Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри
кібербезпеки
та захисту інформації
Н.В. Лукова-Чуйко

“_____”_____2021 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
_____магістра_____
(назва освітньо-кваліфікаційного рівня)

галузь знань 12 «Інформаційні технології»
(шифр і назва галузі знань)

напрям підготовки/ спеціальність 125 «Кібербезпека»
(код і назва напряму підготовки)

кваліфікація _____
(код і назва кваліфікації)

на тему: Методи дослідження кібербезпеки розумного будинку

Виконавець: студент курсу VI, групи КБм-21

_____ **Бєліков Андрій Миколайович**
(підпис) (прізвище ім’я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Керівник	Наконечний В.С.		

Нормоконтроль			

Київ 2021

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту
інформації
Н.В. Лукова-Чуйко

“___”_____2021 року

ЗАВДАННЯ
на виконання дипломної роботи

напряму підготовки 125 «Кібербезпека»
(код і назва напряму підготовки)

студенту **КБм-21** **Бєліков Андрій Миколайович**
(група) (прізвище ім’я по-батькові)

Тема дипломної роботи *Методи дослідження кібербезпеки розумного будинку*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ
Тема дипломної роботи затверджений на засіданні кафедри кібербезпеки та захисту інформації протоколом №2 від __ . __ . 2021 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ
Об’єкт досліджень Методи дослідження безпеки системи розумного будинку

Предмет досліджень Методи пом'якшення ризиків безпеки що можуть виникнути в системі розумного будинку

Мета роботи Аналіз та комплексне визначення проблем в безпеці сучасного

розумного будинку та надання рекомендацій щодо їх вирішення.

Вихідні дані для проведення роботи Механізми оцінки ризиків системи розумного будинку

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ

Практична цінність Вперше була проведена комплексна оцінка ризику безпеки для всієї системи розумного будинку та надані методичні рекоменації щодо пом'якшення ризиків

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота повинна виконуватися згідно діючої законодавчої та нормативної бази в сфері аудиту інформаційної безпеки

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	12.10.2020 – 16.10.2020
Аналіз літератури	17.10.2020 – 10.12.2020
Аналіз міжнародного документу для визначення біометричних методів	11.12.2021 – 12.01.2021
Дослідження процессу біометричної ідентифікації	23.01.2021 – 12.02.2021
Дослідження поширених методів	13.02.2021 – 25.02.2021
Аналіз механізмів	26.02.2021 – 16.03.2021
Дослідження та розробка ПЗ	17.03.2021 – 04.04.2021
Проведення порівняльної характеристики різних методів	05.04.2021 – 16.04.2021
Вибір найефективнішого методу ідентифікації	17.04.2021 – 29.04.2021
Формування висновків і рекомендацій вдосконалення системи ідентифікації	30.04.2021 – 07.05.2021
Оформлення пояснювальної записки	08.05.2021 – 12.05.2021

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Підготовка до захисту дипломної роботи	13.05.2021 – 15.05.2021

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект _____

_____

_____

Соціальний ефект _____

_____

_____

7. ДОДАТКОВІ ВИМОГИ

_____

_____

Завдання видав _____ __Наконечний В.С.__
(підпис) (ініціали, прізвище)

Завдання прийняв
до виконання _____ __Бєліков А.М.___
(підпис) (ініціали, прізвище)

Дата видачі завдання: __ «_____» 2020 року
Термін подання дипломної роботи до ЕК __ «_____»2021 року

УДК 621.391

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Методи дослідження кібербезпеки розумного будинку» складається зі вступу, основної частини, що містить 7 розділів, висновків, списку літератури та джерел. Загальний обсяг роботи – 111 сторінок. Робота містить 12 рисунків та 46 таблиць. Список використаних джерел включає 44 джерела.

Об'єкт дослідження – процес дослідження безпеки системи розумного будинку.

Предмет дослідження – методи пом'якшення ризиків безпеки що можуть виникнути в системі розумного будинку.

Мета роботи – аналіз та визначення проблем в безпеці сучасних розумних будинків та надання рекомендацій щодо їх вирішення.

Метод дослідження – для дослідження проблеми була використана методологія OCTAVE Allegro, яка спрямована на забезпечення надійності результатів та дозволяє комплексно оцінити можливі ризики безпеки.

Наукова новизна – у існуючих роботах, що висвітлюють питання безпеки системи розумного будинку відсутні можливі рішення чи контрзаходи для вирішення потенційних загроз безпеки, тож у цій роботі була проведена комплексна оцінка ризику безпеки для всієї системи.

Практична цінність – виконана робота може бути використана в якості основи для специфікації вимог безпеки в системі розумному будинку в подальшому.

Ключові слова: інтернет речей, розумні будинки, інтелектуальні будинки, автоматизація будівель, розумні будівлі, оцінка ризиків безпеки, рекомендації щодо безпеки, загрози безпеці, заходи безпеки.

ЗМІСТ

ВСТУП

Інтернет IoT - парадигма, що фокусується на взаємозв'язку речей та пристроїв між собою та користувачами [3]. З часом більшість зв'язків в Інтернеті речей переходять від зв'язку „від людини до речі" до зв'язку „від речі до речі". Очікується, що ця технологія стане важливою для розвитку розумних будинків, з метою принести зручність та ефективність у наше життя та наші будинки. Але інтеграція цієї технології матиме важливе значення для нашої безпеки.

Підключення всіх приладів усередині будинку до Інтернету та між собою призводить до можливих проблем безпеки, конфіденційності, достовірності та цілісності даних. Ця технологія дуже вразлива до різних атак, які роблять розумний дім на базі IoT небезпечним для проживання, тому для оцінки рівня безпеки таких осель необхідно оцінити ризики безпеки.

Для того, щоб будь-яка технологія мала успіх і досягла широкого використання, вона повинна завоювати довіру користувачів, забезпечуючи достатню безпеку та конфіденційність. Оскільки будинки дедалі більше комп'ютеризуються та наповнюються пристроями, потенційні атаки, спрямовані на комп'ютерну безпеку та їх вплив на мешканців вимагають більшого дослідження.

Дана робота базується на використанні методології OCTAVE Allegro, яка фокусується головним чином на інформаційних ресурсах та проводить оцінку ризику безпеки з метою висвітлення різних недоліків безпеки в розумному домі та пропонування контрзаходів щодо виявлених проблем, що задовольняють більшість вимог безпеки. Також в роботі буде запропоновано декілька рекомендацій для користувачів. Результати дослідження, задокументовані в дипломній роботі, стануть корисним внеском, який може бути використаний як основа для специфікації вимог безпеки.

СКОРОЧЕННЯ

BAS	Система автоматизації будівель
DOS	Відмова в обслуговуванні
DTLS	Безпека транспортного рівня
IDS	Система виявлення вторгнень
IoT	Інтернет речей
IoE	Інтернет усього
IPS	Система запобігання проникненню
IPsec	Безпека Інтернет-протоколу
KNX	Konnex
LAN	Локальна мережа
LON	Локальна операційна мережа
NFC	Зв'язок на невеликих відстанях
OCTAVE	Методологія оцінки критично важливих загроз, активів та вразливостей
PAN	Персональна мережа
PLC	Зв'язок лінії електропередач
SH	Розумний дім
SHAS	Розумна система автоматизації будинку

РОЗДІЛ 1
СИСТЕМА РОЗУМНОГО БУДИНКУ ЯК КОМПОНЕНТ I_OT

1.1 Передумови розвитку

Загалом, не існує загального визначення терміну Інтернет речей. Існує багато різних людей, які визначили цей термін, хоча його початкове використання приписується експерту з цифрових інновацій Кевіну Ештону [1]. У всіх визначеннях описується, що перша версія Інтернету стосувалася даних, створених людиною, тоді як наступна версія стосувалась даних, створених речами, тому вона називалася Інтернетом речей. Існує багато визначень для Інтернету речей. Нижче наведено деякі визначення:

IoT визначали як «динамічну глобальну мережеву інфраструктуру з можливостями самоконфігурування на основі стандартів та сумісних протоколів зв'язку; фізичні та віртуальні «речі» в IoT мають атрибути і здатні бути інтегрованими як інформаційна мережа» [2].

Мета IoT - підвищити функції Інтернету та зробити його більш корисним. 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 різноманітних технологій. Це також можна описати як написання алгоритму дій для різних об’єктів, які можуть помітити зміни у своєму фізичному стані та відреагувати на них.

Загальним визначенням IoT є опис того, що комп’ютери, датчики та об’єкти взаємодіють між собою та обробляють дані, тому можна стверджувати, що IoT - це нова технологічна система, об’єднана низкою інформаційних технологій [3]. Інтернет речей поєднує різні технології в

напівавтономну мережу. Він підключає окремі пристрої до мережі та з'єднує їх між собою. У мережі також існує програмне забезпечення що виконує функції головного мозку системи для обробки даних шляхом аналізу та використання даних, зібраних підключеними пристроями, для прийняття рішень та ініціювання дій з іншими пристроями [4].

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

Елементи IoT зображені на рисунку 1.1 [7]

Рисунок 1.1 - Елементи IoT [7]

Розумні середовища спрямовані на використання 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 комфорт і поліпшити якість нашого життя.

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

За допомогою IoT можна отримати віддалений доступ до електронних пристроїв, встановлених у вашому домі, та керувати ними в будь-якому місці

та в будь-який час. Наприклад, розумні будинки дозволять своїм мешканцям автоматично відкривати гараж, коли добираються додому, готувати каву, керувати системами кондиціонування, смарт-телевізорами та іншими побутовими приладами всередині будинку. Розумні пристрої та системи автоматизації складають Smart Home (SH) [4].

В основному розумні будинки оснащені автоматичними системами для виконання різних запрограмованих операцій та завдань, таких як регулювання температури, освітлення, мультимедіа, робота з вікнами та дверима тощо [10].

