцій, які забезпечують відповідність продукту, процесу чи системи (та її відповідність) своїм відповідним та передбачувані вимоги щодо безпеки, правові та ділові вимоги.

У проспекті після Макондо (див. (Вибух глибоководного горизонту) та світі Piper Alpha роль інженерії цілісності була піддана посиленому контролю. Мало того, що добре керована інженерна програма цілісності може допомогти операторам визначити та зменшити ризики безпеки до їх ескалації, але зосередження уваги на цілісності активів також може зіграти важливу роль як у досягненні операційної досконалості, так і в продовженні життя застарілих активів.

Типовими обов'язками інженера доброчесності є координація ефективного та економічно ефективного здійснення інспекцій та програм управління цілісністю та забезпечення цілісності заводських установок, включаючи всі наземні та морські споруди, трубопроводи, стаціонарне обладнання, системи трубопроводів тощо.

4.3.3 Доступність

Гарантування того, що інформаційний актив залишатиметься доступним для уповноважених осіб.

Визначається як ймовірність того, що відремонтована система або елемент системи функціонують у певний момент часу за певного набору екологічних умов. Доступність залежить від надійності та ремонтопридатності та детально обговорюється далі в цій темі (ASQ 2011).

Помилка - це подія (події) або непрацездатний стан, при якому будь-який

предмет або частина предмета не виконує або не буде виконувати функції, як зазначено (GEIA 2008). Механізм відмови - це фізичний, хімічний, електричний, термічний або інший процес, що призводить до відмови (GEIA 2008).

В комп'ютеризованих системах дефект або несправність програмного забезпечення може бути причиною несправності (Laprie 1992), якій могла передувати помилка, яка була внутрішньою для елемента. Режим відмови - це спосіб або наслідок механізму, за допомогою якого елемент виходить з ладу (GEIA 2008, Laprie 1992.). Серйозність режиму відмови полягає у величині його впливу (Laprie 1992).

4.4 Обсяг роботи

Основна увага системи - це інформаційні активи. Усі інші критично важливі активи можна ідентифікувати та оцінити, виявивши зв’язок між ними та інформаційним активом.

Якщо бізнес хоче досягти успіху, його інформацію, яка є критично важливим і стратегічним активом, слід захищати або надійно керувати ним. Це те саме у випадку розумного будинку, критично важливі інформаційні ресурси та контейнери повинні бути захищені, інакше буде великий негатив впливає на зацікавлені сторони розумного будинку, особливо на мешканців, різними способами. Тому ми повинні чітко розуміти, що ми намагаємось захистити і чому, перш ніж вибирати конкретні рішення.

Як ми вже згадували у розділі 2.2, існують різні типи застосування розумних будинків;

Розумні будинки для безпеки, Розумні будинки для догляду за людьми, Розумні будинки для охорони здоров’я, Розумні будинки для догляду за дітьми, Розумні будинки для енергоефективності та Розумні будинки для кращого життя (музика, розваги тощо). Ми розглянемо не всіх, а деякі.

Як було зазначено раніше у розділах, застосування методології буде обмежене лише інформаційною безпекою та її контейнерами в контексті

розумного будинку, і на основі огляду літератури, проведеного в главі 3, було з'ясовано, що існує необхідність проведення (застосування) комплексної оцінки ризику безпеки, яка охоплює або розглядає структуру розумного будинку (розділ 3.2) та висвітлює ризики безпеки, що піддаються критичній інформаційній безпеці у всіх підсистемах системи автоматизації розумного будинку (АСРД), як всередині та зовні розумного будинку, як показано на малюнку 7, а саме:

1) Всередині розумного будинку (внутрішня домашня мережа зв'язку):
   a) Підсистема 1: Серед домашніх пристроїв (датчики та пускачі).
   b) Підсистема 2: між пристроями та домашнім шлюзом.
2) Поза розумним будинком (зовнішня мережа зв'язку):
   a) Підсистема 3: між домашніми шлюзами та Інтернетом.

У цій оцінці ризику безпеки ми розглядаємо і намагаємося знайти ризики безпеки, пов’язані з усіма підсистемами або всіма частинами Системи автоматизованого розумного будинку (АСРД).

Варто згадати, що в розумному будинку існує основна система, яка підключена до всіх інших пристроїв. Це означає, що якщо хакер отримає доступ до основної системи, він може отримати доступ до всіх інших пристроїв.

Ми можемо зазначити, що безпека - це ланцюг, і як ланцюг настільки міцний, як найслабша ланка, система безпеки є настільки ж безпечною, як і найслабша її частина. Зловмисники атакують найслабші частини системи (не найсильніші), оскільки саме ті частини, які найімовірніше легко ламаються. З незахищеної частини або незахищеного пристрою зловмисник отримує доступ до всіх інших пристроїв. Тому важливо не мати будь-якого незахищеного пристрою або частини в АСРД. При проведенні оцінки ризику слід враховувати всі деталі.

Підсистема 1:

У підсистемі 1 є багато пристроїв, які підключені між собою через внутрішню систему зв'язку (дротову або бездротову). Пристрої IoT, оснащені датчиками, будуть виконувати роль колекторів, а вбудовані в виконавчі механізми - як виконавці. Пристрій з обома датчики та виконавчий механізм будуть сприймати і виконувати.

У нас є також контролер пристроїв, який підключений до декількох домашніх пристроїв і складається з інтерфейсного модуля, модуля бездротового зв'язку та мікроконтролера для контролю його роботи.

Підсистема 2:

Ця підсистема складається в основному з модуля мережевого інтерфейсу, мікроконтролера, бази даних, веб-сервера та інтерфейсу користувача. Інтерфейс користувача - це веб-сторінка або програма певної платформи (Windows, Android або iOS), яка підключається до бази даних через веб-сервер. База даних містить всю інформацію про всі домашні пристрої та їх поточний стан.

Користувачеві необхідно пройти автентифікацію перед тим, як отримати доступ до основної системи та контролювати систему розумного будинку, надаючи правильні облікові дані користувача (ім’я користувача та пароль або облікові дані користувача).

Мікроконтролер - це мозок, який управляє всіма операціями та комунікаціями в розумній домашній мережі. Модуль мережевого інтерфейсу управляє всім зв’язком між контролерами домашнього пристрою та системою, що складається з мікроконтролера, веб-сервера, користувацького інтерфейсу та бази даних.

Підсистема 3:

У підсистемі 3 ми маємо деякі частини, а саме Домашній маршрутизатор (домашній шлюз), Інтернет та пристрої користувачів, такі як ПК, ноутбук, смартфон та планшети.

Домашній маршрутизатор підключає систему розумного дому до Інтернету. Ця можливість дозволяє користувачам з правильними обліковими даними підключати та керувати своїм розумним будинком віддалено з будь-якого місця за допомогою таких пристроїв, як їхні смартфони, які отримують інформацію з бази даних через веб-сервер.

4.5 Ідентифікація критичних інформаційних засобів

Перш за все, ми повинні знати, що означає інформаційний актив та його критичність (див. Визначення у розділі 4.2), а п.5отім для проведення оцінки ризику нам потрібно визначити колекцію найважливіші (критичні) інформаційні активи, на яких проводиться наша оцінка ризику безпеки з метою їх захисту.

4.5.1 Ідетнифікація критичних інформаційних засобів в АСРД

Очікується, що ці інформаційні ресурси стануть основними об’єктами зловмисної атаки:

1) Інформація, зібрана пристроями (датчиками) / Інформація про стан розумного будинку (Підсистема 1).

2) Відеопотік камери спостереження (Підсистема 1).

3) Повноваження користувача (ім’я користувача та пароль) (Підсистема 2).

4) Інформаційні ресурси (картинки, документи, музика) (Підсистем 1-2).

5) Інформація про розумне налаштування будинку або Посібники користувача для побутової техніки (Підсистем 1-2).

6) Інтелектуальна структура будинку/інформація про запаси (Підсист. 1-2).

7) Інформація про журнали (Підсистема 2).

8) Інформація (дані), що передаються через домашній шлюз (Підсистема 3).

9) Мобільний пристрій / Пристрій користувача (Підсистема 3).

10) Інформація про відстеження місцезнаходження (Підсистема 3).

Всередині розумного будинку (внутрішня домашня мережа зв'язку):

Підсистема 1. Серед домашніх пристроїв (датчики та пускачі):

1) Інформація, зібрана пристроями (датчиками) / Інформація про стан розумного будинку.

2) Відеопотік камери спостереження.

Підсистема 2. Між пристроями та домашнім шлюзом:

1) Повноваження користувача (ім’я користувача та пароль).

2) Інформаційні ресурси (картинки, документи, музика).

3) Інформація про розумне налаштування будинку або Посібники

користувача для побутової техніки.

4) Інтелектуальна структура будинку / інформація про запаси.

5) Інформація про журнали.

Поза розумним будинком (зовнішня мережа зв'язку):

Підсистема 3. Між домашніми шлюзами та Інтернетом:

1) Інформація (дані), що передається через домашній шлюз.

2) Мобільний пристрій / Пристрій користувача.

3) Інформація про відстеження місцезнаходження.

4.6 Процес оцінки безпеки

У цьому розділі ми проводимо (всебічну) оцінку ризику безпеки, проходячи всі етапи розробленої системи оцінки. Для проведення оцінки ризику ми будемо використовувати створені шаблони.

Як ми вже згадували раніше, система передбачає 8 етапів, організованих у 4 етапи (див. Малюнок 12). За допомогою робочих аркушів, передбачених методологією, чи можемо ми охопити результати кожного кроку в оцінці ризику та використати їх для вкладання в наступний крок, який наступний. Індивідуальні кроки застосовуються до кожного ідентифікованого інформаційного активу. Нижче кожен крок описаний більш докладно.

4.6.1 Встановлення критеріїв вимірювання ризиків

Метою цього кроку є встановлення того, що може бути наслідком ризику для бізнес-стратегії та цілей чи критичних факторів успіху (комерційні зацікавлені сторони) та для мешканців розумного будинку (некомерційні зацікавлені сторони). Цей етап складається з двох видів діяльності. У першій діяльності ми визначаємо набір якісних та кількісних заходів для оцінки впливу ризиків на виявлені критично важливі інформаційні активи (Розділ 4.5.1) у Розумному Домі. Під час другого заходу ми надаємо пріоритет зонам впливу відповідно до їх важливості для власника АСРД або зацікавлених сторін.

Категорії критеріїв оцінки включають:

1) Репутація.

2) Впевненість та довіра клієнтів.

3) Життя, здоров’я, безпека.

4) Штрафи та законодавчі санкції, спричинені недотриманням вимог.

5) Фінансові.

6) Продуктивність.

Ми розглянемо їх у відповідних секціях даної роботи.

Таблиця 4.1 - Критерії вимірювання ризиків - Репутація та впевненість клієнта

КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКУ - РЕПУТАЦІЯ ТА ДОВІРА КЛІЄНТА			
Зона впливу	**Низька**	**Середня**	**Висока**
Репутація (Некомерційні зацікавлені сторони)	На репутацію некомерційних зацікавлених сторін впливає мінімум, а для відновлення вимагаються незначні зусилля чи витрати.	Репутація некомерційних зацікавлених сторін пошкоджена. Час і зусилля, необхідні для відновлення, менше 10 тис. Дол. США.	Репутація некомерційних зацікавлених сторін безповоротно знищується або пошкоджується. Більше $ 10 тис. Часу та зусиль, необхідних для відновлення.
Репутація (Комерційні зацікавлені сторони)	На репутацію комерційних зацікавлених сторін впливає мінімум, а для відновлення потрібно майже ніяких зусиль чи витрат.	Репутація комерційних зацікавлених сторін пошкоджена, а часу та зусиль, необхідних для відновлення, менше 100 тис. Дол.	Репутація комерційних зацікавлених сторін безповоротно знищується або пошкоджується. Більше $ 100 тис. Часу та зусиль, необхідних для відновлення.
Втрати клієнта (Комерційні зацікавлені сторони)	Впасти менше 5% від кількості клієнтів в результаті втрати довіри.	Зниження на 5-10% клієнтів через втрату довіри.	Понад 10% зменшення кількості споживачів через втрату довіри.
Інші:			

Перш ніж заповнювати результати, нам слід знати, хто є зацікавленими сторонами, коли ми проводимо оцінку ризику в системі автоматизації розумного будинку (АСРД). Зацікавлені сторони в цьому випадку можна класифікувати на комерційні зацікавлені сторони (постачальники, постачальники інфраструктури, сторонні постачальники програмного та апаратного забезпечення тощо) та некомерційні зацікавлені сторони (державні установи та муніципалітети та кінцеві споживачі (жителі) (Таблиця 4.1).

Примітка: При встановленні критеріїв оцінки ризику ми враховуватимемо як зацікавлені сторони, так і моніторингові суми та відсотки на першому кроці є припущеннями автора.

У таблиці 1 ми бачимо, наскільки збиток від репутації та довіри клієнтів вплине на зацікавлені сторони розумного будинку.

Таблиця 4.2 - Критерії вимірювання ризиків - Фінансові

КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКІВ - ФІНАНСОВІ			
Зона впливу	**Низька**	**Середня**	**Висока**
Експлуатаційні та матеріальні витрати (Некомерційні зацікавлені сторони: жителі)	Одноразова фінансова втрата (Некомерційні зацікавлені сторони: жителі)	Щорічні експлуатаційні витрати збільшуються на 2-5%.	Щорічні експлуатаційні витрати збільшуються більш ніж на 5%.
Втрата доходу (Комерційні зацікавлені сторони)	Менше 5% річних втрат доходу.	5-10% річних втрат доходу.	Більше 10% річних втрат доходу.
Одноразова фінансова втрата (Некомерційні зацікавлені сторони: жителі)	Одноразова фінансова вартість менше 10 тис. Доларів.	Одноразові фінансові витрати від 10 000 до 25 000 доларів	Одноразові фінансові витрати перевищують $ 25 тис
Інші:			

У таблиці 4.2 наведено критерії для сфери фінансового впливу. Ми враховуємо операційні та матеріальні витрати для некомерційних зацікавлених сторін (Кінцевих споживачів), втрату доходу для комерційних зацікавлених сторін (постачальників, постачальників, постачальників тощо) та одноразові фінансові втрати для некомерційних зацікавлених сторін (Кінцевих споживачів). Ми представляємо це з різними відсотками та грошовими значеннями за трьома шкалами.