SH - дуже перспективна сфера, яка має різні переваги, такі як забезпечення комфорту, безпеки, більш раціональне використання енергії та інших ресурсів, що сприяє значній економії. Ця область досліджень дуже важлива і з часом буде збільшуватися, оскільки вона також пропонує потужні засоби для допомоги та підтримки потреб людей похилого віку та людей з обмеженими можливостями, для моніторингу навколишнього середовища та контролю за безпекою [11, 12]. Відповідно до статті Кевіна Роялза [13], основними цілями розумного будинку є підвищення автоматизації внутрішніх процесів, спрощення управління побутовими приладами та зменшення шкідливих викидів в навколишнє середовище. Споживання енергії та комфорт мешканців також є ключовими факторами [14].

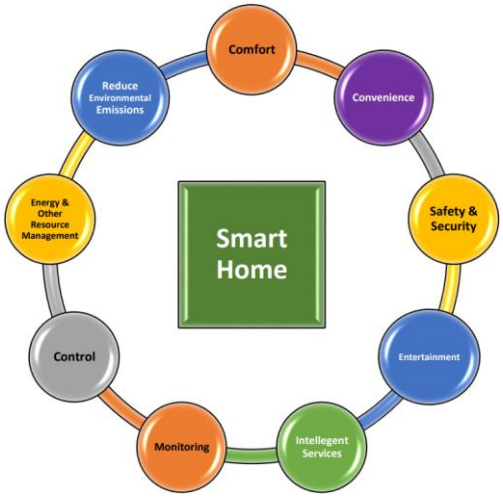

Рисунок 1.2 - Цілі розумного будинку

Більшість комерційних систем домашньої автоматизації можна розділити на дві категорії [7]: системи з локальним управлінням та системи з дистанційним управлінням. Локально керовані системи використовують домашній контролер для досягнення домашньої автоматизації, що дозволяє користувачам повністю використовувати свою систему автоматизації всередині будинку за допомогою стаціонарного або бездротового інтерфейсу. 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 через телефон [15].

Система інтеграції розумного будинку складається приблизно з трьох важливих об'єктів [12]:

По-перше, фізичні компоненти (електронне обладнання - розумні датчики та інші прилади).

По-друге, система зв'язку (дротова / бездротова мережа), яка зазвичай з'єднує фізичні компоненти.

По-третє, інтелектуальна обробка інформації (наприклад, за допомогою програми штучного інтелекту) [5].

На рисунку 1.3 показано розумний дім та його підсистеми [16].

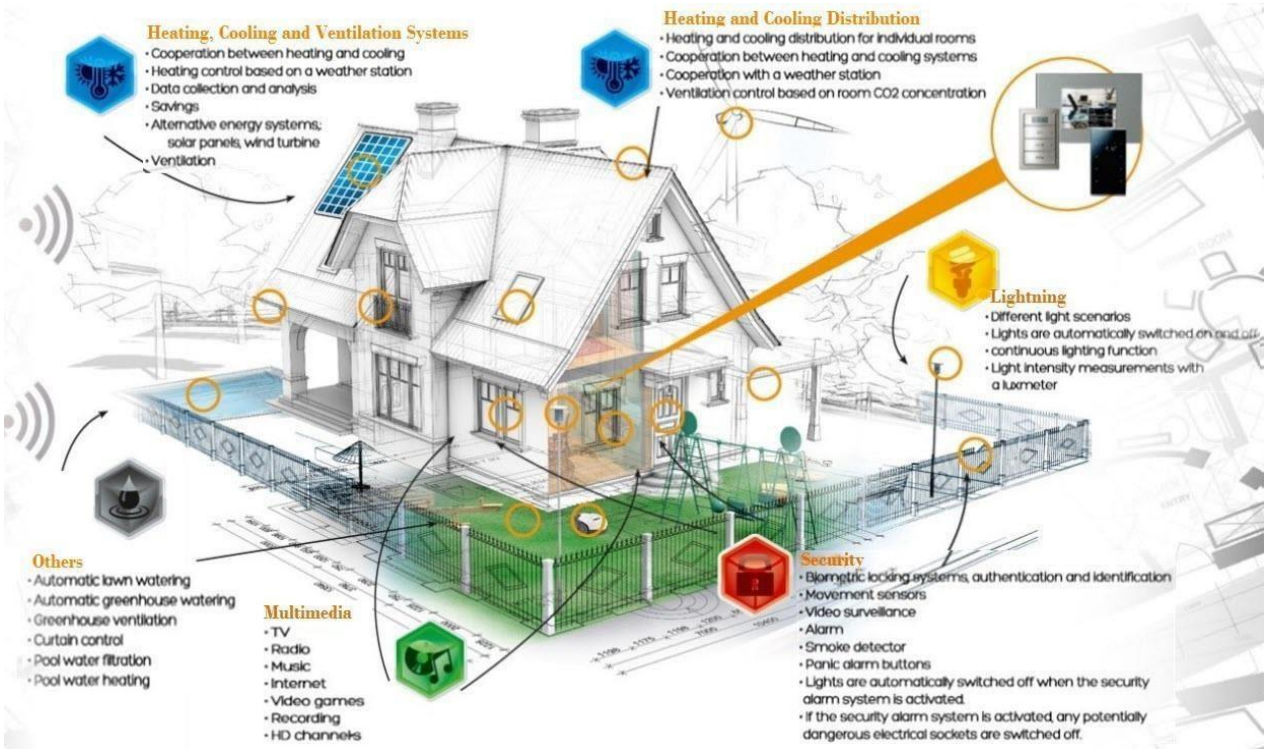

Рисунок 1.3 - Розумний дім та його підсистеми

Інтеграція технології IoT в наші будинки може стати потенційною причиною виникнення дір в безпеці, тому розумні будинки, засновані на IoT, вимагають високого рівня безпеки, оскільки домашнє середовище містить важливу та приватну інформацію. Сучасні технології пропонують як можливості, так і ризики. Розумний дім на базі IoT дуже вразливий до атак з Інтернету, якщо хакер отримає доступ до системи то він може вторгнутись у конфіденційність користувача, викрасти особисту інформацію, і тому необхідно вжити відповідні заходи [17].

Кількість пристроїв IoT швидко зростала, недавня оцінка показує, що в 2010 році було 12,5 мільярда пристроїв, підключених до Інтернету, і прогнозується збільшення до 50 мільярдів пристроїв до 2025 року [18]. Це призведе до багатьох проблем безпеки.

Запропоноване дослідження буде зосереджене на аналізі питань безпеки в інтелектуальних домах, що базуються на Інтернеті речей, та в кінці дасть деякі рекомендації щодо підвищення безпеки кінцевому користувачеві.

1.2 Постановка проблеми

Останні статті стосовно розвитку IoT та Smart Homes викликали суспільний інтерес. Потреба в безпеці в розумних будинках навіть більша, ніж у всіх інших обчислювальних системах. Потрібно переконатися, що інформація не викрадена, не модифікована або до неї не було отримано доступу.

Очевидно, що в традиційних будинках зловмисники можуть викрасти цінності з будинку лише в тому випадку, якщо вони фізично знаходяться в домі. Але в розумному будинку зловмисник має можливість отримати доступ до будинку та керувати ним з будь-якої точки світу в будь-який час та стежити за мешканцями будинку за допомогою підключених камер.

Системи розумного будинку дозволяють користувачеві контролювати, наприклад, термостати, пральні машини, робота-прибиральника, розважальні системи, системи безпеки, детектори диму, дверні замки. При введенні цієї технології у наші будинки виникають компроміси між зручністю, контролем, безпекою та конфіденційністю [19].

Зловмисники можуть вторгнутися в конфіденційність користувача, викрасти приватну інформацію та відстежувати мешканців всередині будинку, якщо їм вдасться зламати розумний дім або його пристрій [17]. Варто зазначити, що розумний дім є привабливою мішенню для зловмисника, оскільки він містить особисту інформацію.

Дане дослідження стосуватиметься оцінки ризиків інформаційної безпеки в розумних будинках на базі IoT. Ця робота досліджує загрози інформаційної безпеки при підключенні інтелектуальних пристроїв один до одного та до Інтернету при проектуванні розумного будинку, щоб поінформувати користувачів про ризики безпеки, покращити безпеку та дати

рекомендації.

1.3 Дослідження літератури стосовно розумних будинків

На основі аналізу літератур теми дослідження, можна зробити висновок, що потрібно 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.

Під час дослідження 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 з питань інформаційної безпеки виникають у Smart Homes?
2. Які можуть бути наслідки цих загроз?
3. Чи можна запропонувати контрзаходи?
4. Що можна рекомендувати користувачам для підвищення безпеки?

Дуже важливо провести дослідження з питань безпеки в Smart Homes, щоб краще зрозуміти та уникнути серйозних наслідків. Без оцінки ризику безпеки або висвітлення загроз неможливо надати гарантію системі та вжиті заходи безпеки.

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

1.4 Очікуваний внесок

Результати дослідження стануть корисним внеском у забезпечення кращого розуміння загроз безпеці щодо даної теми та допоможуть користувачам усвідомити потенційні ризики та заходи, які можуть бути вжиті для зменшення цих ризиків щодо їхніх розумних будинків. Сподіваюсь, що отримані результати призведуть до подальших досліджень в галузі безпеки Інтернету речей, до якої можна віднести систему Smart Home.

Результатом цього дослідження буде перелік виявлених загроз безпеці з можливими наслідками, рішення та рекомендації для користувачів з метою зменшення ризиків безпеки. Результати дипломної роботи можуть бути використані для вдосконалення впровадження технології IoT у розумні будинки з урахуванням ризиків безпеки.

Основна увага в цьому дослідженні буде зосереджена на виявленні проблем безпеки, відповідних контрзаходів, а також на наданні рекомендацій користувачам. Основна увага в цій роботі присвячена оцінці ризику безпеки критично важливих інформаційних активів у типовому розумному будинку за допомогою методології OCTAVE Allegro для визначення та аналізу існуючих ризиків в безпеці.

1.5 Технологія розумного будинку та IoT

Сучасні розробки інформаційно-комунікаційних технологій, пов'язані з комп'ютерними мережами, вбудованими системами та штучним інтелектом, зробили бачення розумного будинку технічно можливим. Отож, удосконалюючи традиційні системи автоматизації будинку новими розумними функціями, стало можливим демонструвати різні форми штучного інтелекту. Технологія розумного будинку - це технологія підвищення якості життя.

1.6 Області застосування

Інтернет речей забезпечує гнучкість та масштабованість системи, яка може підтримувати безліч різних додатків. Його популярність призвела до створення різноманітних програмних додатків, зокрема розумних будинків.

Основною сферою застосування системи автоматизації розумного будинку (SHAS) стає навколишнє середовище за допомогою контролю системи освітлення, опалення, вентиляції та кондиціювання повітря [21].

Існують різні типи застосування розумних будинків [23]:

- 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 більшої енергоефективності;
- розумні будинки для кращого життя (музика, розваги тощо).

1.7 Структура будинку

Розумний дім може бути описаний як будинок, що обладнаний розумними об'єктами. Домашня мережа дозволяє транспортувати інформацію між об'єктами по житловому шлюзу при підключенні розумного будинку до зовнішнього Інтернет-світу.

Прилади, що входять до системи розумного будинку включають безліч компонентів, таких, як побутову техніку або побутову електроніку, які підключені до системи автоматизації будинку та керуються нею. Різні типи технологій підключення, такі як WLAN, Bluetooth, Z-Wave-інтерфейси тощо, використовуються для прямого підключення до керуючої мережі.

Існують датчики для широкого спектру використання, наприклад, для вимірювання температури, вологості, світла, газу та виявлення руху чи шуму. Пристрої IoT, оснащені датчиками, будуть виконувати роль зі збору даних, а вбудовані в систему виконавчі механізми виконувати корисну роботу.

Мережа управління 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 [25]:

- бездротова передача
- кабельна передача

Ethernet є найбільш широко використовуваним протоколом для побутової мережі дротового зв'язку, а бездротовими протоколами, доступними для домашньої мережі, є ZigBee, Bluetooth та інші .

Книга ДеСільви [22] робить огляд на основні технологій бездротового зв'язку, які становлять важливу частину інфраструктури сучасних розумних будинків. Деякі з цих технологій інтегровані в сенсорні та мережеві пристрої. Інші бездротові технології, такі як GSM можуть утворювати велику мережу і в той же час можуть інтегруватися з іншими технологіями короткого радіусу дії.

Згідно з літературою [21], комунікаційні мережі, як правило, реалізуються за дворівневою ієрархічною моделлю, як показано на рис 1.5.

Верхній рівень магістралі пов'язує кілька підмереж управління з високою пропускною здатністю. Він також забезпечує зв'язок із зовнішнім світом (наприклад, Інтернетом). Вузли управління розташовані на магістралі, оскільки вони вимагають загального огляду.

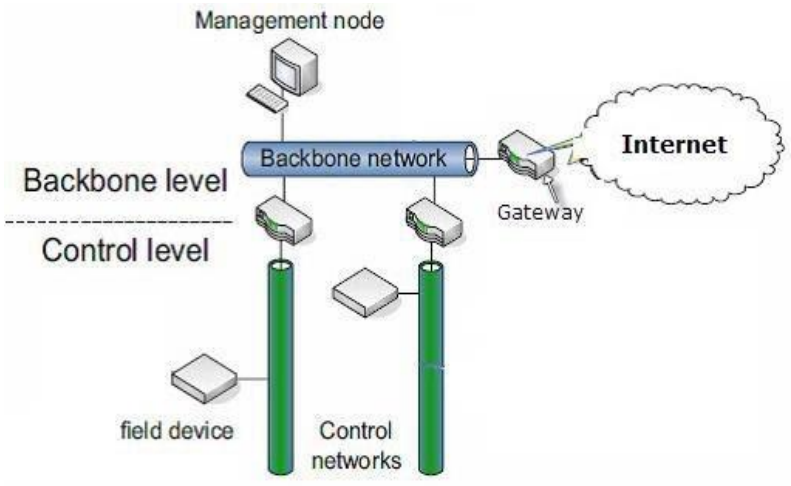

Рисунок 1.5 - Дворівнева модель комунікаційної мережі

Контролер - це комп'ютерна система, яка діє як мозок системи будинку [17]. Він збирає інформацію за допомогою датчиків і отримує команди через пристрої дистанційного керування. Контролер діє на основі команд або набору заздалегідь визначених правил, використовуючи виконавчі механізми або засоби зв'язку, такі 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 системи свого дому, може запитувати інформацію про стан пристрою з бази даних через веб-сервер. Мікроконтролер управляє всіма операціями та зв'язками в домашній мережі.

Пристрої дистанційного керування, такі як смартфони, планшети, ноутбуки та ПК, можна використовувати для підключення до програми автоматизації дому на домашньому контролері. Вони роблять це або шляхом підключення 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 рисунку 1.6 показані компоненти типової системи розумного будинку.

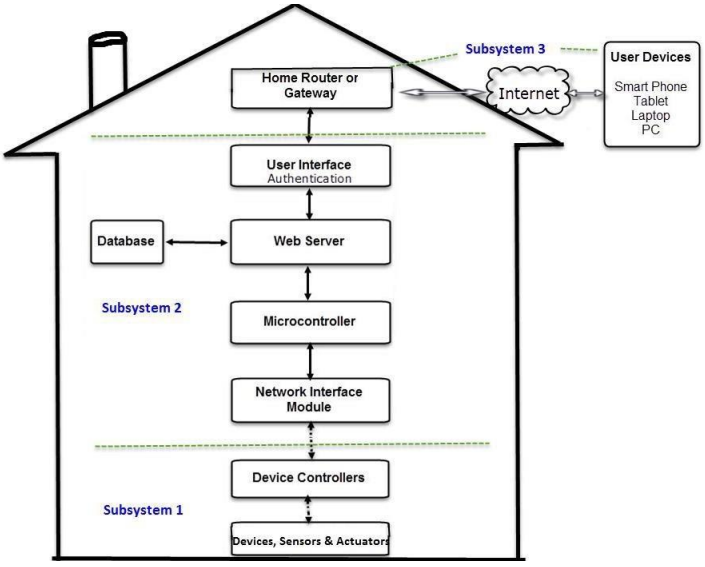

Рисунок 1.6 - Система автоматизації будинку

Для того, щоб точно знати, де в системі розташовані ризики безпеки, дивлячись на рисунок 1.6 стає можливим розділити всю систему на три підсистеми (частини) залежно від того, де відбувається корисна робота: всередині або поза розумним будинком. 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 [24].

Нижче наведені підсистеми системи автоматизації будинку.

- всередині розумного будинку (внутрішня домашня мережа зв'язку):
  - підсистема 1: серед домашніх пристроїв;
  - підсистема 2: між пристроями та домашнім шлюзом;
- поза розумним будинком (зовнішня мережа зв'язку):
  - підсистема 3: між домашніми шлюзами та Інтернетом.

1.8 Архітектура системи

У літературі [27] автори представляють модель архітектури шарів інтелектуальної системи управління будинком, засновану на Інтернеті речей, яка включає рівень сприйняття, мережевий рівень та рівень додатків.

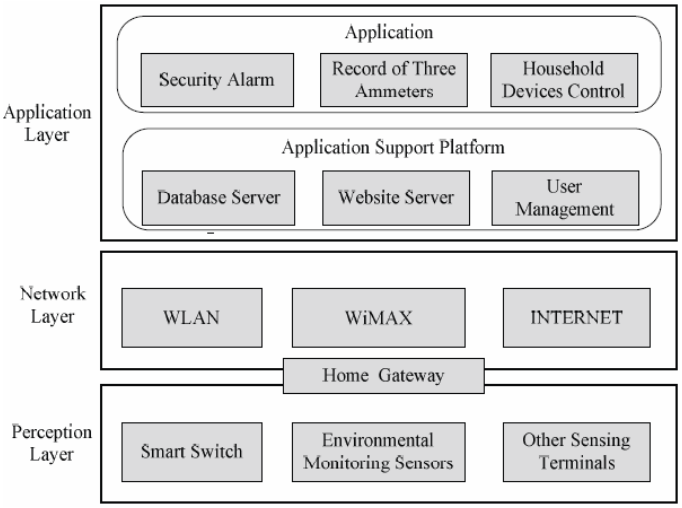

Рисунок 1.7 - Модель архітектури шарів системи керування розумним будинком на основі IoT

В літературі [28] пропонується система розумного будинку на основі IoT та представлена архітектура системи відповідно до багатошарової архітектури Інтернету речей. Система розділена на три шари; сенсорний і виконавчий рівень, мережевий рівень та рівень додатків.