У таблиці 4.3 наведені критерії для зони впливу на продуктивність. Ми вважаємо втрату продуктивності для комерційних зацікавлених сторін. Ми представляємо це з витратами на зрив критерію зі значеннями, як показано на

трьох шкалах.

Таблиця 4.3 - Критерії вимірювання ризиків - Продуктивність

КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКІВ - ПРОДУКТИВНІСТЬ			
Зона впливу	**Низька**	**Середня**	**Висока**
Години роботи персоналу (Комерційні зацікавлені сторони)	Робочий час персоналу збільшує витрати на оплату праці менш ніж на $50 тис.	Час роботи персоналу збільшує витрати на оплату праці від $50 до $100 тис.	Робочий час персоналу збільшує витрати на оплату праці більш ніж на $100 тис.
Інші:			

У таблиці 4.4 наведено критерії для зони впливу на безпеку та здоров'я. Ми розглядаємо актив людського життя (мешканців), напр. життя, здоров'я та безпека кінцевих споживачів розумного будинку (некомерційні зацікавлені сторони) та представляти їх зі значеннями, як показано у трьох шкалах.

Таблиця 4.4 - Критерії вимірювання ризиків - Безпека та здоров’я

Зона впливу	**Низька**	**Середня**	**Висока**
Життя (Некомерційні зацікавлені сторони: жителі)	Жодних втрат або значної загрози життю кінцевих користувачів. Відсутність регуляторної відповіді.	Життя користувачів загрожує, але, отримавши медичну допомогу, вони одужають. Просто мінімальна відповідь регуляторів.	Втрата життя користувачів. Значна відповідь регуляторних органів.
Здоров'я (Некомерційні зацікавлені сторони: жителі)	Мінімальне, негайно піддається лікуванню погіршення здоров’я користувачів із відновленням протягом днів. Мінімальна регуляторна реакція.	Тимчасові або відновлювані порушення здоров'я користувачів. Лише мінімальна регуляторна реакція.	Постійне порушення значущих активів здоров’я користувачів. Значна відповідь регуляторних органів, що включає розслідування
Безпека (Некомерційні зацікавлені сторони: жителі)	Безпека кінцевого споживача ставиться під сумнів, але відповідь регуляторів відсутня.	Це впливає на безпеку кінцевого користувача. Мінімальна регуляторна реакція.	Безпека кінцевого користувача порушує. Значна відповідь регуляторних органів, що включає розслідування
Інші:			

У таблиці 4.5 наведено критерії вимірювання ризику - Штрафи та юридичні санкції. Ми розглядаємо штрафи, позови та розслідування проти комерційних зацікавлених сторін, якщо з ними щось піде не так.

Таблиця 4.5 - Критерії вимірювання ризиків - Штрафи та юридичні покарання

Зона впливу	Низька	Середня	Висока
Штрафи (Комерційні зацікавлені сторони)	Штрафи менше $ 100 тис. Стягуються.	Стягуються штрафи від 100 до 250 тис. Доларів.	Штрафи, що перевищують 250 тис. Доларів, стягуються.
Позови (Комерційні зацікавлені) сторони)	Жоден позов або позови на суму менше 100 тис. Дол. США не реєструються проти комерційних зацікавлених сторін.	Жоден позов або позови від 100 до 500 тис. Доларів проти комерційних зацікавлених сторін не реєструються.	Жоден позов або позови на суму понад 500 тис. Доларів не реєструються проти комерційних зацікавлених сторін.
Розслідування (Комерційні зацікавлені сторони)	Жодних запитів від державних та інших слідчих організацій	Запит інформації від уряду чи іншої слідчої організації.	Поглиблене розслідування порушується проти продавців урядом чи іншою слідчою організацією.
Інші:			

Таблиця 4.6 дає нам можливість визначити додаткові сфери впливу. Однак ми не будемо розглядати будь-яку додаткову область удару, тому цей аркуш буде залишено порожнім.

Встановивши наведені вище критерії оцінки ризику, ми сформували основу для оцінки ризику визначених інформаційних активів. Як ми вже згадували раніше, ці критерії допомагають нам виміряти ступінь впливу розумного будинку, якщо реалізується ризик для інформаційного активу.

Зараз ми створили збірник критеріїв оцінки ризику, що відображають різні сфери впливу, які є життєво важливими для зацікавлених сторін АСРД, як комерційних, так і некомерційних зацікавлених сторін. Наші сфери впливу включали репутацію та довіру споживачів, фінансові показники, продуктивність праці, безпеку та здоров’я користувачів і, нарешті, штрафи та юридичні санкції. Потім нам потрібно їх ранжувати та розставляти за пріоритетами та призначати

значення від найважливіших до найменш важливих, тому що ми повинні визнати, які зони впливу є найбільш значущими. Ми використовуємо цей рейтинг та встановлення пріоритетів пізніше під час оцінки ризику, і це допоможе нам розробити відносний показник ризику, який визначає, як боротися з ризиками, які ми будемо ідентифікувати в оцінці. Найважливіша категорія отримує найвищий бал (5), а найменш важливий - найнижчий (1), як показано в таблиці 4.6.

Таблиця 4.6 - Приорітезація зон впливу

ПРИОРІТЕЗАЦІЯ ЗОН ВПЛИВУ	
ПРИОРІТЕТ	ЗОНИ ВПЛИВУ
4	Репутація та впевненість клієнта
3	Фінансові
2	Продуктивність
1	Безпека та здоров’я
0 (не застосовується)	Клієнт-специфічні

4.6.2 Розробка інформаційного профілю достоїнств

На цьому кроці ми профілюємо критично важливі інформаційні ресурси, які визначені критичними (див. Підрозділ 4.5.1). У процесі профілювання ми встановлюємо чіткі межі для активу, визначаємо його вимоги до безпеки, а потім визначаємо всі місця, де актив зберігається, транспортується або переробляється. Це дозволить нам повністю визначити всі вразливі точки інформаційних активів. Відповідно до заявлених критеріїв ми проводимо оцінку та аналіз профільних активів.

У процесі профілювання ми встановлюємо чіткі межі для активу, визначаємо його вимоги до безпеки, а потім визначаємо всі місця, де актив зберігається, транспортується або обробляється, або де ці активи використовуються власниками розумних будинків або АСРД, як активів доступ, і хто відповідає за активи.

Щоб зробити його менш складним, на цьому кроці ми продовжуємо процес оцінки ризиків і починаємо розглядати підсистеми, описані в розділі 4.4, щоб чітко пояснити, де розташовані ризики в системі розумного будинку (особливо

всередині або зовні розумний дім). Ми повторюємо всі кроки (від кроку 2 до кроку 8) для кожного ідентифікованого інформаційного ресурсу:

Всередині розумного будинку (внутрішня домашня мережа зв'язку):

Підсистема 1: Серед домашніх пристроїв (датчики та пускачі)

1) Інформація, зібрана пристроями (датчиками) / Інформація про стан розумного будинку.

2) Відеопотік камери спостереження Усередині розумного будинку (підрозділ 1) ми маємо два вищезазначені інформаційні ресурси, і ми вивчити активи безпеки їх. Після цього ми починаємо з активів безпеки, пов'язаних з підсистемою 2.

Далі наведено опис критично важливих інформаційних ресурсів (Інформація, зібрана пристроями (датчики) / Інформація про стан розумного будинку), як описано вище.

Профіль критичної інформації (інформація, зібрана пристроями (датчики) / інформація про статус розумного будинку).

1) Критичний актив (*Що є критично важливим інформаційним активом?*)

Інформація, зібрана пристроями (датчиками) / Інформація про стан розумного будинку

2) Обґрунтування вибору (*Чому цей інформаційний актив важливий для організації?*)

Ці інформаційні активи дуже важливі, оскільки вони використовуються в повсякденних робочих процесах та операціях системи розумного будинку.

3) Далі він показує поточний стан розумного будинку. Дані датчиків можна використовувати, наприклад для виявлення таких ризиків, як повінь, пожежа, з попередженнями та постійним моніторингом.

4) Опис (*Який узгоджений опис цього інформаційного активу?*)

Цей інформаційний актив визначає результати роботи пристроїв, наприклад він визначає, які дії будуть виконувати виконавчі механізми. Ця інформація визначає безпеку та зручність розумного будинку, що є основними цілями АСРД. Він використовується АСРД як вхід для створення результату. Різні дії, вжиті на

основі цього інформаційного ресурсу. Якщо його безпека порушиться, це суттєво порушить здатність АСРД досягти своїх цілей.

5) Власник (*Хто володіє цим інформаційним активом?***)**

Власник - власник Системи автоматизації розумного будинку (АСРД), який несе основну відповідальність за цей інформаційний актив.

6) Вимоги безпеки (*Які вимоги до безпеки цього інформаційного активу?***)**

- **Конфіденційність.** Лише уповноважений персонал може переглядати цей інформаційний ресурс таким чином: Лише мешканці мають право доступу до цього інформаційного ресурсу. Постачальникам послуг може також знадобитися доступ до цього інформаційного ресурсу для надання правильної послуги згідно з контрактами.

- **Цілісність.** Лише уповноважений персонал може модифікувати цей інформаційний ресурс таким чином: Тільки жителі мають право маніпулювати цим інформаційним активом.

- **Доступність.** Цей актив повинен бути доступний для виконання цією особою таких функцій: Актив повинен бути готовим до використання, коли він потрібен мешканцям або іншим суміжним системам.

Цей актив повинен бути доступний протягом 24 годин, 7 днів на тиждень, 52 тижні на рік. Ці інформаційні ресурси повинні бути доступними цілодобово та без вихідних.

Він повинен бути доступний розумній системі для функціонування. Короткі відключення не викликають великих проблем. Тривале переривання (більше 8 годин) може спричинити значну проблему.

- **Інші.** Цей актив має спеціальні вимоги щодо захисту дотримання нормативних вимог, а саме: /.

7) Найважливіші вимоги безпеки (*Яка найважливіша вимога безпеки цього інформаційного активу?***)**

- **Конфіденційність;**
- **Цілісність;**
- **Доступність;**

- **Інші.**

4.6.3 Визначення інформаційних контейнерів

Визначаючи критично важливі інформаційні активи, потрібно ідентифікувати контейнери інформаційних активів. Контейнером інформаційного активу є місце, де інформація живе. Контейнери можуть бути технічними (програмне забезпечення, апаратне забезпечення, сервери та мережі), фізичними (на паперах, компакт-дисках, DVD-дисках) або людьми (хто знає про інформацію). Вони також можуть бути як внутрішніми, так і зовнішніми для організації. Всі ці контейнери також є частиною аналізу.

В таблиці 4.7 ми вказуємо (технічні, фізичні та персональні) контейнери “Інформація, що збирається пристроями (датчиками) / Інформація про стан розумного будинку”.

Таблиця 4.7 - Карта середовища ризику активів інформації (Технічна) для того, що збирається пристроями (датчики)/Інформація про стан розумного будинку

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. Файл даних	АСРД власник (мешканці)
2. База даних: Інформаційний актив знаходиться на серверах баз даних і веб-сервери.	АСРД власник (мешканці)
3. Внутрішня мережа розумного дому. Вся інформація подорожує по цій мережі.	АСРД власник (мешканці)
4. ПК (робочі станції)	мешканці
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. Інтернет: ці інформаційні ресурси переміщуються в Інтернеті кожного разу, коли кінцевий користувач підключається до АСРД поза будинком за допомогою таких пристроїв, як ПК, смартфон, планшет тощо	

4.6.4 Визначення проблемних зон

Метою цього кроку є визначення проблемних областей. Для кожного ідентифікованого інформаційного активу ми визначаємо конкретні проблеми, які можуть негативно вплинути на безпеку активу. На цьому кроці ми описуємо потенційний вплив, якщо загроза сталася, та деякі умови, що спричиняють це. За допомогою опису, який базується на місцях зберігання, визначених на кроці 3, ми

отримуємо детальне розуміння того, де знаходяться активи під загрозою.

Ми визначаємо проблемні сфери, застосовуючи знання та якийсь здоровий глузд.

4.6.5 Визначення загрозливих сценаріїв

На кроці 5 ми розробляємо сценарії загроз для кожного ідентифікованого інформаційного активу. Сценарій загрози включає один або кілька активів, діючу особу, засіб, мотив та перелік небажаних результатів.

Актор може бути або природним (шторм, повінь, пожежа або інше лихо), автоматизованим (зловмисне програмне забезпечення), або інтелектуальні (злочинець, активіст чи інша потенційно шкідлива людина).

Засіб - це вразливість та використання, що використовуються актором щодо інформаційного активу.

Мотивом є прагнення актора застосувати засоби. Небажаним результатом є пошкодження інформаційного активу. Результат - це завжди вихід з розкриття, модифікації, переривання чи знищення.

Загроза може бути пов'язана з різними факторами, такими як людина, що використовує технічний або фізичний метод, технічні проблеми або будь-яка інша пов'язана з цим проблема.

Отже, цей крок допомагає нам визначити, які сценарії загроз частіше реалізуються. Ми можемо визначити загрозу за допомогою контейнерів, в яких знаходяться активи, що зберігаються або передаються. Крім того, ми робимо припущення щодо можливих сценаріїв загрози та їх впливу.

4.6.6 Визначення ризиків

Ризик - це можливість заподіяння шкоди чи збитків і складається з події, наслідку та невизначеності. Для кожного робочого аркуша ризику активів інформації (аркуш 10) ми застосовуємо сценарії загрози до його активів, припускаючи, що сценарій загрози був реалізований, вплив на оцінюється зацікавленими сторонами розумного будинку. Ми визначаємо ризики безпеки (Загрози + Вплив), які застосовуються до різних рівнів інфраструктури розумного будинку, і коротко пояснюємо кожен ризик безпеки.

4.6.7 Аналіз ризиків

На цьому етапі ідентифіковані ризики оцінюються за допомогою критеріїв вимірювання, встановлених на першому кроці. Ці оцінки використовуються для визначення пріоритетів ризиків для зменшення наслідків.

Для кожного робочого аркуша інформаційного ризику (аркуш 10) нам потрібно виконати наступне:

1) Перегляд заяви про наслідки та присвоєння значення «високий», «середній» та «низький» у області Значення стовпця (8) з урахуванням Критеріїв вимірювання ризику (робочі аркуші 1-6).

2) Розрахунок балу для кожної зони удару шляхом множення рангу площі удару (робочий аркуш рейтингу зони впливу, робочий аркуш 7) на значення удару (високий = 3, середній = 2, низький = 1). Ми реєструємо результат у стовпці балів, а потім підсумовуємо бали, і ця сума є відносним балом ризику.

4.6.7 Вибір запобіжного підходу

На кроці 8 бали ризику, розраховані на попередньому кроці, використовуються для визначення пом'якшувальних дій. Восьмим і останнім кроком розробленої системи є вибір підходу для вирішення кожної з пріоритетних загроз.

Існує кілька підходів для вибору: прийняти, пом'якшити загрозу чи вплив, передати загрозу або відкласти.

Після виявлення ризиків (відповідно до загрози та вразливості) та показників ризиків може бути визначений план зменшення наслідків для уникнення або обмеження виявлених ризиків та негативних наслідків, що виникають від них.

4.7 Ризик інформаційного майна для інформації, яку збирають пристрої (датчики) / інформація про статус розумного будинку

4.7.1 Область занепокоєння 1

Інформаційний актив - Інформація, зібрана пристроями (датчиками) /

Інформація про стан розумного будинку.

Області занепокоєння:

1) Інформаційний актив навмисно змінюється зловмисними людьми, а розумний лічильник електроенергії показує велике споживання електроенергії. Таким чином, для оплати рахунків потрібно багато грошей.

2) DOS-атаки (заклинювання та фальсифікація) на фізичному рівні датчики не для виявлення таких ризиків, як пожежа, повінь, несподівані рухи тощо.

3) Компроміс датчика руху може бути використаний для визначення часу є люди вдома.

4) Зчитування стану замків дверей та сигналізації може бути використано для визначення, коли розумний будинок зайнятий.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

Зловмисна особа (хакер, поганий постачальник).

2. Засоби (Як би це зробив актор? Що б вони робили?)

- Хакерські інструменти;
- Апаратний дефект.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

- Фінансовий;
- Інцидент.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

- Модифікація;
- Переривання.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Лише уповноважені члени АСРД повинні мати доступ до цієї інформації та керування нею.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Висока.

7. Наслідки

Які наслідки для організації або власника інформаційного активу мають наслідки результату та порушення вимог безпеки? Якщо вимоги безпеки цих

інформаційних активів порушуються, власник розумного будинку або мешканці можуть нанести значну фінансову шкоду.

Датчики не виявлять таких ризиків, як пожежа, повінь чи будь-який дивний рух усередині розумного будинку. Таким чином, виникають великі фінансові втрати.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?)* (Див. таблиця 4.8)

Таблиця 4.8 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	4 * 3 = 12
Фінансова (3)	Високий (3)	9
Продуктивність (2)	Низький (1)	2
Бзепека та Здоров’я (5)	Високий (3)	15
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
Відносний показник ризику		39

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Технічні (внутрішні мережі). Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Застосовуйте багатошарові заходи безпеки.

2) Фізичні. Тримайте всі фізичні сховища в надійному місці. Регулярно підтримуйте апаратні засоби, створюйте резервні копії всієї важливої інформації.

3) Людські. Програма підготовки мешканців з питань обізнаності про

безпеку, яка поінформує їх про ризики безпеки.

4) Інтернет. Використовуйте захищений канал зв'язку за допомогою VPN, використовуючи IPsec, SSL або TLS.

4.7.2 Область занепокоєння 2

Інформаційний актив - Інформація, зібрана пристроями (датчиками) / Інформація про стан розумного будинку.

Області занепокоєння: Система розумного дому виведена з ладу.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

Збій живлення.

2. Засоби (Як би це зробив актор? Що б вони робили?)

Втрата живлення.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

Інцидент.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

Переривання.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Блок живлення повинен бути постійно доступним цілодобово та без вихідних.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Середня.

7. Наслідки

Якщо сценарій загрози був реалізований, система розумного будинку стає небезпечною та непередбачуваною для власника, наприклад двері та вікна не розблокуються.

Система розумного будинку не працює належним чином, як передбачалося. Це може спричинити негативний вплив на функціональність та роботоспроможність розумного будинку.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?)* (Див. таблиця 4.9)

Таблиця 4.9 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Середній (2)	8
Фінансова (3)	Високий (3)	9
Продуктивність (2)	Низький (1)	2
Бзепека та Здоров'я (5)	Середній (2)	10
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
	Відносний показник ризику	30

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Фізичні. Ви повинні мати надлишкове джерело безперебійного живлення (ДБЖ). Використовуйте спеціальні надлишкові резервні системи з джерелами безперебійного живлення (ДБЖ).

2) Людські. Переконайтеся, що у вас є програма поінформованості користувачів, щоб вони усвідомили важливість джерела живлення та інші загрози безпеці.

4.7.3 Профіль критичної інформації (відеопотік камер спостереження)

(1) Критичний актив (*Що є важливим інформаційним активом?)*

Відеопотік камер спостереження.

(2) Обґрунтування вибору (*Чому цей інформаційний актив важливий для організації?)*

Цей інформаційний ресурс дуже важливий, оскільки камери спостереження є частиною системи розумного будинку, а відеопоток камери спостереження використовується, наприклад для віддаленого прийому несподіваних відвідувачів або для виявлення незвичних рухів всередині розумного будинку та подання

тривоги користувачеві, коли він не вдома.

(3) Опис (*Який узгоджений опис цього інформаційного активу?)*

Без цього інформаційного ресурсу система розумного будинку (АСРД) не буде повною і не зможе правильно досягти своїх цілей.

(4) Власник(и) (*Хто володіє цим інформаційним активом?)*

Власник - власник Системи автоматизації розумного будинку (АСРД), який відповідає за цей інформаційний актив.

(5) Вимоги безпеки (*Які вимоги до безпеки цього інформаційного активу?)*

- **Конфіденційність** - Лише уповноважений персонал може переглядати цей інформаційний ресурс таким чином: Лише мешканці мають право доступу до цього інформаційного ресурсу.
- **Цілісність** - Лише уповноважений персонал може модифікувати цей інформаційний ресурс таким чином: Тільки жителі мають право маніпулювати цим інформаційним активом.
- **Доступність** - Цей актив повинен бути доступний для того, щоб ця особа могла виконувати свою роботу таким чином:

Актив повинен бути доступним для використання, коли це потрібно лише мешканцям.

Цей актив повинен бути доступний протягом 24 годин, 7 днів на тиждень, 52 тижні на рік. Ці інформаційні ресурси повинні бути доступними цілодобово та без вихідних.

Він повинен бути доступним для користувача з метою функціонування. Коротких відключень немає викликати будь-які серйозні проблеми. Тривале переривання (більше 8 годин) може спричинити значну проблему.

(6) Найважливіші вимоги безпеки (*Яка найважливіша вимога безпеки для цього інформаційного активу?)*

- Конфіденційність;
- Доступність.

В таблиці 4.10 наведено опис технічних ризиків для відеопотоку камер спостереження. А в таблиці 4.11 наведено опис фізичних ризиків дяя відеопотоку

камер спостереження.

Таблиця 4.10 - Карта середовища ризику використання інформаційних ресурсів (технічна) для відеопотоку камер спостереження

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. Smart TV, ПК (робочі станції)	Власник розумного будинку (мешканці)
2. База даних: Інформаційний актив передусім розміщений на серверах баз даних та веб-серверах.	Власник розумного будинку (мешканці)
3. Внутрішня мережа розумного дому. Вся інформація подорожує по цій мережі.	Власник розумного будинку (мешканці)
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. Інтернет: ці інформаційні ресурси переміщуються по Інтернету кожен час, коли кінцевий користувач підключається до АСРД поза межами будинку через користувацькі пристрої, такі як ПК, смартфон, планшет тощо.	Користувач розумного дому
2. Пристрої пульта дистанційного керування користувача (смартфони, планшети, ПК)	Користувач розумного дому

Таблиця 4.11 - Карта середовища ризику використання інформаційних ресурсів (фізична) для відеопотоку камер спостереження

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. Камери можуть записувати події та зберігати їх у носіях інформації та надсилати копію до бази даних вдома.	мешканці
2. Носій DVD, відеокасети.	мешканці
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
Носії даних, що зберігаються поза розумним будинком	мешканці

4.7.3 Ризик інформаційного майна для відеопотоку камер спостереження

Інформаційний актив - Відеопотік камер спостереження

Області занепокоєння:

Неавторизована особа отримує доступ до камер спостереження розумного

будинку. Виявлення поведінки та діяльності користувачів.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

Зловмисник (зловмисна особа).

2. Засоби (Як би це зробив актор? Що б вони робили?)

Злом інструментів або викрадення пристрою пульта дистанційного керування користувача.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

- Зловмисні цілі (шпигунство);
- Моніторинг;
- Допитливість.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

Розкриття.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Стрічки камери слід берегти від несанкціонованих очей. Лише авторизований користувач повинен їх бачити або мати.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Висока.

7. Наслідки

Якщо сценарій загрози був реалізований, зловмисник отримує доступ до розумного будинку, а потім вимагає грошей (викуп) за відмову. Цінна інформація (діяльність) буде продана іншим.

Зловмисник може спостерігати за мешканцями розумного будинку, вивчати їхні розпорядки дня та виявляти їх поведінку та діяльність.

Таким чином, конфіденційність мешканців порушується.

Успіх хакерської дії означає фінансову шкоду власнику будинку.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?*) (Див. таблицю 4.12)

Таблиця 4.12 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	12
Фінансова (3)	Високий (3)	9
Продуктивність (2)	Низький (1)	2
Бзепека та Здоров’я (5)	Середній (2)	10
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
Відносний показник ризику		34

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Технічні. Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Застосовуйте багатошарові заходи безпеки.

2) Фізичні. Тримайте всі фізичні сховища в надійному місці. Регулярно підтримуйте апаратні засоби, створюйте резервні копії всієї важливої інформації. Встановлюйте камери лише в безпечних місцях вдома, щоб уникнути фальсифікацій.

3) Людські. Переконайтеся, що у вас є програма інформування користувачів, яка поінформує їх про такі ризики безпеки.

4.8 Підсистема 2: між пристроями та домашнім шлюзом

1) Інформаційні ресурси (картинки, документи, музика) (Підсистеми 1-2).

2) Інформація про розумне налаштування будинку або Посібники користувача для побутової техніки (Підсистеми 1-2).

3) Повноваження користувача (ім’я користувача та пароль) [Інтерфейс користувача] (Підсистема 2).

4) Інтелектуальна структура будинку та інформ. про запаси (Підсистем 1-2).

5) Логи.

Усередині розумного будинку (підрозділ 2) ми маємо вищезазначені п’ять інформаційних активів і вивчаємо їх активи безпеки. Він складається з 27 таблиць. Після цього ми починаємо з активів безпеки за межами розумного будинку, пов'язаних з підсистемою 3.

4.8.1 Профіль критично важливого інформаційного ресурсу (інформаційні ресурси (зображення, документи, відео, музика тощо)

1. Критичний актив (*Що є важливим інформаційним активом?)*

Інформаційні ресурси (Картинки, документи, відео, музика тощо).

2. Обґрунтування вибору (*Чому цей інформаційний актив важливий для організації?)*

Цей інформаційний ресурс важливий, оскільки містить приватну інформацію про користувачів.

3. Опис (*Який узгоджений опис цього інформаційного активу?)*

Ця інформація може зберігатися локально або передаватися через локальні мережі. Ці ресурси є приватними та містять щоденну інформацію користувачів у реальному часі. Їх можна знайти фізично або цифрово.

4. Власник(и) (*Хто володіє цим інформаційним активом?)*

Власником цієї інформації є мешканці.

5. Вимоги безпеки (*Які вимоги до безпеки цього інформаційного активу?)*

- **Конфіденційність** - Лише уповноважений персонал може переглядати цей інформаційний ресурс таким чином: Мешканці можуть переглядати власну конфіденційну інформацію, а деякі відвідувачі можуть переглядати частину цієї інформації залежно від чутливості.

- **Цілісність** - Лише уповноважений персонал може модифікувати цей інформаційний ресурс таким чином: Тільки жителі мають право маніпулювати цим інформаційним активом.

- **Доступність** - Цей актив повинен бути доступний для того, щоб ця особа могла виконувати свою роботу таким чином: Ці інформаційні ресурси

повинні бути доступними для власників, коли це потрібно для щоденного використання. Цей актив повинен бути доступний протягом X годин, X днів на тиждень, X тижнів / рік. Цей актив повинен бути доступним для власників стільки, скільки їм потрібно.

6. Найважливіші вимоги безпеки (*Яка найважливіша вимога безпеки для цього інформаційного активу?)*

- Конфіденційність;
- Доступність.

Таблиця 4.13 - Карта середовища ризику активів інформації (Технічна) для (Інформаційні ресурси (зображення, документи, відео, музика тощо)

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. ПК.	мешканці
2. Комунікаційні мережі.	мешканці
3. База даних.	мешканці
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
/	

В таблиці 4.13 наведено опис технічних ризиків для відеопотоку камер спостереження.

4.9 Ризик інформаційного майна для інформаційних ресурсів (картинки, документи, відео, музика тощо)

4.9.1 Область занепокоєння 1

Інформаційний актив - Інформаційні ресурси (картинки, документи, відео, музика тощо).

Області занепокоєння:

Несанкціоновані особи можуть переглядати фотографії та приватні документи членів сім'ї розумного дому та виставляти їх іншим.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

Будь-хто в Інтернеті, який діє як хакер.

2. Засоби (Як би це зробив актор? Що б вони робили?)