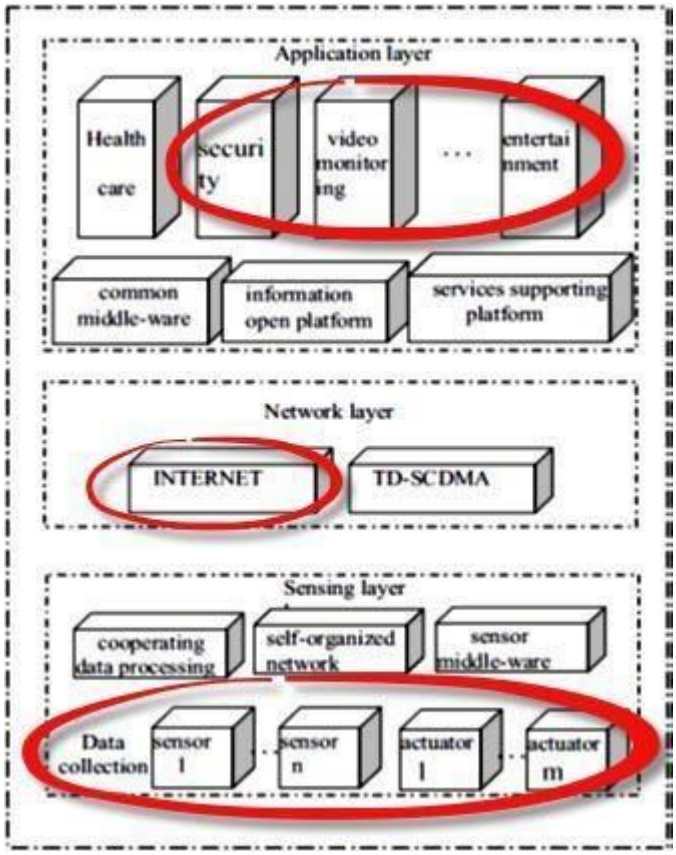

Рисунок 1.8 - Архітектура системи розумного будинку на основі IoT

Розумний дім - основний компонент Інтелектуального житлового кварталу. Коли концепція технології IoT проектується ще до реалізації розумного будинку, традиційний розумний дім набуває нових барв [29]. Він починає охоплювати набагато ширший діапазон контролю за життєзабезпеченням людини. 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 малюнку 1.8, і на малюнку 1.9 показані різні шари та різні області. Але в цій роботі увага приділялась до областей, які виділені червоним кольором.

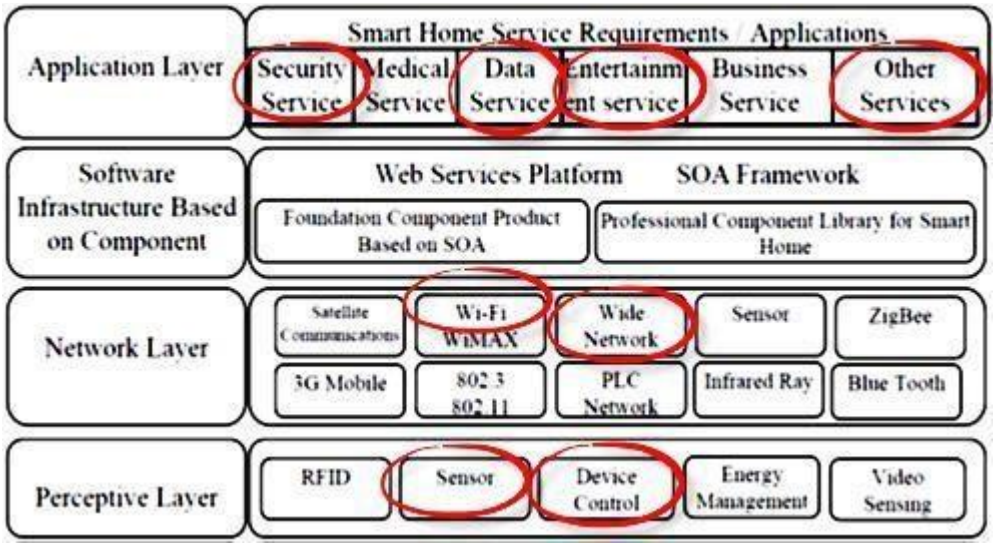

Рисунок 1.9 - Архітектура програми для розумного будинку на основі IoT та компонентних технологій

Коротко кажучи, рівень сприйняття складається з різних типів модулів збору та управління. Основна його функція - сприйняття та збір інформації. Основна робота рівню програмного застосунку полягає в обробці даних.

1.9 Огляд літератури

Мета цього підрозділу - підтвердити наукове значення роботи, показавши попередні дослідження в даній області та обґрунтувати їх необхідність.

Публікації, що писалися протягом останнього десятиліття з 2010 по 2020 рік, були знайдені за допомогою пошуку в Google. Використовуваними термінами пошуку були „проблеми безпеки в розумних будинках”, „розумне середовище”, „розумний будинок”, „інтелектуальні будинки”, та „системи домашньої автоматизації”, що призвело до вибору понад 100 різних джерел. Джерела відфільтровано, і обрано найбільш актуальні джерела.

У цьому підрозділі насамперед представлено попередні роботи про безпеку в розумних будинках на базі IoT.

Цей підрозділ описує різні питання з безпеки, що стосуються системи розумного будинку відповідно до рис. 1.9 та ключових понять, описаних у попередньому розділі: пристроїв, датчиків, виконавчих механізмів, мережи управління, контролерів, пристроїв дистанційного керування, а також використовуваних технологій та архітектур.

Побутову техніку можна підключити до дротової або бездротової мережі через домашній шлюз. 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 якоїсь з вразливостей.

Атака на домашній шлюз може безпосередньо призвести до нападу на всю мережу дому, оскільки це точка, яка з'єднує дім із зовнішнім світом [25].

Типами вразливих місць безпеки можуть бути злом домашнього пристрою, вірусна атака, витік інформації та порушення конфіденційності [25].

Існують різні способи проникнення в розумний дім. Оскільки багато пристроїв підключені до Інтернету, злочинець може напасти на найменш захищений з них і використати його для проникнення в систему. Інша можливість - зараження комп’ютерів або мобільних пристроїв шкідливим програмним забезпеченням і їх подальше використання для проникнення в мережу. Залежно від намірів зловмисника інтерес представляють різні групи пристроїв Smart Home. Перші широкомасштабні атаки, найімовірніше, будуть націлені на продукти групи контрольних систем.

Автори в літературі [31] роблять висновок, що хакер має дві різні можливості для отримання доступу до функцій управління, а саме мережеві атаки та атаки на пристрої. Під час мережевих атак хакер може спробувати перехопити, маніпулювати, сфабрикувати або перервати передані дані. Атаки на пристрої можна класифікувати на атаки на програмне забезпечення та

фізичні атаки. Крім того, існує можливість того, що зловмисник може замаскуватися під внутрішнього користувача [25].

Бездротові датчики стали дуже розповсюдженими пристроями для моніторингу та відстеження рухомих об'єктів розумного будинку, і тому вони стали ціллю для різних атак.

Існують різні атаки на бездротову сенсорну мережу [34]:

- відтворення та вибіркове пересилання даних;
- мережева маршрутизація;
- ідентифікація / автентифікація вузлів (підслуховування, видавання себе за інших).

У літературі [35] описуються типи атак WSN та система виявлення вторгнень для запобігання цим типам атак. Автори описують кібератаки, що відбуваються в бездротових мережах, а саме атаки відмови в обслуговуванні (DoS) та вибіркове пересилання даних.

На малюнку 1.10 зображені потенційні загрози в системі BAS. Атака може бути на трафік контрольної або магістральної мережі, або безпосередньо на пристрій взаємозв'язку (наприклад, шлюз) або інший пристрій з використанням його мережевого або локального інтерфейсу зв'язку [21].

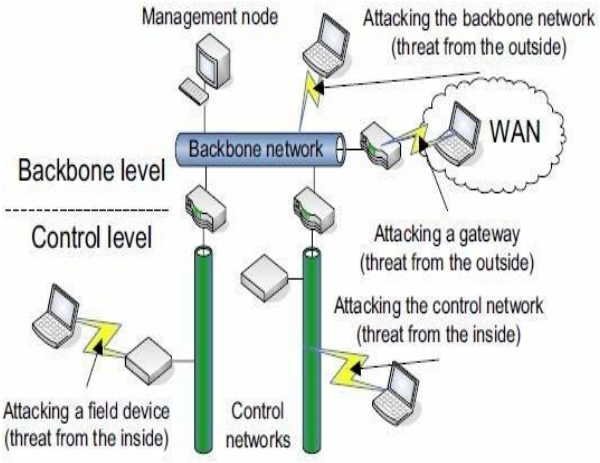

Рисунок 1.10 - Дворівнева модель та загрози безпеки

Хакери можуть спробувати маніпулювати (перехоплювати, модифікувати, фабрикувати або переривати) трафік в мережі [21].

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

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

1. підслуховування;
2. відмова в обслуговуванні (DoS);
3. викрадення даних;
4. Sinkhole та Wormhole атаки.

У літературі [40] представлена модель безпеки для захисту інформаційного потоку в межах домашньої мережі. Запропонована модель здатна ефективно управляти потоком інформації в домашній мережі, використовуючи відсутність конфіденційної інформації.

Peter H. представив швидку вбудовану систему розпізнавання обличчя для додатків розумного будинку. Система вбудована в домашнє мережеве середовище та забезпечує автоматичну ідентифікації користувачів [42].

Зв'язок між мережевим обладнанням та віддаленим пристроєм може бути легко порушена, якщо не вжити заходів безпеки. Для забезпечення автентифікації та цілісності повідомлень автори однієї з статей [39] пропонують модель захисту середовища розумного будинку за допомогою моделі, що включає потужний симетричний блок-шифр із низьким енергоспоживанням: AES256, та обмін ключами для полегшення управління.

Висновки за розділом 1

Проводячи огляд літератури, стає зрозуміло, що більшість з наведених статей про розумні будинки головним чином зосереджуються на можливих проблемах безпеки, які можуть трапитися з системою. Багато потенційних проблем в безпеці повторюються різними авторами в різні роки, і лише деякі з них відрізняються. Дивлячись на малюнок 1.6, не було знайдено жодного прикладку, який би охоплював всю архітектуру розумних будинків починаючи від будинку до віддаленого сервера. Дослідження зосереджуються лише на деяких частинах системи, і в цій роботі була покрита ця прогалину у дослідженні шляхом проведення комплексної оцінки ризику безпеки для всієї системи.

Окрім того, у цих роботах відсутні відповідні можливі рішення чи контрзаходи щодо кожної знайденої загрози.

Ризик безпеки в розумному будинку заключається в тому, що існує можливість заподіяння шкоди або виникнення втрат в результаті таких дій, як небажані дії людей чи виникнення природних катаклізмів. Ці ризики потрібно усунути, застосовуючи засоби контролю, щоб протистояти загрозам та мінімізувати їх вплив.

Надзвичайно важливим є захист системи будинку від зловмисників, які намагаються отримати контроль над системою. Для різних типів інтелектуальних приладів існують різні типи загроз в безпеці, які необхідно вирішити, щоб можна було ними безпечно користуватися.

Посилаючись на роботи відомих фахівців, акцент робився на виборі питань безпеки, та спробі дати їх адекватне резюме. Огляд літератури допоміг визначити проблеми безпеки в системі будинку, які потребують вирішення. Потім було коротко описано ризики безпеки в розумному будинку, що потрібно вирішити та пом'якшити заради безпеки користувачів.

У наступних розділах поданої роботи будуть знайдені відповіді на такі питання:

1. Які загрози безпеці виникають у розумних будинках на базі IoT?
2. Які наслідки цих загроз?
3. Чи є до них відповідні заходи протидії?
4. Що потрібно рекомендувати користувачам?

РОЗДІЛ 2
ВИБІР МЕТОДОЛОГІЇ ДОСЛІДЖЕННЯ

2.1 Оптимальна методологія дослідження

Для того, щоб мати можливість відповісти на вищезазначені питання дослідження, необхідно вибрати відповідну методологію дослідження. Оптимальна методологія для цього дослідницького проекту - це OCTAVE Allegro. Підхід OCTAVE Allegro спрямований на забезпечення надійності результатів та дозволяє комплексно оцінити ризики, зосереджуючись головним чином на інформаційних активах. Підхід аналізує, як інформація використовується користувачами або системами. Крім того, він зосереджується на місці, де інформація зберігається, і на тому, чи існують ризики пов'язані з нею. Критично важливі активи можна визначити та оцінити, виявивши зв’язок між ними та інформаційним активом. OCTAVE Allegro надає вказівки, робочі листи та анкети для проведення оцінки ризику.

OCTAVE Allegro добре підходить для відповіді на дослідницькі питання, оскільки вона має вісім кроків, які можна відобразити для вирішення проблем дослідження. Можна згрупувати кроки методології (вісім етапів) на чотири фази, як показано нижче на малюнку 2.1 [24].

Компонування етапів методології у 4 етапи для вирішення проблем дослідження

Етапи OCTAVE Allegro [15]:

1. встановлення критеріїв вимірювання ризику;
2. розробка профілю активів інформації;
3. визначення контейнерів для інформації;
4. визначення питанн, що викликають занепокоєння;
5. визначення сценаріїв загрози;

6. визначення ризики;
7. аналіз ризиків;
8. вибір підходу пом’якшення наслідків.

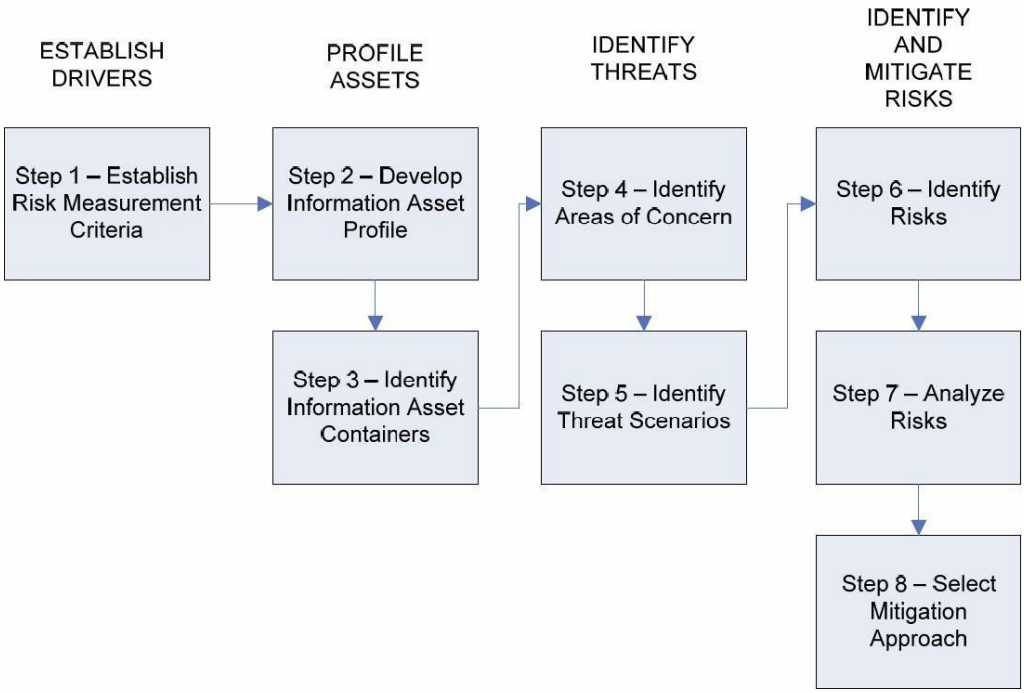

Рисунок 2.1 - OCTAVE Allegro [24]

Фаза 1:

На цьому етапі (Крок 1) була створена основна робота для оцінки ризику інформаційних активів, розробляючи набір критеріїв оцінки ризику для розумного будинку. Ці критерії дозволяють нам 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. Наприклад, сфери впливу можуть включати охорону здоров’я та безпеку користувачів, фінанси, репутацію, закони та нормативні акти тощо. Отже, потрібно описати ці критерії в кількох сферах впливу, а

потім ставимо їх пріоритетами від найважливіших до найменш важливих. Найважливіша категорія отримує найвищий бал (5), а найменш важлива - найнижчий (1).

Фаза 2:

На цьому етапі (Крок 2 та Крок 3) потрібно спочатку визначити критично важливі інформаційні ресурси. У процесі профілювання будуть встановлені 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 SHAS, як відбувається доступ до активів та хто відповідає за активи. Було задокументовано логічні, технічні, фізичні та людські активи. Таким чином, стає можливим визначити точки, в яких вимоги безпеки інформаційного активу порушуються.

Фаза 3:

На етапі 3 (кроки 4 та 5) увага приділялась виявленню загроз відповідно до кожного з ідентифікованих активів у контексті місць, де інформаційний актив зберігається, транспортується або обробляється.

Області, що викликають занепокоєння (вразливості), охоплюються та розширюються у сценарії загрози, що додатково деталізують властивості загрози. Далі буде визначено конкретні загрози, які можуть негативно вплинути на безпеку активу.

Заключний етап (Визначення та пом'якшення ризиків):

У кінці (Крок 6, Крок 7 і Крок 8), визначаються ризики для інформаційних активів, визначаючи, як сценарії загрози можуть вплинути на розумний дім, та аналізуємо їх.

Нарешті, після цього кроку визначається стратегія зменшення наслідків для кожного з виявлених ризиків.

Загроза + Вплив = Ризик

Проаналізуємо ризики та присвоїмо якісне значення для опису ступеня впливу на зацікавлені сторони SH, коли реалізується сценарій загрози та наслідки впливу (оцінка ризиків). Значення впливу визначається критеріями оцінки ризику. Буде використано оцінки для визначення пріоритетів заходів щодо пом'якшення наслідків.

Потім починається процес сортування виявлених ризиків за їх оцінками. Далі ризики класифікуються та призначається підхід до пом'якшення для кожного з них. Потім, розробляється стратегія зменшення наслідків для всіх ризиків, які було вирішено зменшити.

2.2 Критерії вибору методології

Виконуючи оцінку ризику безпеки, важливо знати, що потрібно захищати і навіщо. Очевидно, що захист інформаційних активів є необхідною складовою захисту безпеки розумного будинку, оскільки він визначає майбутній успіх системи розумного будинку.

Ось чому в цій роботі увага приділялась тому, щоб головним чином зосередитись на безпеці інформаційних активів і на тому, де ця інформація зберігається, проводячи оцінку ризику безпеки в розумному будинку. OCTAVE Allegro - це підходяща методологія для оцінки інформаційних активів, оскільки вона забезпечує найкращий опис для досягнення цілей, та відповіді на поставлені дослідницькі запитання:

1. Які загрози безпеці виникають у Smart Homes на базі IoT?
2. Який вплив цих загроз?
3. Чи можна запропонувати відповідні контрзаходи?
4. Що рекомендувати користувачам?

У наступних розділах буде проведена оцінка ризику безпеки для розумного будинку на основі IoT із використанням підходу OCTAVE Allegro.

Будуть виявлені критично важливі інформаційні ресурси для розумного будинку, а також його вразливі місця та можливі загрози. В результаті буде запропоновано план зменшення ризиків.

Висновки за розділом 2

OCTAVE Allegro найкраще підходить для вирішення проблем дослідження порівняно з іншими методологіями оцінки ризику безпеки [30]. Вона складається з восьми етапів, які організовані у чотири фази. За допомогою робочих листів, передбачених методологією, стає можливим охарактеризувати результати кожного кроку в оцінці ризику та використати результати для оцінки наступних кроків. Таким чином, це дозволяє оцінювати актив поетапно та легше досліджувати проблемні ситуації.

РОЗДІЛ 3
ПРОЦЕС ОЦІНКИ РИЗИКУ БЕЗПЕКИ СИСТЕМИ РОЗУМНОГО БУДИНКУ

3.1 Оцінка ризику безпеки

Перш ніж почати застосовувати процеси з методології оцінки ризику безпеки, спершу потрібно визначити саму оцінку ризику безпеки, а також усі терміни, які будуть використані в процесі проведення оцінки ризику безпеки.

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

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

3.2 Що таке оцінка ризику безпеки?

Існує багато визначень терміну оцінка ризику безпеки. Відповідно до “Посібника з управління ризиками” NIST [45], Оцінку ризиків безпеки можна визначити як процес виявлення загроз, ймовірності виникнення, наслідків, та механізмів захисту для їх пом’якшення.