Хакерські інструменти.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

Допитливість.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

Розкриття.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Тільки уповноважені особи можуть переглядати цей інформаційний ресурс.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Низька.

7. Наслідки

Якщо вимоги безпеки цих інформаційних активів порушені, конфіденційність користувача розумного будинку буде порушена. Репутація мешканців отримає шкоду через розголошення цього активу. Успіх хакерської дії означає фінансову шкоду власнику будинку.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?*) (Див. таблицю 4.14)

Таблиця 4.14 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	12
Фінансова (3)	Низький (1)	3
Продуктивність (2)	Низький (1)	2
Бзепека та Здоров'я (5)	Низький (1)	5
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
Відносний показник ризику		23

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та*

фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?)**:**

1) Технічні (Внутрішні мережі). Політика контролю доступу повинна застосовуватися для регулювання доступу до системних ресурсів. Захистіть усі системи, застосувавши багаторівневі рівні захисту, такі як шифрування, встановлення в систему антивірусної (антивірусної) програми, системи запобігання / виявлення вторгнень.

2) Мережеві взаємодії. Встановіть безпечний мережевий зв'язок, застосовуючи методи шифрування. (Використовуйте зашифрований канал зв'язку).

3) Фізичні. Використовуйте шифрування.

4) Людські. Тренінг щодо обізнаності користувачів.

4.9.2 Область занепокоєння 2

Інформаційний актив - Інформаційні ресурси (картинки, документи, відео, музика тощо).

Області занепокоєння:

Носії інформації (жорсткі диски) не будуть доступні через несправність обладнання або втрату живлення. (призводить до відмови в користуванні DOS для користувача.).

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*)**:**

Постачальник апаратури.

2. Засоби (Як би це зробив актор? Що б вони робили?)

- Відмова обладнання;
- Втрата потужності.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

Інцидент.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

Знищення.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Інформаційний актив не буде доступний для авторизованих користувачів.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Низька.

7. Наслідки

Якщо стався збій системи та немає резервних копій цих інформаційних ресурсів, вони не підлягають відновленню, і ви втратите їх назавжди.

Інформаційні активи не захищені, щоб бути доступними, і їх не можна використовувати за призначенням.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?*) (Див. таблицю 4.15)

Таблиця 4.15 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Низький (1)	4
Фінансова (3)	Низький (1)	3
Продуктивність (2)	Низький (1)	2
Безпека та Здоров'я (5)	Низький (1)	5
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
	Відносний показник ризику	15

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) **Жорсткі диски.** Обов'язково зробіть резервні копії всіх своїх систем, що містять цінну інформацію. Таким чином ви можете відновити особисту

інформацію.

2) **Живлення**. Переконайтеся, що джерело безперебійного живлення (ДБЖ).

4.10 Профіль критичної інформації (Інформація про розумне налаштування будинку або Посібники користувача для побутової техніки)

1. Критичний актив (*Що є важливим інформаційним активом?)*

Інформація про розумний дім / Посібники користувача.

2. Обґрунтування вибору (*Чому цей інформаційний актив важливий для організації?)*

Цей інформаційний ресурс дуже важливий, особливо для нетехнічних мешканців, оскільки без цього активу буде неможливо налаштувати систему розумного будинку або керувати пристроєм Smart Home..

3. Опис (*Який узгоджений опис цього інформаційного активу?)*

Цей інформаційний ресурс можна знайти фізично чи в цифровому форматі та зберігати локально, або передавати через локальні мережі. Ці ресурси є приватними та містять цінну інформацію про систему розумного будинку. Він може містити докладні кроки про те, як виконати конкретне завдання або процес. Він містить кроки налаштування або інструкції, які вказують вам, як щось робити. Речі пояснюються малюнками, а малюнки можуть бути різними мовами.

4. Власник(и) (*Хто володіє цим інформаційним активом?)*

Власник розумного будинку. Постачальник.

5. Вимоги безпеки (*Які вимоги до безпеки цього інформаційного активу?)*

- **Конфіденційність** - Лише уповноважений персонал може переглядати цей інформаційний ресурс таким чином: Лише уповноважені особи повинні мати доступ до цих посібників користувача з метою розуміння. Звичайно, творець активу має до нього доступ.

- **Цілісність** - Лише уповноважений персонал може модифікувати цей інформаційний ресурс таким чином: Ніхто не має права вносити зміни або маніпулювати вмістом цього інформаційного ресурсу, крім уповноваженого

творця.

• **Доступність** - Цей актив повинен бути доступний для того, щоб ця особа могла виконувати свою роботу таким чином: Інформаційний актив повинен бути доступним у разі потреби. Цей актив повинен бути доступний протягом X годин, X днів на тиждень, X тижнів / рік. Вони повинні бути на руках, коли вони потрібні.

6. Найважливіші вимоги безпеки (*Яка найважливіша вимога безпеки для цього інформаційного активу?)*

- Цілісність;
- Доступність.

В таблиці 4.16 наведено карту технічних ризиків для інформації про налаштування розумного будинку.

Таблиця 4.16 - Карта середовища ризику активів інформації (Технічна) для Інформації про налаштування розумного будинку / Посібники користувача

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. Як файл даних, що зберігається в системах розумного будинку.	мешканці
2. Він може подорожувати через домашню мережу.	мешканці
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
Зберігається в цифровому вигляді в системах постачальників	постачальник

4.11 Інформація про ризик активів для інформації про налаштування розумного будинку / Посібники користувача

Інформаційний актив - Інформація про розумний дім / Посібники користувача.

Області занепокоєння:

Інформацію про розумне налаштування будинку або Посібники користувача змінюють несанкціоновані зловмисні особи.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

- Зловмисні особи;
- Можуть бути продавцями-конкурентами.

2. Засоби (Як би це зробив актор? Що б вони робили?)

Хакерські інструменти.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

Нанести збитки системам конкурентів.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

Модифікація.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Тільки уповноважений постачальник, який створив актив, може змінити його вміст з метою оновлення. Кваліфіковані кадри (професії) у цій галузі можуть вносити в неї зміни.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Низька.

7. Наслідки

Якщо цей актив буде змінено несанкціонованою особою, це може призвести до неправильного використання різних систем і навіть до того, що хтось постраждає і буде коштувати життя. Буде важко правильно налаштувати систему розумного будинку, отже виникатимуть несправності. Інформаційні активи не захищені від шкоди, і їх не можна використовувати за призначенням.

Таблиця 4.17 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	12
Фінансова (3)	Середній (2)	6
Продуктивність (2)	Низький (1)	2
Безпека та Здоров’я (5)	Високий (3)	15
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
Відносний показник ризику		36

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?*) (Див. таблицю 4.17)

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Технічні. Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Застосовуйте багатошарові заходи безпеки. Захистіть усі системи, застосувавши багаторівневі рівні захисту, такі як шифрування, встановлення в систему антивірусної (антивірусної) програми, системи запобігання / виявлення вторгнень

2) Мережеві взаємодії. Тримайте всі фізичні сховища в надійному місці. Регулярно підтримуйте апаратні засоби, створюйте резервні копії всієї важливої інформації. Зашифруйте всі дані на фізичних носіях.

3) Людські. Поінформуйте користувачів про розголошення цієї інформації за допомогою програм обізнаності та навчання для користувачів.

4.12 Профіль критично важливої інформації (облікові дані користувача)

1. Критичний актив (*Що є важливим інформаційним активом?)*

Креденшели користувача.

2. Обґрунтування вибору (*Чому цей інформаційний актив важливий для організації?)*

Цей інформаційний ресурс важливий, оскільки він є способом автентифікації, щоб захистити системи всередині розумного будинку від сторонніх осіб..

3. Опис (*Який узгоджений опис цього інформаційного активу?)*

Це інформація про автентифікацію користувача для входу в системи розумного будинку і, як правило, складається з ідентифікатора користувача та пароля для ідентифікації та перевірки користувача.

4. Власник(и) (*Хто володіє цим інформаційним активом?)*

Власником цього інформаційного ресурсу є уповноважений користувач (мешканці).

5. Вимоги безпеки (*Які вимоги до безпеки цього інформаційного активу?)*

• **Конфіденційність** - Лише уповноважений персонал може переглядати цей інформаційний ресурс таким чином: Тільки мешканці, яким дозволено використовувати систему розумної автоматизації будинку (АСРД).

• **Цілісність** - Лише уповноважений персонал може модифікувати цей інформаційний ресурс таким чином: Тільки жителі, які є власником цього майна, можуть періодично змінювати ці дані.

• **Доступність** - Цей актив повинен бути доступний для того, щоб ця особа могла виконувати свою роботу таким чином: Цей актив повинен бути постійно доступним, щоб мати можливість отримати доступ до систем. Цей актив повинен бути доступний протягом X годин, X днів на тиждень, X тижнів / рік. Цей об'єкт повинен бути доступний, доки користувач не змінить їх наступного разу.

6. Найважливіші вимоги безпеки (*Яка найважливіша вимога безпеки для цього інформаційного активу?)*

- Конфіденційність;
- Цілісність;
- Доступність.

4.13 Ризик інформаційного майна для облікових даних користувача

4.13.1 Область занепокоєння 1

Інформаційний актив - Крденшили користувача.

Області занепокоєння:

Неавторизована особа отримує ці облікові дані та може ввійти в основну систему розумного будинку.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

Зловмисник (зловмисна особа).

2. Засоби (Як би це зробив актор? Що б вони робили?)

Знаходить посвідчення, написані наочно:

1) Проведення соціальної інженерії.
2) Спробує паролі за замовчуванням, які постачаються з типовими обладнаннями.
3) Атака грубої сили.
4) Використання key-logger.
5) Програма для моніторингу на робочому столі.
6) Програма відновлення пароля.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

- Зловмисні цілі;
- Фінансові.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

Розкриття.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Лише авторизований користувач повинен мати ці облікові дані.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Середня.

7. Наслідки

Зловмисник отримує доступ до головної системи розумного будинку і вимагає грошей. Актор виконує несанкціоновані операції. Втрата контролю над АСРД.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?*) (Див. таблицю 4.18)

Таблиця 4.18 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	12
Фінансова (3)	Високий (3)	9
Продуктивність (2)	Середній (2)	4
Безпека та Здоров'я (5)	Високий (3)	15
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
	Відносний показник ризику	41

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Технічні. Не використовуйте компрометовані пристрої, щоб отримати доступ до систем розумного будинку. Заблокуйте доступ до систем за допомогою біометрії (сканери відбитків пальців). Застосовуйте сувору політику паролів.

2) Фізичні. Не пишіть складні ідентифікатори користувача та паролі на папері і не ховайте їх біля робочої станції чи системи.

3) Людські. Переконайтеся, що у вас є програма поінформованості користувачів, яка поінформує їх про соціальну інженерію, інші ризики безпеки та відповідно керує їхньою системою автоматизації будинку.

4.13.2 Область занепокоєння 2

Інформаційний актив - Крденшили користувача.

Області занепокоєння:

Несанкціонована особа отримує доступ до системи розумного будинку та може керувати розумним будинком.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

Зловмисник (зловмисна особа).

2. Засоби (Як би це зробив актор? Що б вони робили?)

Знаходить або викрадає мобільний пристрій, який уже підключений до системи розумного дому.

3. Мотив (*Яка причина актора для того, щоб це зробити?***)**

- Зловмисні цілі;
- Фінансові;
- Допитливість.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

Знищення.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Лише авторизований користувач повинен мати ці облікові дані.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Середня.

7. Наслідки

Зловмисник отримує доступ до головної системи розумного будинку і вимагає грошей. Актор виконує несанкціоновані операції. Втрата контролю над АСРД.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?*) (Див. таблицю 4.19)

Таблиця 4.7 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	12
Фінансова (3)	Високий (3)	9
Продуктивність (2)	Середній (2)	4
Безпека та Здоров’я (5)	Високий (3)	15
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
Відносний показник ризику		41

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Технічні. Не використовуйте компрометовані пристрої, щоб отримати доступ до систем розумного будинку. Використовуйте захищені пристрої з функцією входу, які автоматично отримують медальйон через короткий час після використання. Лише 2 рази можливість отримати доступ інакше отримує блокування.

2) Фізичні. Не відкладайте свій мобільний телефон від себе, наприклад у кишеню куртки та повісьте. Покладіть його з собою в надійне місце.

3) Людські. Будьте в курсі крадіжок.

4.14 Профіль критичної інформації (структура розумного будинку / інформація про запаси)

1. Критичний актив (*Що є важливим інформаційним активом?)*

Інтелектуальна структура будинку / інформація про запаси.

2. Обґрунтування вибору (*Чому цей інформаційний актив важливий для організації?)*

Цей інформаційний актив важливий, оскільки інвентарний документ містить детальну інформацію про системи, прилади та пристрої розумного будинку. Інвентаризація розумного будинку не тільки допомагає користувачеві створити детальний перелік вмісту розумного будинку, але надає йому / їй інтерактивний метод документування та обслуговування систем розумного будинку.

3. Опис (*Який узгоджений опис цього інформаційного активу?)*

Інвентаризацію розумного будинку можна створити, починаючи з переліку

всіх основних приладів, пристроїв та систем розумного будинку та документування всієї детальної інформації про них. Наявність домашнього інвентарю корисно для цілей страхування.

4. Власник(и) (*Хто володіє цим інформаційним активом?)*

Власником розумного дому.

5. Вимоги безпеки (*Які вимоги до безпеки цього інформаційного активу?)*

• **Конфіденційність** - Лише уповноважений персонал може переглядати цей інформаційний ресурс таким чином: Тільки мешканці, яким дозволено використовувати систему розумної автоматизації будинку (АСРД).

• **Цілісність** - Лише уповноважений персонал може модифікувати цей інформаційний ресурс таким чином: Власник розумного будинку та страхова компанія уповноважені переглядати цей інформаційний актив.

• **Доступність** - Цей актив повинен бути доступний для того, щоб ця особа могла виконувати свою роботу таким чином: Лише власник розумного будинку має право змінювати цей інформаційний ресурс для оновлення системи та оновлення списку. Цей актив повинен бути доступний протягом X годин, X днів на тиждень, X тижнів / рік. Лише власник розумного будинку має право змінювати цей інформаційний ресурс для оновлення системи та оновлення списку.