Оцінка ризику є найважливішим аспектом будь-якого процесу дослідження безпеки. За допомогою всебічного вивчення та оцінки ризику можна визначити заходи щодо пом’якшення наслідків. Без оцінки ризиків впроваджені рішення безпеки ризикують не відповідати бажаним цілям безпеки системи розумного будинку. Це допомагає кінцевим користувачам прийняти правильне рішення щодо своїх розумних будинків, а також дає змогу робити рекомендації щодо вдосконалення.

3.3 Перелік визначень

Ось деякі визначення цих термінів, які будуть використані в рамках процесу оцінки ризику безпеки на робочих листах даної методології [44].

Актив - Цінний 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 інформаційних активів - Контейнером інформаційного активу є місце, де зберігається інформація. Контейнери можуть бути технічними (програмне забезпечення, сервери та мережі), фізичними (на паперах, компакт-дисках, DVD-дисках) або людьми.

Критично важливий інформаційний актив: Найважливіший актив, який може завдати величезної шкоди організації, якщо вимоги до його безпеки були порушені.

Загроза - Подія, яка може завдати шкоди активу або поставити його під загрозу. Загроза стає ймовірною коли ініціатор загрози використовує вразливість.

Вплив - Матеріальний або нематеріальний вплив загрози на актив.

Ризик - Це поєднання загрози та впливу. Ризик - це можливість заподіяння шкоди або збитків.

Пом'якшення - Дія, направлена на зменшення ризиків або зменшення ризику організацій за допомогою різних заходів.

3.4 Вимоги безпеки до активів інформаційної безпеки

Кожен захищений інформаційний ресурс повинен бути наділений такими якостями: конфіденційністю, цілісністю та доступністю.

Крім того, вимога з підвищення безпеки є основним елементом щодо розробки та реалізації планів з 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. Тому надзвичайно важливо зберігати конфіденційність, цілісність та доступність інформації.

Конфіденційність - це гарантування того, що доступ до інформаційного активу мають лише уповноважені особи.

Цілісність – це гарантування того, що інформаційний актив залишається у передбачуваному стані. Це гарантує, що інформація залишається достовірною і точною.

Доступність – це гарантування того, що інформаційний актив залишатиметься доступним для уповноважених осіб.

Основною складовою методології OCTAVE Allegro є інформаційні активи. Усі 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 нею. Подібно до розумного будинку, критично важливі інформаційні ресурси повинні бути захищені, інакше це призведе до фатальних не передбачуваних результатів. Тому повинно чітко розуміти, що потрібно захистити і чому, перш ніж вибирати конкретні рішення.

Як зазначено раніше у розділах, методологія буде застосована лише для огляду інформаційної безпеки в контексті розумного будинку, і на основі огляду літератури, проведеного раніше, було з'ясовано, що існує необхідність проведення комплексної оцінки безпеки, яка охоплює та розглядає структуру розумного будинку та висвітлює ризики безпеки, у всіх підсистемах системи автоматизації розумного будинку (SHAS) як всередині будівлі, так і за її межами, як показано на малюнку 2.1, а саме:

- Всередині розумного будинку (внутрішня домашня мережа зв'язку):
    - підсистема 1: Серед домашніх пристроїв;
    - підсистема 2: між пристроями та домашнім шлюзом.
- Поза межами розумного будинка (зовнішня мережа зв'язку):
    - підсистема 3: між домашніми шлюзами та Інтернетом.

Під час оцінки ризику безпеки було розглянуто рисунок 2.1 і були відібрані ризики, пов’язаніз усіма підсистемами або всіма частинами системи автоматизованого розумного будинку. Варто згадати, що в розумному будинку існує основна система, яка підключена до всіх інших пристроїв. Це означає, що якщо хакер отримує доступ до основної системи, він може отримати доступ до всіх інших пристроїв.

Можна зазначити, що безпека може бути порівняна з ланцюгом, і система є настільки ж безпечною, як і її найслабша ланка. Зловмисники атакують найслабші частини системи. З незахищеної частини або незахищеного пристрою зловмисник отримує доступ до всіх інших пристроїв.

При проведенні оцінки ризику слід враховувати всі деталі [37]:

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 збирати дані, а вбудовані в виконавчі механізми виконувати команди.

Також є контролер пристроїв, який підключений до декількох з них, і він складається з інтерфейсного модуля, модуля бездротового зв'язку та мікроконтролера що контролює роботу.

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, що була

розроблена для певної платформи, яка підключається до бази даних через веб-сервер [31].

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, ввівши правильні облікові дані користувача (ім'я користувача та пароль).

Мікроконтролер - це мозок, який управляє всіма операціями та комунікаціями в мережі розумного будинку. Модуль мережевого інтерфейсу відповідає за зв'язок між контролерами домашніх пристроїв та системою, що складається з мікроконтролера, веб-сервера, користувацького інтерфейсу та бази даних.

Підсистема 3:

У підсистемі 3 є домашній маршрутизатор (домашній шлюз), інтернет та пристрої користувачів, такі як ПК, ноутбуки, смартфони та планшети.

Домашній маршрутизатор підключає систему розумного дому до Інтернету. Отже користувачі, що знають правильні облікові дані можуть підключати та керувати своїм розумним будинком віддалено з будь-якого місця за допомогою своїх смартфонів.

3.5 Визначення критично важливих інформаційних ресурсів

Перш за все, потрібно знати, що означає інформаційний актив та його критичність (див. визначення у розділі 3.2), а потім для проведення оцінки ризику нам потрібно визначити сукупність найважливіших (критичних) інформаційних активів, для яких будуть оцінені ризики безпеки. Далі наведемо перелік критично важливих інформаційних ресурсів в SHAS [31].

Очікується, що наступні інформаційні ресурси стануть головними об'єктами зловмисної атаки:

1. інформація, зібрана пристроями (датчиками) / Інформація про стан розумного будинку [Підсистема 1];

2. відеопоток камери спостереження [Підсистема 1];

3. повноваження користувача (ім’я користувача та пароль) [Підсистема 2];

4. інформаційні ресурси (картинки, документи) [Підсистема 1, 2];

5. інформація про налаштування будинку [Підсистема 1, 2];

6. інтелектуальна структура будинку [Підсистема 1, 2];

7. інформація (дані), що передаються через домашній шлюз [Підсистема 3];

8. мобільний пристрій користувача [Підсистема 3];

9. інформація про відстеження місцезнаходження користувача [Підсистема 3].

Нижче інформація представлена у вигляді підсистем системи розумного будинку

- Всередині розумного будинку (внутрішня домашня мережа зв'язку):
    - Підсистема 1: Серед домашніх пристроїв (датчики та пускачі):
        - інформація, зібрана пристроями (датчиками) / Інформація про стан розумного будинку;
        - відеопоток камери спостереження.
    - Підсистема 2: між пристроями та домашнім шлюзом:
        - ім’я користувача та пароль;
        - інформаційні ресурси (картинки, документи, музика);
        - інформація про налаштування будинку.
- Поза розумним будинком (зовнішня мережа зв'язку):
    - Підсистема 3: між домашніми шлюзами та Інтернетом:
        - інформація (дані), що передається через домашній шлюз;
        - мобільний пристрій користувача;

- інформація про відстеження місцезнаходження користувача.

3.6 Процес оцінки ризику безпеки

У цьому підрозділі буде проведена оцінка ризику безпеки, відповідно до етапів методології OCTAVE. Для проведення оцінки ризику будуть використані шаблони, надані методологією OCTAVE Allegro (44).

Як вже було зазначено раніше, методологія OCTAVE Allegro передбачає 8 етапів, (дивіться рис. 2.1). За допомогою робочих аркушів, передбачених методологією, можна використати результати кожного з кроків в оцінці ризику для оцінки наступного кроку.

Індивідуальні кроки застосовуються до кожного ідентифікованого інформаційного активу. Нижче кожен крок описаний більш докладно:

3.7 Вибір критеріїв вимірювання ризику

Метою цього кроку є аналіз того які можуть бути ризики для комерційно зацікавлених сторін та для мешканців розумного будинку. Цей етап складається з двох видів діяльності.

По-перше, визначається набір якісних та кількісних заходів для оцінки впливу ризиків на виявлені критично важливі інформаційні активи у розумному домі.

По-друге, розставляються пріоритети відповідно до їх важливості для власника SHAS або зацікавлених сторін.

Категорії критеріїв оцінки OCTAVE Allegro включають [15]:

- репутацію;
- довіру клієнтів;
- життя, здоров’я, безпеку;
- штрафи та юридичні санкції, спричинені недотриманням вимог;

- фінансові критерії;
- критерії продуктивність роботи.

Ми розглянемо їх у відповідних робочих аркушах OCTAVE Allegro (робочі листи 1-7).

Перш ніж заповнювати робочі аркуші, слід знати, хто буде зацікавленими сторонами, коли буде проведена оцінка ризику в системі автоматизованого розумного будинку (SHAS). Зацікавлені сторони в цьому випадку можна поділити 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).

У таблиці 1 описано, наскільки зміни в репутації та довіри клієнтів вплине на зацікавлені сторони розумного будинку (як комерційні, так і некомерційні) у трьох критеріях: низький, помірний та високий.

Примітка: Усі таблиці - це робочі аркуші, які надає методологія OCTAVE Allegro, за винятком таблиці 4.1, яка є таблицею результатів.

Таблиця 3.1

Критерії вимірювання ризику - репутація та довіра споживачів

Робочий лист Allegro 1	**КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКУ - РЕПУТАЦІЯ ТА ДОВІРА КЛІЄНТА**		
Область впливу	**Низька**	**Помірна**	**Висока**
Репутація *(Некомерційні зацікавлені сторони)*	На репутацію некомерційних зацікавлених сторін впливає мінімально, а для відновлення не потрібно майже ніяких зусиль чи витрат.	Репутація некомерційних зацікавлених сторін пошкоджена. Необхідно менше 10 тис. доларів США для відновлення	Репутація некомерційних зацікавлених сторін безповоротно знищується або пошкоджується. Більше $ 10 тис. доларів необхідно

			для відновлення.
Репутація *(Комерційні зацікавлені сторони)*	На репутацію комерційних зацікавлених сторін впливає мінімально, а для відновлення вимагаються незначні зусилля чи витрати.	Репутація комерційних зацікавлених сторін пошкоджена, і для відновлення потрібно менше 100 тис. доларів	Репутація комерційних зацікавлених сторін безповоротно знищується або пошкоджується. Більше $ 100 тис. доларів необхідно для відновлення.
Втрата клієнтів *(Комерційні зацікавлені сторони)*	Впасти менше 5% від кількості клієнтів в результаті втрати довіри.	Зменшення споживачів на 5–10% через втрату довіри.	Більше 10% скорочення споживачів через втрату довіри.

У таблиці 3.2 наведено критерії для сфери фінансового впливу. Далі будуть розраховані операційні та матеріальні витрати для некомерційних зацікавлених сторін, втрату доходів для комерційних зацікавлених сторін (продавців, постачальників ПЗ, і т. д.) і одноразові фінансові втрати кінцевих користувачів. Представимо це з різними процентними і грошовими показниками в трьох шкалах.

Таблиця 3.2

Критерії оцінки ризиків - фінансові

Робочий лист Allegro 2	**КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКУ - ФІНАНСОВІ**		
Вплив	**низький**	**помірний**	**високий**
Операційні і матеріальні витрати *(Некомерційнийзацік*	Збільшення річних експлуатаційних витрат менш ніж на 2%.	Щорічні експлуатаційні витрати збільшуються на 2-	Щорічні експлуатаційні витрати збільшуються більш

авлені сторони: жителі)		5%.	ніж на 5%.
втрата доходу *(Комерційні зацікавлені сторони)*	Втрата доходу менше 5% на рік	Від 5 до 10% щорічної втрати доходу	Втрата річного доходу понад 10%
Фінансові втрати *(Некомерційнийзацік авлені сторони: жителі)*	Одноразові фінансові витрати менше 10 тис. Доларів США	Одноразові фінансові витрати від 10 до 25 тисяч доларів	Одноразові фінансові витрати більше 25 тисяч доларів

У таблиці 3.3 наведено критерії для області впливу на продуктивність. Потрібно розрахувати втрату продуктивності для комерційних зацікавлених сторін.

Таблиця 3.3

Критерії вимірювання ризиків - продуктивність

Робочий лист Allegro 3	**КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКУ - ПРОДУКТИВНІСТЬ**		
Вплив	**низький**	**помірний**	**високий**
Години роботи персоналу*(Комерційні зацікавлені сторони)*	Години роботи персоналу збільшують витрати на робочу силу менш ніж на 50 тисяч доларів.	Години роботи персоналу збільшують витрати на робочу силу між 50 тисячами і 100 тисячами доларів.	Години роботи персоналу збільшують витрати на робочу силу більш ніж на 100 тисяч доларів.

У таблиці 3.4 показані критерії для області впливу на безпеку і здоров'я. Потрібно розглянути аспекти людського життя, наприклад, здоров'я і безпеку кінцевих користувачів розумного будинку (некомерційні зацікавлені

сторони), і продемонструємо їх за допомогою значень, представлених в трьох шкалах.

Таблиця 3.4

Критерії вимірювання ризику - безпека і здоров'я

Робочий лист Allegro 4		**КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКУ - БЕЗПЕКА І ЗДОРОВ'Я**	
Вплив	**низький**	**помірний**	**високий**
Життя *(Некомерційний зацікавлені сторони: жителі)*	Ніяких втрат або значної загрози для життя кінцевих користувачів. Немає відповіді від регулюючих органів.	Життя користувачів знаходиться під загрозою, але, отримавши медичну допомогу, вони одужають.	Загибель користувачів.
Здоров'я *(Некомерційнийзацік авлені сторони: жителі)*	Мінімальні втрати, Здоров'я відновлюється протягом декількох днів.	Тимчасове погіршення здоров'я користувачів.	Сильне погіршення здоров'я користувачів.
Безпека *(Некомерційнийзацік авлені сторони: жителі)*	Безпека кінцевого користувача поставлена під сумнів, але відповіді з боку регулюючих органів немає.	Порушено безпеку кінцевого користувача.	Безпека кінцевого користувача порушена. Значна відповідь регуляторних органів, що включає розслідування

У таблиці 3.5 показані критерії оцінки ризику - штрафи і судові санкції. Потрібно розглянути штрафи, судові позови і розслідування проти комерційних зацікавлен их сторін, якщо в них виникне якесь лихо.

Таблиця 3.5

Критерії оцінки ризику - штрафи і судові санкції

Робочий лист Allegro 5	**КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКУ - ШТРАФИ І ЮРИДИЧНІ ПОКАРАННЯ**		
Вплив	**низький**	**помірний**	**високий**
Штрафи *(Комерційний зацікавлені сторони)*	Накладаються штрафи менше 100 тисяч доларів.	Стягуються штрафи від 100 до 250 тисяч доларів.	Штрафи більш ніж 250 тисяч доларів.
Судові позови*(Комерційні зацікавлені сторони)*	Ніяких судових позовів або судові позови на суму менше 100 тисяч доларів.	Ніяких судових процесів або судові процесів на суму від 100 тис. До 500 000 тис. доларів.	Ніяких судових позовів або судові позови на суму понад 500 тисяч доларів проти комерційних зацікавлених сторін.
Розслідування *(Комерційні зацікавлені сторони)*	Ніяких запитів від уряду або інших слідчих організацій	Запит на отримання інформації від уряду або інший слідчої організації.	Уряд або інші слідчі органи ініціюють поглиблене розслідування щодо постачальників.

Таблиця 3.6 дає нам можливість визначити додаткові області впливу, відмінні від запропонованих методологією OCTAVE Allegro. Однак будь-які додаткові зони впливу не будуть розглянуті, тому цей робочий лист залишиться порожнім.

Таблиця 3.6

Критерії вимірювання ризику - визначаються користувачем

Робочий лист Allegro 6	**КРИТЕРІЇ ВИМІРЮВАННЯ РИЗИКУ - ВИЗНАЧЕННЯ КОРИСТУВАЧА**		
Вплив	**низький**	**помірний**	**високий**
/	/	/	/

Описавши вищезгадані критерії вимірювання ризику, була закладена основа для оцінки ризиків інформаційних активів. Як вже було згадано раніше, ці критерії допомагають виміряти ступінь впливу на розумний будинок, якщо реалізується ризик для інформаційного активу.

Тепер був створений набір критеріїв виміру ризику, що відображають різні області впливу, які життєво важливі для зацікавлених сторін SHAS, як комерційних, так і некомерційних зацікавлених сторін.

Області впливу включали репутацію і довіру клієнтів, фінанси, продуктивність, безпеку і здоров'я користувачів і, нарешті, штрафи і судові санкції. Потім потрібно зробити ранжування і розставити пріоритети, а також визначити значення від найбільш важливих до найменш важливих, тому що потрібно розуміти, які галузі впливу в пріоритеті.

Буде використано ранжування і розстановка пріоритетів пізніше при оцінці ризиків, і це допоможе розробити відносну оцінку ризику, яка визначає те, як боротися з ризиками, які будуть визначені при оцінці. Найважливіша категорія отримує найвищий бал (5), а найменш важлива - найнижча (1), як показано в таблиці 3.7.

Таблиця 3.7

Пріоритезація областей впливу

Робочий лист Allegro 7	**РОБОЧИЙ ЛИСТ ПРО ПРІОРИТИЗАЦІЮ ВПЛИВУ**
ПРІОРИТЕТ	**ОБЛАСТІ ДІЇ**
4	Репутація і довіра клієнтів
3	Фінанси
2	Продуктивність
5	Безпека і здоров'я
1	Штрафи та правові санкції
0 (немає даних)	Визначені користувачем

3.7.1 Розробка профілю інформаційних активів

На цьому етапі будуть описані інформаційні активи, які визначені як критичні. В процесі профілювання встановлюються чіткі межі для активу, визначаються його вимоги до безпеки, а потім визначаються всі місця, де актив зберігається, транспортується або обробляється.

Це дозволить повністю виявити всі вразливі місця інформаційних активів. За заявленими критеріям в подальшому оцінюються і аналізуються профільовані активи.

Щоб зробити актив менш складним, продовжується процес оцінки ризиків для кожного з них і починається розгляд підсистеми, щоб прояснити, де ризики знаходяться всередині або зовні в системі розумного будинку.

Далі повторюються всі кроки (від кроку 2 до кроку 8) для кожного ідентифікованого інформаційного активу.

- Усередині розумного будинку (внутрішня домашня комунікаційна мережа):
    - Підсистема 1: Серед домашніх пристроїв (датчики і виконавчі механізми):
        - інформація, що збирається пристроями;
        - відеопотік камери спостереження.

Усередині розумного будинку є два вищевказаних інформаційних активи.

У таблиці 3.8 буде охарактеризована критично важлива інформація, яка збирається пристроями.