Таблиця 4.20 - Карта середовища ризику активів інформації (Технічна) для інтелектуальної структури будинку / інформації про інвентар

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. ПК (робочі станції)	Власник розумного будинку
2. База даних дому	Власник розумного будинку
3. Внутрішня комунікаційна мережа дому	Власник розумного будинку
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. Зовнішня мережа зв'язку, якщо інформація доступна через Інтернет	
2. Мережа страхового зв'язку	

6. Найважливіші вимоги безпеки (*Яка найважливіша вимога безпеки для цього інформаційного активу?)*

- Конфіденційність;
- Цілісність.

В таблиці 4.20 наведено карту середовища ризику активів інформації (Технічної) для інтелектуальної структури будинку або інформації про інвентар.

4.15 Ризик інформаційного майна для інтелектуальної структури будинку / інформації про запаси

Інформаційний актив - Інтелектуальна структура будинку / інформація про запаси.

Області занепокоєння:

Погані можуть отримати доступ до цього інформаційного ресурсу та шукати певні пристрої з відомими вразливими місцями для атаки на систему розумного будинку.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

- Нападник чорного капелюха;
- Конкуренти.

2. Засоби (Як би це зробив актор? Що б вони робили?)

- Злом;
- Пошук засобів масової інформації, що містять цей актив;
- Соціальна інженерія.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

- Зловмисні цілі;
- Фінансові;
- Допитливість.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

Розкриття.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Інвентаризаційна інформація повинна бути конфіденційною, і доступ до неї мають лише уповноважені особи.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Середня.

7. Наслідки

Якщо конфіденційність інформаційного активу порушена, зловмисник виявляє слабкий пристрій із відомими вразливими місцями та атакує його. За допомогою нього він може знайти спосіб отримати доступ до основної системи та керувати нею. якщо це станеться, то він може робити все, що забажає, залежно від його наміру. Розумний дім буде принаймні не безпечним для проживання.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?*) (Див. таблицю 4.21)

Таблиця 4.21 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	12
Фінансова (3)	Високий (3)	9
Продуктивність (2)	Низький (1)	2
Безпека та Здоров’я (5)	Високий (3)	15
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
	Відносний показник ризику	39

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Технічні. Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Використовуйте протоколи захисту зв'язку, такі як SSL

/ TLS через TCP / IP або DTLS через UDP.

Використовуйте механізми шифрування. Застосовуйте багатошарові заходи безпеки для захисту всіх систем. Використовуйте СВВ (система виявлення вторгнень) / СЗП (система запобігання вторгненню).

2) Інтернет. Використовуйте захищений канал зв'язку за допомогою VPN за допомогою IPsec, SSL або TLS.

3) Фізичні. Регулярно підтримуйте всі апаратні засоби, створюйте резервні копії всієї важливої інформації. Зберігайте всі резервні носії інформації в захищених місцях як усередині, так і зовні розумного будинку.

4) Людські. Програма підвищення обізнаності для мешканців з метою ознайомлення їх з ризиками безпеки та соціальною інженерією.

4.16 Профіль критичної інформації (логи)

1. Критичний актив (*Що є важливим інформаційним активом?)*

Логи.

2. Обґрунтування вибору (*Чому цей інформаційний актив важливий для організації?)*

Цей інформаційний актив є дуже важливим, оскільки реєстрація подій безпеки, які відбуваються в розумній домашній мережі, є єдиним способом, яким ми можемо визначити, що система або знаходиться в процесі компрометації, або була порушена. Тільки знаючи, що відбувається в мережі, ми можемо належним чином захищатися від атак.

3. Опис (*Який узгоджений опис цього інформаційного активу?)*

Події безпеки повинні реєструватися, а доступ до журналів повинен бути задокументований та захищений від розголошення стороннім користувачам.

4. Власник(и) (*Хто володіє цим інформаційним активом?)*

Власником розумного дому.

5. Вимоги безпеки (*Які вимоги до безпеки цього інформаційного активу?)*

- **Конфіденційність** - Лише уповноважений персонал може переглядати цей

інформаційний ресурс таким чином: Власник розумного будинку (адміністратор) має право переглядати цей інформаційний актив.

• **Цілісність** - Лише уповноважений персонал може модифікувати цей інформаційний ресурс таким чином: Лише власник розумного будинку має право змінювати цей інформаційний об’єкт.

• **Доступність** - Цей актив повинен бути доступний для того, щоб ця особа могла виконувати свою роботу таким чином:

Цей актив повинен бути доступний за потреби власника розумного будинку (адміністратора).

Цей актив повинен бути доступний протягом X годин, X днів на тиждень, X тижнів / рік.

Немає великих вимог щодо доступності цього активу.

Якраз у разі потреби.

6. Найважливіші вимоги безпеки (*Яка найважливіша вимога безпеки для цього інформаційного активу?)*

- Конфіденційність;
- Цілісність.

Таблиця 4.82 - Карта середовища ризику активів інформації (Технічна) для логів

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. ПК (робочі станції)	Власник розумного будинку
2. База даних дому	Власник розумного будинку
3. Внутрішня комунікаційна мережа дому	Власник розумного будинку
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
Зовнішня мережа зв'язку, якщо інформація доступна через Інтернет	

В таблицях 4.22 та 4.23 наведено карти для логів технічних та фізичних відповідно ризиків інформації.

Таблиця 4.93 - Карта середовища ризику активів інформації (фізична) для логів

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
CD, DVD, USB	
Внутрішні бекапи	
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
Зовнішні бекапи	

4.17 Ризик інформаційного майна для логів

Інформаційний актив – Логи.

Області занепокоєння:

Зловмисник може отримати доступ до даних журналів та отримати з них корисну інформацію (конфігурації системи), що є серйозним недоліком безпеки, що дозволяє йому атакувати систему розумного дому.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

- Нападник чорного капелюха;
- Конкуренти.

2. Засоби (Як би це зробив актор? Що б вони робили?)

Злом (бекдор, троянські коні).

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

- Зловмисні цілі;
- Нанести шкоду.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

- Розкриття;
- Модифікація;
- Знищення.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Інформація про журнали повинна бути конфіденційною, і доступ до неї мають лише уповноважені особи.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Висока.

7. Наслідки

Якщо конфіденційність інформаційного активу порушена, зловмисник знаходить спосіб отримати доступ до основної системи та контролювати її. Якщо це трапиться, тоді він може робити все, що забажає, залежно від свого наміру, розумний дім буде принаймні не безпечним для проживання.

8. Тяжкість (Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?) (Див. таблицю 4.24)

Таблиця 4.104 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	12
Фінансова (3)	Високий (3)	9
Продуктивність (2)	Низький (1)	2
Безпека та Здоров’я (5)	Високий (3)	15
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
Відносний показник ризику		39

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Технічні. Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Журнали повинні бути анонімними.

Уникайте реєстрації інформації, яка давала б корисну інформацію зловмиснику. Обмежте доступ до журналів, застосовуючи механізми контролю доступу. При надсиланні у віддалену систему журнали повинні бути захищені криптографічними механізмами. Застосовуйте багатошарові заходи безпеки для захисту всіх систем.

2) Інтернет. Використовуйте захищений канал зв'язку за допомогою VPN за допомогою IPsec, SSL або TLS.

3) Фізичні. Регулярно підтримуйте всі апаратні засоби, створюйте резервні копії всієї важливої інформації. Зберігайте всі резервні носії інформації в захищених місцях як усередині, так і зовні розумного будинку.

4) Людські. Програма навчання обізнаності для власника системи, щоб бути в курсі ризиків безпеки, пов'язаних з реєстрацією подій системи.

4.18 Поза розумним будинком (зовнішня мережа зв'язку)

Підсистема 3. Між домашніми шлюзами та Інтернетом:

1. Інформація (дані), що передається через домашній шлюз
2. Мобільні особисті дані та програми
3. Інформація про відстеження місцезнаходження

4.19 Профіль критично важливого інформаційного ресурсу (інформація (дані), передана через домашній шлюз)

1. Критичний актив (*Що є важливим інформаційним активом?)*

Інформація (дані), що передається через домашній шлюз.

2. Обґрунтування вибору (*Чому цей інформаційний актив важливий для організації?)*

Цей інформаційний актив важливий, оскільки він передається через невід’ємну частину системи розумного будинку, яка пов’язує домогосподарство із зовнішнім середовищем.

3. Опис (*Який узгоджений опис цього інформаційного активу?)*

Основним завданням домашнього шлюзу є досягнення обміну інформацією та перетворення між різними протоколами зв'язку домашньої мережі, а також обмін даними та інформацією із зовнішніми мережами.

4. Власник(и) (*Хто володіє цим інформаційним активом?)*

Власником розумного дому.

5. Вимоги безпеки (*Які вимоги до безпеки цього інформаційного активу?)*

- **Конфіденційність** - Лише уповноважений персонал може переглядати цей інформаційний ресурс таким чином: Доступ до цього інформаційного ресурсу мають мати лише уповноважені особи, такі як власник розумного будинку. Постачальникам послуг також може знадобитися надсилати та отримувати дані через домашній шлюз для надання послуг.

- **Цілісність** - Лише уповноважений персонал може модифікувати цей інформаційний ресурс таким чином: Ніхто не має права змінювати цей інформаційний актив, крім власника розумного будинку (адміністратор).

- **Доступність** - Цей актив повинен бути доступний для того, щоб ця особа могла виконувати свою роботу таким чином: Інформаційний актив повинен бути доступним у разі потреби.Цей актив повинен бути доступний протягом X годин, X днів на тиждень, X тижнів / рік. Немає великих вимог щодо доступності цього активу. Тільки, коли потрібно.

Таблиця 4.115 - Карта середовища ризику активів інформації (технічна) для інформації (даних), що передається через домашній шлюз

ВНУТРІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
1. Шлюз дому	Власник розумного будинку
2. Внутрішня комунікаційна мережа дому	Власник розумного будинку
ЗОВНІШНІ	
ОПИС КОНТЕЙНЕРА	ВЛАСНИК(-И)
Зовнішня комунікаційна мережа	

6. Найважливіші вимоги безпеки (*Яка найважливіша вимога безпеки для цього*

інформаційного активу?)

- Конфіденційність;
- Цілісність.

Опис технічних ризиків у таблиці 4.25.

4.20 Ризик інформаційного майна для інформації (даних), переданої через домашній шлюз

Інформаційний актив – Інформація (дані), що передається через домашній шлюз.

Області занепокоєння:

Зловмисник може викрасти інформацію та пакет даних, передані через домашній шлюз.

1. Актор (*Хто буде використовувати зону, що викликає занепокоєння чи загрозу?*):

Нападник.

2. Засоби (Як би це зробив актор? Що б вони робили?)

- Постукування по лінії;
- Перехоплення пакетів даних.

3. Мотив (*Яка причина актора для того, щоб це зробити?*)

- Пошкодити ШАС
- Збити систему.

4. Результат (*Яким буде наслідком вплив на інформаційний актив?*)

- Розкриття;
- Модифікація.

5. Вимоги безпеки (*Як будуть порушені вимоги до захисту інформаційного активу?)*

Лише уповноважений персонал може переглядати та змінювати цей інформаційний актив.

6. Імовірність (*Яка ймовірність того, що може виникнути такий сценарій загрози?*)

Висока.

7. Наслідки

Якщо конфіденційність інформаційного активу порушена, зловмисник знаходить спосіб отримати доступ до основної системи та контролювати її. Якщо це трапиться, тоді він може робити все, що забажає, залежно від свого наміру. Розумний дім буде принаймні не безпечним для проживання.

8. Тяжкість (*Наскільки серйозними є ці наслідки для організації або власника активу за зоною впливу?*) (Див. таблицю 4.26)

Таблиця 4.126 - Оцінка тяжкості

Зона впливу	**Значення**	**Рахунок**
Репутація та Клієнтська Довіра (4)	Високий (3)	12
Фінансова (3)	Високий (3)	9
Продуктивність (2)	Низький (1)	2
Безпека та Здоров'я (5)	Високий (3)	15
Штрафи та Юридичні покарання (1)	Низький (1)	1
Клієнт-специфічні (0)	порахувати не можна	/
	Відносний показник ризику	39

9. Зменшення ризику (*Виходячи із загального балу для цього ризику, яку дію ви виконаєте?*)

Зменшити.

Для ризиків, які ви вирішили зменшити, виконайте такі дії (*На якому контейнері ви б застосували елементи керування? Який адміністративний, технічний та фізичний контроль ви б застосували до цього контейнера? Який залишковий ризик все-таки буде прийнятий організацією?*)**:**

1) Технічні. Захистіть мережевий рівень за допомогою служб мережевої безпеки та контролю доступу, таких як обмеження IP-адреси, шифрування мережевого рівня та використання брандмауерів. Для безпечної передачі даних використовуйте захищений протокол, такий як SSL. Встановлення антивірусу (антивірусного програмного забезпечення). Цей актив повинен бути доступний для того, щоб ця особа могла виконувати свою роботу таким чином: Інформаційний актив повинен бути доступним у разі потреби.Цей актив повинен

бути доступний протягом X годин, X днів на тиждень, X тижнів / рік. Немає великих вимог щодо доступності цього активу. Тільки, коли потрібно.

2) Фізичні. Переконайтеся, що домашній шлюз доступний для сторонніх людей.

3) Людські. Навчальна програма з підвищення рівня обізнаності для мешканців розумного будинку.

4.21 Результати та підсумки

4.21.Інформація, зібрана пристроями (датчиками)

Загрози: Зміна даних, атаки DOS, компрометація пристрою (датчика), розкриття інформації, переривання функцій.

Наслідки: Датчики не можуть виявити вдома такі ризики, як пожежа, повінь або якісь дивні рухи.

Маніпулюйте вимірами датчика, щоб проникнути в систему з неправильними даними, наприклад викликати певні спрацьовування.

Фінансові втрати Якщо погані хлопці дізнаються, що вас немає вдома, вони можуть задумати проникнути додому.

Оцінка ризику: 39.

Контр міри: Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP.

Технічне обслуговування обладнання. Резервні копії. Програма підготовки мешканців з питань обізнаності з питань безпеки.

Використовуйте захищений канал зв'язку за допомогою VPN за допомогою IPsec, SSL або TLS. Використовуйте спеціальні надлишкові резервні системи з джерелами безперебійного живлення (ДБЖ). Проводити багатошарові заходи безпеки.

4.20.2 Відео. Подача камер спостереження

Загрози: Камери спостереження. Контроль моніторингу та шпигунства.

Наслідки: Порушення конфіденційності користувачів. Фінансові збитки.

Оцінка ризику: 34.

Контр міри: Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP.

Використовуйте брандмауер та СВВ (система виявлення вторгнень) / СЗП (система запобігання вторгненню). Встановлюйте камери лише в безпечних місцях вдома, щоб уникнути фальсифікацій.

4.20.3 Інформаційні ресурси (малюнки, документи, музика)

Загрози: Викрадення приватної інформації. Відмова обладнання.

Наслідки: Порушення конфіденційності користувачів. Фінансові збитки. Репутація шкодить втраті інформації.

Оцінка ризику: 23.

Контр міри: Обмежте доступ до системних ресурсів. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Використовуйте зашифрований канал зв'язку. Захистіть усі системи, застосувавши багаторівневі рівні захисту, такі як шифрування, установка антивірусної (антивірусної) програми в систему, вторгнення системи запобігання / виявлення. Використовуйте джерело безперебійного живлення (ДБЖ).

4.20.4 Налаштування розумного будинку. Інформація або Посібники користувача для побутової техніки.

Загрози: Інформація. Модифікація.

Наслідки: Складність у правильній настройці системи розумного дому, отже, виникатимуть несправності. Неправильне використання систем РД. Фінансові збитки.

Оцінка ризику: 36.

Контр міри: Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Проводити багатошарові заходи безпеки.

4.20.5 Повноваження користувача (ім’я користувача та пароль)

Загрози: Уособлення користувача. Викрадення особистих даних та довірок.

Наслідки: Несанкціонований доступ до основної системи розумного будинку та грошові вимоги.

Несанкціоноване виконання операцій. Втрата контролю над АСРД. Фінансові збитки.

Оцінка ризику: 41.

Контр міри: Заблокуйте доступ до систем за допомогою біометрії (сканери відбитків пальців).Впровадити багатофакторну автентифікацію.

Застосовуйте сувору політику парольних фраз.

Захистіть усі системи, застосувавши багаторівневі рівні захисту, такі як шифрування, встановлення в систему антивірусної (антивірусної) програми, системи запобігання / виявлення вторгнень.

Намагайтеся не писати складні ідентифікатори користувача та паролі на папері та заховати їх біля робочої станції чи системи.

4.20.6 Інтелектуальна структура будинку / інформація про запаси

Загрози: Погані можуть отримати доступ до цього інформаційного ресурсу та шукати конкретний пристрій із відомими вразливими місцями для атаки на систему розумного будинку.

Наслідки: Зловмисник знаходить найслабший пристрій з відомими вразливими місцями і атакує його. Потім бере на себе контроль над АСРД. Фінансові збитки.

Оцінка ризику: 39.

Контр міри: Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Використовуйте механізми шифрування. Резервні копії. Застосовуйте багатошарові заходи безпеки для захисту всіх систем. Використовуйте СВВ (система виявлення вторгнень) / СЗП (система запобігання вторгненню). Використовуйте захищений канал зв'язку за допомогою VPN за допомогою IPsec, SSL або TLS.

Програма підвищення обізнаності для мешканців з метою ознайомлення їх з ризиками безпеки та соціальною інженерією.

4.20.7 Логи

Загрози: Зловмисник може отримати доступ до даних журналів та отримати з них корисну інформацію (конфігурації системи), що є серйозним недоліком безпеки, що дозволяє йому атакувати систему розумного дому.

Наслідки: Зловмисник знаходить спосіб отримати доступ до основної системи та керувати нею. Фінансові збитки.

Оцінка ризику: 39.

Контр міри: Обмежте мережевий трафік, до якого мають доступ лише авторизовані користувачі. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP.

4.20.8 Інформація (дані), що передається через домашній шлюз

Загрози: Зловмисник може викрасти інформацію та пакет даних, передані через домашній шлюз.

Наслідки: Зловмисник може додати вірус до пакету даних, потім випускається в систему, забирає системні ресурси шляхом постійної самореплікації, так що система не може виконати відповідну роботу, і це призводить до того, що система остаточно стає непридатною для використання.

Оцінка ризику: 39.

Контр міри: Захистіть мережевий рівень за допомогою служб мережевої безпеки та контролю доступу, таких як обмеження IP-адреси, шифрування мережевого рівня та використання брандмауерів. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP.

Для безпечної передачі даних використовуйте захищений протокол, такий як SSL. Виконайте управління конфігурацією маршрутизатора. Внесіть чорний список шлюзу, щоб уникнути підключення до відомих шкідливих доменів та IP-адрес.

4.20.9 Мобільні особисті дані та програми

Загрози: Зловмисники можуть отримати доступ до смарт-телефону (пульт

дистанційного керування) і вводить шкідливий код у встановлені на ньому програми.

Наслідки: Це робить смартфон таким чином, що він може таємно робити фотографії, записувати розмови та відстежувати місця. Роблячи це, зловмисник робить шпигунські телефони смартфонів Android або iPhone і може відстежувати ваші рухи, перехоплювати SMS-повідомлення та телефонні дзвінки, отримувати списки контактів та електронні листи. Крім того, він може використовувати ваш мікрофон і камеру. Зловмисник може додати інтерфейс управління та управління, щоб дозволити йому дистанційно керувати смартфоном.

Оцінка ризику: 41.

Контр міри: Не використовуйте загальнодоступний Wi-Fi, це дає хакерам доступ до персональних даних. Перш ніж користуватися програмою домашньої автоматизації, скористайтеся послугою зв'язку чи захищеною мережею.

4.20.10 Інформація про відстеження місцезнаходження

Загрози: Зловмисник може спостерігати за потоком даних про місцезнаходження.

Наслідки: Зловмисник може зробити висновок, що власник розумного будинку покинув будинок. Плануйте проникнути в розумний дім, якщо він вільний.

Оцінка ризику: 34.

Контр міри: Обмежте доступ до мережевого трафіку лише авторизованими користувачами. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Інформація про місцезнаходження повинна бути захищена від несанкціонованого доступу. Така інформація не повинна надсилатися в чистому тексті, і, отже, у АСРД необхідний захищений (зашифрований) протокол зв'язку для шифрування трафіку між системою відстеження та пристроєм прослуховування.

Як тільки ми отримаємо результати дослідження, буде необхідність їх обговорити. Як ми вже заявляли раніше, технологія Інтернету речей (IoT) передбачала розвиток розумних будинків, щоб принести зручність та

ефективність у наше життя та наші будинки. Безпека є однією з цілей розумного будинку на основі IoT, але, виходячи з того, що ми виявили вище (ризики для безпеки) в результаті дослідження, ми бачимо, що ці технології дуже вразливі до різних атак безпеки, які роблять IoT- розумна житлова небезпека та небезпека для проживання, якщо нехтувати безпекою.

Тому для оцінки ситуації розумних будинків необхідно оцінити ризики для безпеки. Якщо безпеку в розумному будинку ігнорувати або якщо зручність та функціональність віддавати перевагу безпеці, ці технології матимуть важливе значення для безпеки. Розумний дім - це місце проживання людей, і в ньому має бути безпечно і безпечно жити. Він повинен забезпечувати достатню безпеку та конфіденційність.

Підключення всіх розумних об’єктів усередині будинку до Інтернету та між собою призводить до нових проблем безпеки та конфіденційності, наприклад, конфіденційності, автентичності та цілісності даних, що сприймаються та обмінюються пристроями. Ризики безпеки повинні бути досліджені та розглянуті, як ми це робили в цьому дослідженні.

Ми можемо зробити висновок, що безпека є критично важливим фактором, і її слід серйозно та глибоко (глибокий захист) сприймати в системі розумного будинку, інакше можуть бути серйозні наслідки, а також всі виявлені ризики в цій дисертації будуть справедливими.

З цією метою та для відповіді на запитання дослідження було проведено комплексну оцінку ризиків безпеки за допомогою розробленої системи для оцінки та оцінки ризиків безпеки в типовому розумному будинку з метою висвітлення різних загроз безпеці в розумному домі на базі IoT, наслідків та пропонування контрзаходів щодо виявлених проблем, що задовольняють більшість вимог безпеки.

У цій роботі було виявлено 10 важливих інформаційних активів, за якими проводилась оцінка ризику безпеки з метою їх захисту. Близько 15 пов'язаних ризиків було засновано в різних частинах або підсистемах розумного будинку з різними показниками ризику. Для вирішення цих ризиків або принаймні

пом'якшення їх до прийнятного рівня пропонуються різні плани пом'якшення наслідків. Людський фактор дуже важливий, і його слід враховувати серйозно. Освіта користувачів необхідна для того, щоб зацікавлені сторони, зокрема мешканці, усвідомлювали різні проблеми безпеки, особливо соціальну інженерію.

Робота досягла своїх цілей і дала відповідь на питання дослідження, склавши список ризиків для безпеки в розумному будинку, наслідків та відповідних заходів протидії. Список буде корисним внеском, який може бути використаний як основа для специфікації безпеки вимоги до розумного будинку. Для подальшої роботи оцінка буде розширена, включивши набагато більше ризиків для безпеки та навіть враховуючи інші типи розумних будинків, як зазначено у розділі 2.2.

4.21 Рекомендації

Метою цього розділу є надання деяких рекомендацій зацікавленим сторонам, як комерційним зацікавленим сторонам (постачальникам, постачальникам інфраструктури, стороннім постачальникам програмного та апаратного забезпечення тощо), так і некомерційним зацікавленим сторонам (урядові установи та муніципалітети та кінцевим споживачам (мешканці)), з метою вдосконалення цієї технології (розумний дім на базі Інтернету речей) щодо безпеки.

4.21.1 Рекомендації комерційним зацікавленим сторонам

1) Існує велика потреба інтегрувати безпеку на етапі проектування та розробки.

2) Усі товари та послуги, які впливають на життя та безпеку мешканців, повинні мати вимоги високого рівня безпеки.

3) Безпека поліпшується в системах, блокуючи доступ до сторінки входу на деякий час після послідовних невдалих спроб входу. Це захищає систему від атак грубої сили та атак на основі словників.

4) вимагати від споживачів змінити паролі за замовчуванням під час

процесу налаштування.

5) Існує потреба в юридичній підтримці в забезпеченні конфіденційності в середовищах IoT, і конфіденційність повинна розглядатися вже під час проектування систем IoT.

6) Існує потреба у стандартах безпеки (основна вимога до виробників).

7) Перед випуском продуктів краще протестувати свої заходи безпеки і не забути закрити всі задні двері в продуктах. Погано для вашої репутації.

8) Компанії повинні продовжувати виправляти відомі вразливі місця протягом усього життєвого циклу продукції.

9) Слід розробити методології оцінки ризиків для безпеки, які можуть охоплювати обмеження в пристроях.

10) Будьте прозорими та повідомте своїм клієнтам, як ви використовуєте їх конфіденційну інформацію.

4.21.2 Рекомендації некомерційним зацікавленим сторонам

1) Дуже важливо встановити безпечні імена користувачів та паролі для всіх систем домашньої автоматизації, а не залишати їх за замовчуванням.

2) Зберігайте свої паролі надійними та непередбачуваними. Використовуйте довгий пароль із великими та малими літерами, цифрами та спеціальними символами. Часто міняйте їх на всіх своїх системах та пристроях.

3) Уникайте використання простих для вгадування послідовностей, таких як „123456”.

4) Не використовуйте повторно встановлені вами паролі для інших цілей.

5) Будьте в курсі подій та встановлюйте всі оновлення мікропрограми та програмного забезпечення, доступні для встановлених пристроїв.

6) Споживачі повинні вибирати свої системи та пристрої серед відомих постачальників з доброю репутацією, а не серед постачальників з обмеженим досвідом у галузі безпеки.

7) Уникайте передачі інфраструктури стороннім постачальникам послуг, оскільки вони не впевнені, що вони обізнані про всі ризики та вимоги безпеки.

8) Не обирайте зручність та простоту використання над безпекою, якщо вам

надано вибір.

9) Налаштуйте маршрутизатор та системи належним чином. Для цього ви повинні бути кваліфікованою особою в галузі безпеки, інакше це призводить до власного набору вразливостей. Виберіть свій маршрутизатор із захищеним доступом Wi-Fi (WPA2), щоб забезпечити максимальний захист від хакерів.

10) Оновлення та оновлення пристроїв. Не продовжуйте зі старими.

11) Періодично проводьте тестування на проникнення, щоб переконатися, що ваші системи в безпеці.

12) Ризики та загрози з часом змінюються, тому важливо, щоб користувач періодично переоцінював ризики та переглядав ефективність обраних контрзаходів.

13) Програма тренінгів з питань безпеки є обов'язковою для мешканців дому, щоб поінформувати їх про належні практики безпеки.

14) Розглянемо заходи безпеки на кількох рівнях. Впровадити оборонний підхід.

15) Мобільний телефон використовується як пристрій дистанційного керування. Тому надзвичайно важливо, щоб він постійно залишався під пильним наглядом. Не використовуйте розбиті телефони.

16) Профілактика краще, ніж лікування. Не допускайте зловмисників до ваших систем (СЗП), оскільки як тільки вони потраплять, їх буде важко знайти та заблокувати.

17) Політика повинна вироблятися політиками, щоб її застосовували та дотримувались.

18) Важливо зазначити, що процес ризику є ітеративним. Оцінка ризику повинна бути постійною. Ризики необхідно постійно оцінювати та керувати ними, див. Малюнок 14 нижче.

19) Будьте в курсі соціальної інженерії. Не довіряйте усім.

20) Безперечно захищайте свої мережі Wi-Fi. Використовуйте пристрої, що використовують розширений стандарт шифрування (AES) із розміром ключа не менше 128 біт.

ВИСНОВКИ

Завданнями дипломної роботи було ознайомити з темою Інтернету речей (IoT) та її застосуванням для створення розумних будинків, що забезпечують інтелект, комфорт та покращують якість життя.

Введення технології IoT до нашого будинку призводить до нових викликів безпеці, тому розумні будинки на базі IoT вимагають дуже жорстких вимог безпеки. Ці сучасні технології пропонують як можливості, так і ризики. Розумний дім на базі IoT дуже вразливий до різних загроз безпеці як зсередини, так і за його межами, якщо порушена безпека в розумному будинку чи розумному пристрої, конфіденційність користувача, особиста інформація та безпека мешканців буде під загрозою. Безпека розумного будинку та його інформаційних ресурсів є критично важливою для безпеки та безпеки мешканців. Тому необхідно вжити відповідних заходів, щоб зробити розумний дім більш безпечним та придатним для проживання. Але ми повинні точно знати, що ми намагаємось захистити та чому, перш ніж вибирати конкретні рішення. Ретельна оцінка ризиків безпеки повинна передувати будь-якому впровадженню безпеки, щоб гарантувати, що всі відповідні основні проблеми спочатку виявляються.

Для цього з початку цієї статті було викладено ці питання дослідження, а саме:

1) Які загрози безпеці виникають від Smart Homes на базі IoT?

2) Які наслідки цих загроз (Вплив)?

3) Чи можна запропонувати відповідні контрзаходи?

4) Що рекомендувати користувачам?

В даній роботі була проведена комплексна оцінка ризику безпеки за допомогою розробленої системи та визначено 10 важливих інформаційних активів для проведення оцінки. Процес оцінки ризиків пройшов нормально і призвів до виявлення близько 15 ризиків для безпеки як усередині, так і за межами озумного будинку, як показано в таблиці 61. Звичайно, є багато інших ризиків, які там не зазначені через брак часу та збільшення кількість робочих аркушів, що

обмежували обсяг роботи. Описано наслідки ризиків, припускаючи, що загрози реалізовані.

Запропоновано відповідні контрзаходи для зменшення ризиків до прийнятного рівня, оскільки 100% безпеки ніколи не можна досягти.

У важко зв’язаному та складному середовищі, такому як розумний дім на базі IoT, зловмисник, який компрометує систему домашньої автоматизації, може завдати широкий спектр шкоди. Оцінка ризику встановлена для виявлення найсерйозніших потенційних небезпек. Одне з основних джерел ризику підключений до пристроїв та датчиків. Ризики для обладнання стосуються крадіжок та дефектів, маніпуляцій та саботажу різних пристроїв, що використовуються в АСРД, також потребують пильної уваги. Найвищий показник ризику, який становить 41, пов’язаний з інформаційними активами (обліковими даними користувачів та мобільними особистими даними та програмами), коли вони скомпрометовані. В рамках мережевого спілкування основними ризиками є неадекватна автентифікація та відсутність безпечного каналу зв'язку та шифрування. Найбільш серйозним ризиком є людський фактор, оскільки люди становлять найбільший ризик в системах розумної автоматизації дому, оскільки будинки складаються з людей різного віку, деякі з них, особливо ті, хто має обмежені технічні знання, є більш вразливими до атак соціальної інженерії, неправильного використання та неправильної конфігурації. системи. Завдяки цьому дослідження здійснило свої цілі та відповіло на питання дослідження.

Для подальшої роботи оцінка ризику безпеки буде розширена з урахуванням інших видів застосування розумних будинків, таких як розумні будинки для догляду за людьми, розумні будинки для охорони здоров'я, розумні будинки для догляду за дітьми.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ashton, K. (2009). That ‘internet of things’ thing. RFiD Journal, 22(7), 97-114.
2. Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.
3. Zhong, Y. (2015). I2oT: Advanced Direction of the Internet of Things. ZTECOMMUNICATIONS, 3.
4. Miller, M. (2015). The internet of things: How smart TVs, smart cars, smart homes, and smart cities are changing the world. Pearson Education.
5. N. K. Suryadevara and S. C. Mukhopadhyay, Smart Homes: Design, Implementation and Issues, vol. 14. Springer, 2015
6. Li, J., Huang, Z., & Wang, X. (2011, May). Notice of Retraction Countermeasure research about developing Internet of Things economy: A case of Hangzhou city. 2011 International Conference on E-Business and E-Government (ICEE).
7. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. Communications Surveys & Tutorials, IEEE, 17(4), 2347-2376.
8. Cook, D., & Das, S. (2004). Smart environments: Technology, protocols and applications (Vol. 43). John Wiley & Sons.
9. Harper, R. (2003). Inside the smart home: Ideas, possibilities and methods. Inside the smart home (pp. 1-13). Springer London.
10. Marzano, S. (2003). The new everyday: Views on ambient intelligence. 010 Publishers.
11. Nunes, R. J., & Delgado, J. (2000). An Internet application for home automation. In Electrotechnical Conference, 2000. MELECON 2000. 10th Mediterranean (Vol. 1, pp. 298-301). IEEE.
12. Kausar, F., Al Eisa, E., & Bakhsh, I. (2012). Intelligent Home Monitoring Using RSSI in Wireless Sensor Networks. International Journal of Computer Networks & Communications, 4(6), 33.
13. Saad al-sumaiti, A., Ahmed, M. H., & Salama, M. M. (2014). Smart home activities:

A literature review. Electric Power Components and Systems, 42(3-4), 294-305.

14. Zupancic, D., & Cvetkovic, B. (2014). Smart-home energy management in the context of occupants' activity. Informatica, 38(2), 171.

15. Bin, S., Yuan, L., & Xiaoyi, W. (2010, April). Research on data mining models for the internet of things. In Image Analysis and Signal Processing (IASP), 2010 International Conference on (pp. 127-132). IEEE.

16. Nutihouse. (2016). Available: http://nutihouse.com/

17. Steinberg, Joseph. (2014). "These Devices May Be Spying On You (Even In Your Own Home)". http://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-bespying-on-you-even-in-your-own-home/.

18. EVANS, D. (2011). The internet of things. How the Next Evolution of the Internet is Changing Everything, Whitepaper, Cisco Internet Business Solutions Group (IBSG). http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

19. Montano, C., Lundmark, M., & Mähr, W. (2006). Control vs convenience: critical factors of smart homes. In 2nd Scandinavian Student Interaction Design Research Conference.

20. Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. Journal of Computer and Communications, 3(05), 164.

21. Granzer, W., Kastner, W., Neugschwandtner, G., & Praus, F. (2006). Security in networked building automation systems. na.

22. Al-Qutayri, M. A., & Jeedella, J. S. (2010). Integrated Wireless Technologies for Smart Homes Applications. INTECH Open Access Publisher.

23. De Silva, L. C., Morikawa, C., & Petra, I. M. (2012). State of the art of smart homes. Engineering Applications of Artificial Intelligence, 25(7), 1313-1321.

24. Kyas, O. (2013). How to Smart Home. Tanggal akses terakhir, 3.

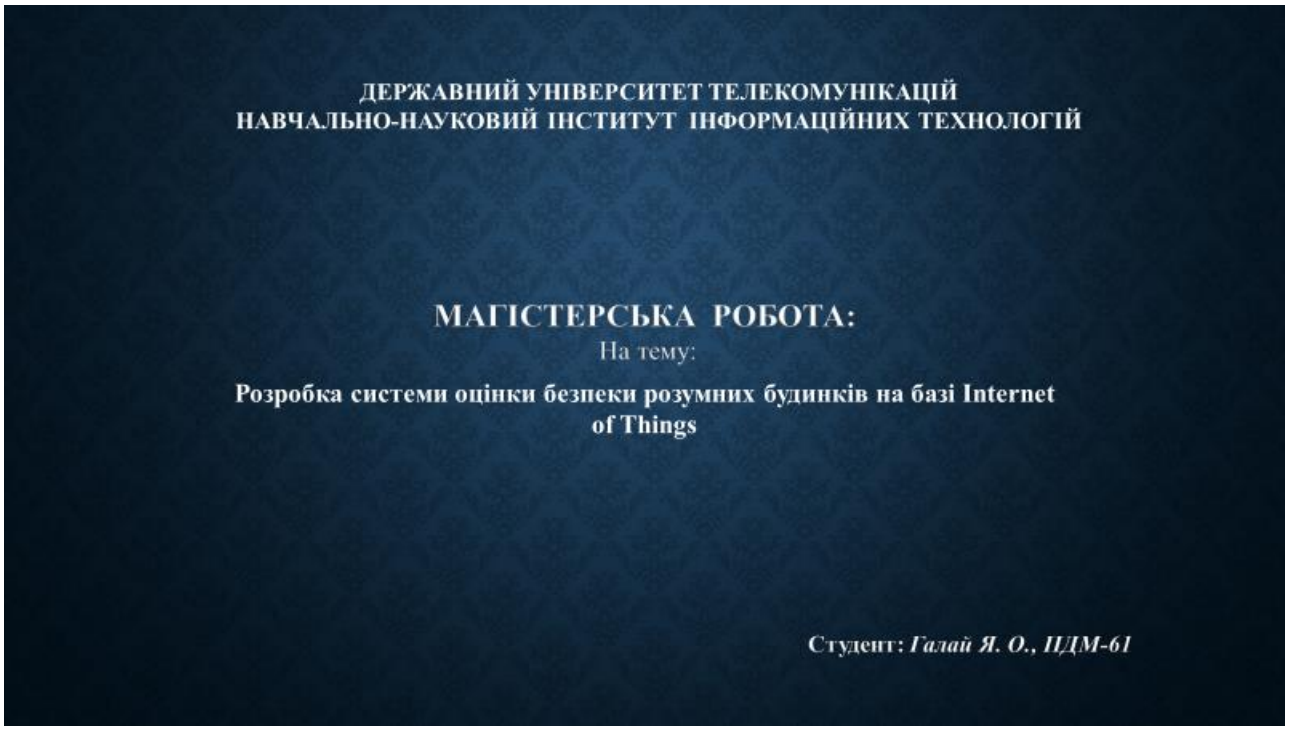
25. Yoo, D. Y., Shin, J. W., & Choi, J. Y. (2007, December). Home-Network Security Model in Ubiquitous Environment. In Proceedings of World Academy of Science, Engineering and Technology (Vol. 26).

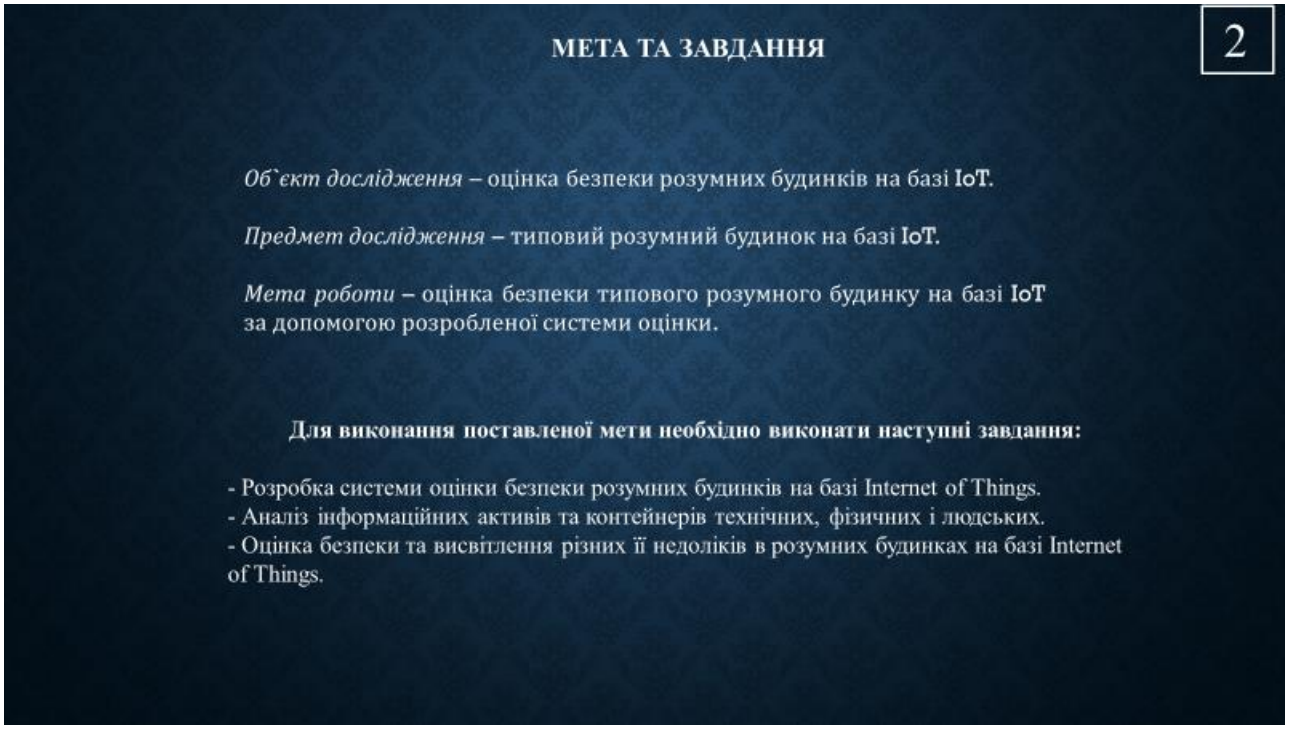
26. Ricquebourg, V., Menga, D., Durand, D., Marhic, B., Delahoche, L., & Loge, C. (2006, December). The smart home concept: our immediate future. In E-Learning in

Industrial Electronics, 2006 1ST IEEE International Conference on (pp. 23-28). IEEE.
27. Chong, G., Zhihao, L., & Yifeng, Y. (2011, September). The research and implement of smart home system based on internet of things. In Electronics, Communications and Control (ICECC), 2011 International Conference on (pp. 2944-2947). IEEE.
28. Bing, K., Fu, L., Zhuo, Y., & Yanlei, L. (2011, July). Design of an Internet of things-based smart home system. In Intelligent Control and Information Processing (ICICIP), 2011 2nd International Conference on (Vol. 2, pp. 921-924). IEEE.
29. Darianian, M., & Michael, M. P. (2008, December). Smart home mobile RFID-based Internet-of-Things systems and services. In Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference on (pp. 116-120). IEEE.
30. Li, B., & Yu, J. (2011). Research and application on the smart home based on component technologies and Internet of Things. Procedia Engineering, 15, 2087-2092.
31. Yoo, D. Y., Shin, J. W., & Choi, J. Y. (2007, December). Home-Network Security Model in Ubiquitous Environment. In Proceedings of World Academy of Science, Engineering and Technology (Vol. 26).
32. Nixon, P. A., Wagealla, W., English, C., & Terzis, S. (2004). Security, privacy and trust issues in smart environments. Smart Environments: Technologies, Protocols and Applications.
33. Schiefer, M. (2015, May). Smart Home Definition and Security Threats. In IT Security Incident Management & IT Forensics (IMF), 2015 Ninth International Conference on (pp. 114-118). IEEE.
34. Papadopoulos, K., Zahariadis, T., Leligou, N., & Voliotis, S. (2008, April). Sensor networks security issues in augmented home environment. In Consumer Electronics, 2008. ISCE 2008. IEEE International Symposium on (pp. 1-4). IEEE.
35. Can, O., & Sahingoz, O. K. (2015, May). A survey of intrusion detection systems in wireless sensor networks. In Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on (pp. 1-6). IEEE.
36. Robles, R. J., Kim, T. H., Cook, D., & Das, S. (2010). A review on security in smart home development. International Journal of Advanced Science and Technology, 15.

37. Liu, Y., Hu, S., & Ho, T. Y. (2014, November). Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks. In Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design (pp. 183-190). IEEE Press.
38. Yang, L., Yang, S. H., & Yao, F. (2006, October). Safety and security of remote monitoring and control of intelligent home environments. In Systems, Man and Cybernetics, 2006. SMC'06. IEEE International Conference on (Vol. 2, pp. 1149-1153). IEEE.
39. Mantoro, T., & Ayu, M. A. (2014, April). Securing the authentication and message integrity for Smart Home using smart phone. In Multimedia Computing and Systems (ICMCS), 2014 International Conference on (pp. 985-989). IEEE.
40. Tong, J., Sun, W., & Wang, L. (2013, May). An information flow security model for home area network of smart grid. In Cyber Technology in Automation, Control and Intelligent Systems (CYBER), 2013 IEEE 3rd Annual International Conference on (pp. 456-461). IEEE.
41. McCune, J. M., Perrig, A., & Reiter, M. K. (2005, May). Seeing-is-believing: Using camera phones for human-verifiable authentication. In Security and privacy, 2005 IEEE symposium on (pp. 110-124). IEEE.
42. Zuo, F., & De With, P. H. (2005). Real-time embedded face recognition for smart home. Consumer Electronics, IEEE Transactions on, 51(1), 183-190.
43. Essaaidi, M., Maugeri, M., & Badica, C. (Eds.). (2010). Intelligent Distributed Computing IV: Proceedings of the 4th International Symposium on Intelligent Distributed Computing-IDC 2010, Tangier, Morocco, September 2010 (Vol. 315). Springer.
44. Gary, S., Alice, G., & Alexis, F. (2002). NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. Gaithersburg, MD: National Institute of Standards and Technology (NIST). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
45. Padyab, A. M., Paivarinta, T., & Harnesk, D. (2014, January). Genre-Based Assessment of Information and Knowledge Security Risks. In System Sciences

ДОДАТКИ


ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
МАГІСТЕРСЬКА РОБОТА:
На тему:
Розробка системи оцінки безпеки розумних будинків на базі Internet of Things
Студент: Галай Я. О., ІДМ-61

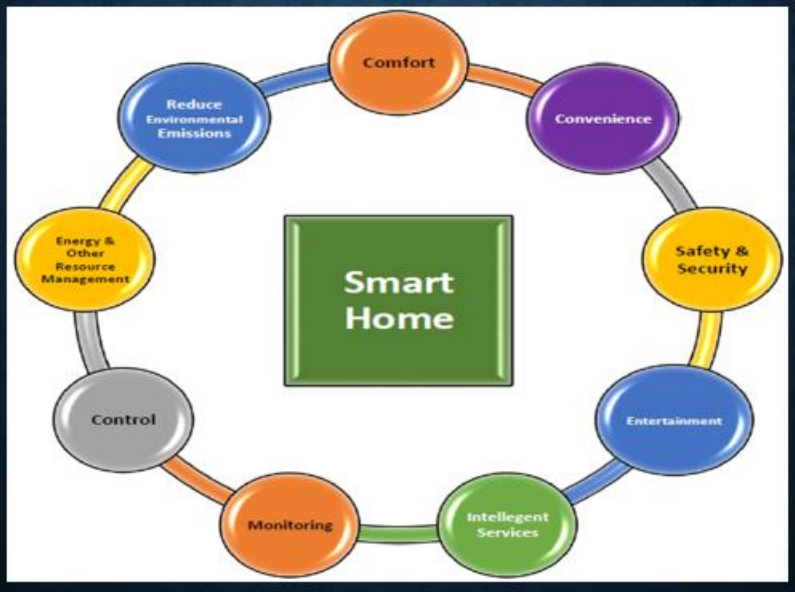

МЕТА ТА ЗАВДАННЯ
2
Об`єкт дослідження – оцінка безпеки розумних будинків на базі IoT.
Предмет дослідження – типовий розумний будинок на базі IoT.
Мета роботи – оцінка безпеки типового розумного будинку на базі IoT за допомогою розробленої системи оцінки.
Для виконання поставленої мети необхідно виконати наступні завдання:
- Розробка системи оцінки безпеки розумних будинків на базі Internet of Things.
- Аналіз інформаційних активів та контейнерів технічних, фізичних і людських.
- Оцінка безпеки та висвітлення різних її недоліків в розумних будинках на базі Internet of Things.

ЗАГАЛЬНІ ВІДОМОСТІ ІНТЕРНЕТУ РЕЧЕЙ

3

ОГЛЯД РОЗУМНИХ БУДИНКІВ НА БАЗІ IoT

4

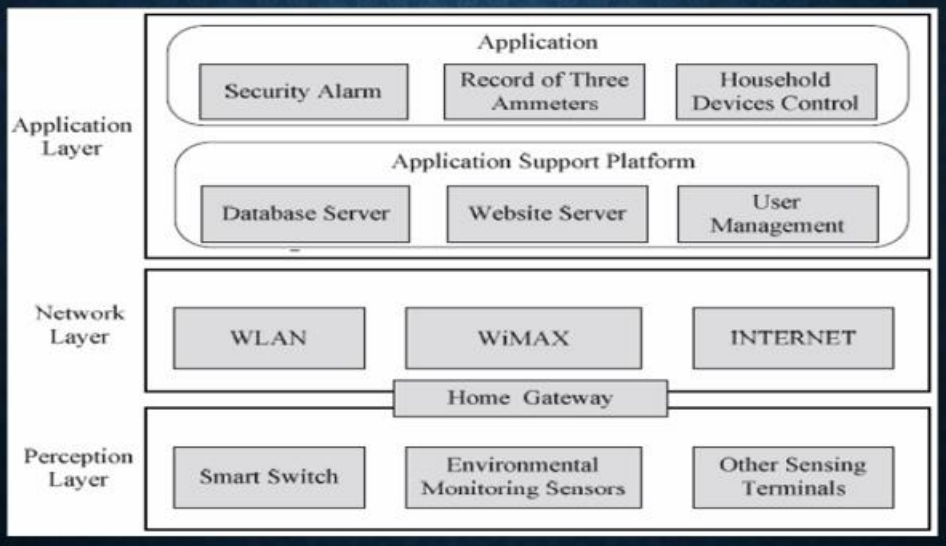


ОГЛЯД РОЗУМНИХ БУДИНКІВ НА БАЗІ IoT

5

РІВНЕНВА АРХІТЕКТУРНА МОДЕЛЬ КОНТРОЛЮЮЧОЇ СИСТЕМИ РОЗУМНОГО БУДИНКУ НА БАЗІ IoT

6



РОЗРОБЛЕНА СИСТЕМА ОЦІНКИ БЕЗПЕКИ

7

- **ФАЗА 1**

  1. Встановити критерії вимірювання ризику.

- **ФАЗА 2**

  2. Розробка профілю активів інформації.

  3. Визначити контейнери інформаційного майна.

- **ФАЗА 3**

  4. Визначити питання, що викликають занепокоєння.

  5. Визначити сценарії загрози.

- **ФАЗА 4**

  6. Визначити ризики.

  7. Проаналізуйте ризики.

  8. Визначити підхід пом'якшення наслідків.

ОПИС ПЕРШОЇ ФАЗИ

8

- На цьому етапі (Крок 1) створюється основа для оцінки ризику інформаційних активів, розробляючи набір критеріїв оцінки ризику для розумного будинку.
- Ці критерії дозволяють виміряти ступінь впливу зацікавлених сторін розумного будинку у випадку виникнення ризику для інформаційного активу. Окрім визнання масштабу впливу, нам потрібно визначити найбільш значну область впливу.
- Ці критерії відображають цілий ряд областей впливу, важливих для зацікавлених сторін розумного будинку. Наприклад, сфери впливу можуть включати охорону здоров'я та безпеку користувачів, фінанси, репутацію, закони та правила тощо. Отже, створюємо ці критерії в кількох сферах впливу, а потім ставимо їх пріоритетами від найважливіших до найменших. Найважливіша категорія отримує найвищий бал (5), а найменш важлива - найнижчий (1).

ОПИС ДРУГОЇ ФАЗИ

9

- На цьому етапі (кроки 2 та 3) спочатку визначаються критично важливі інформаційні ресурси, а потім складається їхій профіль.
- У процесі профілювання встановлюються чіткі межі для активу, визначаються його вимоги до безпеки, а потім визначаються усі місця, де асктив зберігається, транспортується або обробляється, або де ці активи використовуються власниками розумних будинків або автоматизаційна система розумного будинку, як здійснюється доступ до активів та хто відповідає за ці активи. Документується логічні, технічні, фізичні та людські активи.
- Таким чином, можна визначити точки, в яких вимоги безпеки (Конфіденційність, Цілісність та Доступність) інформаційного активу порушуються чи якимось чином їхні активи не мають відповідних задовільняючих умов.

ОПИС ТРЕТЬОЇ ФАЗИ

10

У цій фазі (кроки 4 та 5) зосередження на виявленні загроз щодо ідентифікованих активів контексті місць, де інформаційний актив зберігається, транспортується або обробляється. Області, що викликають занепокоєння (вразливості), охоплюються та розширюються на сценарії загрози, що додатково деталізують властивості загрози. Визначаються конкретні загрози, які можуть негативно вплинути на безпеку об'єкта.

ОПИС ЧЕТВЕРТОЇ ФАЗИ

11

На заключному етапі (крок 6, крок 7 та крок 8) визначаються ризики для інформаційних активів, визначаючи, як сценарії загрози можуть вплинути на розумний дім (наслідки), та їх аналіз. Нарешті, після цього кроку визначається стратегія зменшення наслідків для кожного з виявлених ризиків.

Загроза + Вплив = Ризик.

РЕКОМЕНДАЦІЇ КОМЕРЦІНО ЗАЦІКАВЛЕНИМ СТОРОНАМ

12

1) Існує велика потреба інтегрувати безпеку на етапі проектування та розробки.
2) Усі товари та послуги, які впливають на життя та безпеку мешканців, повинні мати вимоги високого рівня безпеки.
3) Безпека поліпшується в системах, блокуючи доступ до сторінки входу на деякий час після послідовних невдалих спроб входу. Це захищає систему від атак грубої сили та атак на основі словників.
4) вимагати від споживачів змінити паролі за замовчуванням під час процесу налаштування.
5) Існує потреба в юридичній підтримці в забезпеченні конфіденційності в середовищах IoT, і конфіденційність повинна розглядатися вже під час проектування систем IoT.
6) Існує потреба у стандартах безпеки (основна вимога до виробників).
7) Перед випуском продуктів краще протестувати свої заходи безпеки і не забути закрити всі задні двері в продуктах. Погано для вашої репутації.
8) Компанії повинні продовжувати виправляти відомі вразливі місця протягом усього життєвого циклу продукції.
9) Слід розробити методології оцінки ризиків для безпеки, які можуть охоплювати обмеження в пристроях.
10) Будьте прозорими та повідомте своїм клієнтам, як ви використовуєте їх конфіденційну інформацію.

ОПИС ЧЕТВЕРТОЇ ФАЗИ

1. Дуже важливо встановити безпечні імена користувачів та паролі для всіх систем домашньої автоматизації, а не залишати їх за замовчуванням.
2. Зберігайте свої паролі надійними та непередбачуваними. Використовуйте довгий пароль із великими та малими літерами, цифрами та спеціальними символами. Часто міняйте їх на всіх своїх системах та пристроях.
3. Уникайте використання простих для вгадування послідовностей, таких як „123456".
4. Не використовуйте повторно встановлені вами паролі для інших цілей.
5. Будьте в курсі подій та встановлюйте всі оновлення мікропрограми та програмного забезпечення, доступні для встановлених пристроїв.
6. Споживачі повинні вибирати свої системи та пристрої серед відомих постачальників з доброю репутацією, а не серед постачальників з обмеженим досвідом у галузі безпеки.
7. Уникайте передачі інфраструктури стороннім постачальникам послуг, оскільки вони не впевнені, що вони обізнані про всі ризики та вимоги безпеки.
8. Не обирайте зручність та простоту використання над безпекою, якщо вам надано вибір.
9. Налаштуйте маршрутизатор та системи належним чином. Для цього ви повинні бути кваліфікованою особою в галузі безпеки, інакше це призводить до власного набору вразливостей. Виберіть свій маршрутизатор із захищеним доступом Wi-Fi (WPA2), щоб забезпечити максимальний захист від хакерів.
10. Оновлення та оновлення пристроїв. Не продовжуйте зі старими.

ДЯКУЮ ЗА УВАГУ
ДОПОВІДЬ ЗАВЕРШЕНО