Таблиця 3.8

Профіль критично важливих інформаційних ресурсів (інформація, яку збирають пристроями (датчиками) / інформація про стан розумного будинку)

Робочий лист Allegro 8	**КРИТИЧНА ІНФОРМАЦІЯ**	
(1) Критичний актив *Що є важливим інформаційним активом?*	**(2) Обгрунтування вибору** *Чому цей інформаційний актив важливий для організації?*	**(3) Опис** О*пис цього інформаційного активу*
Інформація, що збирається пристроями (датчиками) / інформація про статус розумного будинку	Ці інформаційні активи дуже важливі, тому що вони використовуються в повсякденних робочих процесах і операціях системи розумного будинку. Актив показує поточний стан розумного будинку. Дані датчиків можуть використовуватися, наприклад, для виявлення таких ризиків, як повінь або пожежа,	Цей інформаційний ресурс визначає звідки передається інформація з пристроїв, наприклад, він визначає, які дії будуть виконуватися виконавчими механізмами. Ця інформація визначає безпеку і зручність розумного будинку. Якщо його безпека була порушена, це значно порушить здатність SHAS досягати своїх цілей.
(4) Власник (и)		

Власник системи автоматизації розумного будинку (SHAS), який несе основну відповідальність за цей інформаційний актив.		
(5) Вимоги безпеки		
☐ **Конфіденційність**	Тільки користувач з достатній рівнем привілей може переглядати цей інформаційний актив	Тільки жителі мають право доступу до цього інформаційного активу. Постачальникам послуг також може знадобитися доступ до цього інформаційного активу для надання потрібного сервісу відповідно до договорів.
☐ **чесність**	Лише користувач з достатній рівнем привілей може змінювати цей інформаційний ресурс	Тільки жителі мають право маніпулювати цим інформаційним активом.
☐ **доступність**	Цей актив повинен бути доступек персоналу для виконання своєї роботи	Актив повинен бути готовий до використання щоразу, коли в ньому потребують жителі або інші пов'язані підсистеми будинку.

(6) Найважливіша вимога безпеки *Яка найважливіша вимога безпеки для цього інформаційного активу?*			
☒ Конфіденційність	☒ Чесність	☒Наявність	☐ інша

3.7.2 Визначення контейнерів інформаційних активів

Контейнер інформаційного активу - це місце, де зберігається інформація [32]. Контейнери можуть бути технічними (програмне забезпечення, обладнання, сервери і мережі), фізичними (інформація на папері, компакт-дисках, DVD) або людьми. Вони також можуть бути як внутрішніми, так і зовнішніми по відношенню до організації.

Таблиця 3.9

Карта середовища технічного ризику інформаційних активів для інформації, яка збирається пристроями та датчиками / інформація про стан розумного будинку

Робочий лист Allegro 9a	**КАРТА РИЗИКІВ ТЕХНІЧНИХ ІНФОРМАЦІЙНИХ АКТИВІВ**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. файл даних	Власник
2.База даних: інформаційний актив знаходиться на серверах бази даних	Власник
3.Внутрішня мережа розумного будинку. Вся інформація переміщається по цій мережі.	Власник
4.ПК (робочі станції)	Мешканці будинку
ЗОВНІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1.Інтернет: ці інформаційні ресурси переміщаються в мережі Інтернет кожен раз, коли кінцевий користувач підключається до SHAS ззовні через призначені для користувача пристрої, такі як ПК, смартфон, планшет і т. д.	Мешканці будинку

Таблиця 3.10

Карта середовища фізичного ризику інформаційних активів для інформації, яка збирається пристроями та датчиками / інформація про стан розумного будинку

Робочий лист Allegro 9b	**КАРТА РИЗИКІВ ФІЗИЧНИХ ІНФОРМАЦІЙНИХ АКТИВІВ**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. паперові копії	Мешканці будинку
2. CD, DVD, резервний носій	Мешканці будинку

Таблиця 3.11

Карта середовища людського ризику інформаційних активів для інформації, яка збирається пристроями та датчиками / інформація про стан розумного будинку

Робочий лист Allegro 9c	**КАРТА РИЗИКІВ ЛЮДСЬКИХ ІНФОРМАЦІЙНИХ**
ВНУТРІШНІ КОРИСТУВАЧІ	
ІМ'Я АБО РОЛЬ	**ПІДСИСТЕМА**
1.члени сім'ї	Вся система будинку
ЗОВНІШНІ КОРИСТУВАЧІ	
ПОСТАЧАЛЬНИК	**ПДСИСТЕМА**
1.Гості, Відвідувачі	Вся система будинку
2.Обслуговуючий персонал	Вся система будинку

3.7.3 Визначаємо проблемні області

Мета цього кроку - виявити проблемні області. Для кожного ідентифікованого інформаційного активу визначаються конкретні проблеми, які можуть негативно вплинути на безпеку активу.

На цьому етапі описуюється потенційний вплив у випадку якщо щось сталося. Шляхом опису, заснованого на місцях зберігання інформації, зазначених на кроці 3, буде отримано уявлення про те, де активи піддаються потенційному ризику.

3.7.4 Визначаємо сценарії загроз

На кроці 5 описуються сценарії загроз для кожного ідентифікованого інформаційного активу. Сценарій загрози включає в себе один або декілька активів, дійової особи і список небажаних результатів.

Суб'єкт загрози може бути природним (шторм, повінь, пожежа або інше лихо), автоматизованих (шкідливе ПЗ) або інтелектуальним (злочинець або потенційно небезпечна людина) [27].

Засіб - це вразливість або експлойт, який використовується суб'єктом проти інформаційного активу [28].

Мотив - це бажання злочинця застосувати засоби. Небажаний результат - пошкодження інформаційного активу.

Таким чином, цей крок допомагає нам визначити, які сценарії загроз з більшою ймовірністю можуть статися.

Можна ідентифікувати загрозу через контейнери, в яких зберігаються або передаються активи. Далі робиться припущення про можливі сценарії загроз і їх наслідки

3.7.5 Виявлення ризиків

Ризик - це можливість заподіяння шкоди або збитків, який складається з події та наслідків [29]. Для кожного робочого аркуша ризиків інформаційних активів (робочий лист 10) застосовуються сценарії загроз відповідно до його

активів, припускаючи, що сценарій загрози стався насправді, і оцінюється вплив на зацікавлені сторони розумного будинку.

Було визначено ризики безпеки, які відносяться до різних рівнів інфраструктури розумного будинку, і коротко пояснюємо кожен з ризиків безпеки.

3.7.6 Аналізуємо ризики

На цьому етапі ідентифіковані ризики оцінюються з використанням критеріїв виміру, встановлених на першому етапі. Оцінки використовуються для визначення пріоритетів ризиків що мають бути зниженні.

Для кожного робочого аркуша інформаційних ризиків (робочий лист 10) необхідно виконати наступне [30]:

По-перше переглянути наслідки і присвоєння значень ступеню «високий», «середній» і «низький» в області значень стовпця (8) з урахуванням критеріїв виміру ризиковості (робочі листи 1-6) по мірі виконання.

По-друге, розрахувати бали для кожної області впливу шляхом множення рангу області впливу (таблиця ранжирування областей впливу, робоча таблиця 3.7) на значення впливу (висока = 3, середняі = 2, низька = 1).

Результат записується в стовпець балів, а потім підсумовуємо бали, і ця сума є оцінкою відносного ризику.

3.7.7 Вибір підходу для пом'якшення наслідків

На восьмому кроці оцінки ризику, визначаються дії щодо його зниження. Восьмий і останній крок методології OCTAVE Allegro - вибір підходу для боротьби з кожною з пріоритетних загроз.

Можна вибрати кілька підходів: прийняти, зменшити загрозу або вплив, передати загрозу або відкласти.

Після визначення ризиків і їх оцінки можна визначити план пом'якшення наслідків, щоб уникнути або обмежити виявлені ризики і пов'язані з ними негативні наслідки.

Таблиця 3.12

Ризик інформаційного майна який збирають пристрої

<table>
<tr><td colspan="2">Allegro- Робочий лист 10</td><td colspan="2">РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ</td></tr>
<tr><td rowspan="8">Ризик інформаційних активів</td><td rowspan="8">Загроза</td><td>Інформаційний актив</td><td colspan="2">Інформація, що збирається пристроями (датчиками) / інформація про статус розумного будинку</td></tr>
<tr><td>Область інтересів</td><td colspan="2">1. Інформаційний актив навмисно змінений зловмисниками, через це лічильник напреги показує високе споживання електроенергії. Таким чином, для оплати рахунків потрібно заплатити багато грошей.
2. DoS-атаки на можуть змусити датчики не реагувати на такі ризики, як пожежа, повінь, несподівані рухи і т. д.
3. Компрометацію датчика руху можна використовувати, щоб визначити, чи є люди вдома.
4. Зчитування статусу дверних замків і систем сигналізації можна використовувати для визначення того, коли розумний будинок не захищен від вторгнення.</td></tr>
<tr><td>(1) Дійова особа.</td><td colspan="2">Хакер</td></tr>
<tr><td>(2) Засоби Як би це зробила дійова особа? Що б вона зробили?</td><td colspan="2">Використала б інструменти злому та ідентифікований апаратний дефект</td></tr>
<tr><td>(3) Мотив</td><td colspan="2">Фінансова вигода</td></tr>
<tr><td>(4) Результат</td><td>☐ розкриття
☒модифікація</td><td>☐ Руйнування
☒ переривання</td></tr>
<tr><td>(5) Вимоги безпеки</td><td colspan="2">Тільки авторизовані мешканці будинку повинні мати доступ до цієї інформації і мати можливість маніпулювати нею.</td></tr>
</table>

		(6) Імовірність	☒ Висока	☐**Середня**	☐ **низька**
	(7) Наслідки *Які наслідки для організації або власника інформаційних активів в результаті порушення вимог безпеки?*		(8) *Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?*		
	Якщо вимоги до безпеки цих інформаційних активів будуть порушені, власнику розумного будинку або жителям може бути завдано значних фінансових збитків. Датчики не будуть реєструвати такі ризики, як пожежа, повінь або якись дивний рух всередині розумного будинку. Таким чином, виникають великі фінансові втрати.Якщо хакери дізнаються, що вас немає вдома, вони можуть спланувати проникнення в будинок.		**Область впливу**	**значення**	**оцінка**
			Репутація (4)	Високе (3)	4 * 3 = 12
			Фінанси (3)	Високе (3)	9
			Продуктивність (2)	Низьке (1)	2
			Безпека і здоров'я (5)	Високе (3)	15
			Штрафи(1)	Низьке (1)	1
			Обумовлена користувачем зона впливу (0)	N / A	/
	Оцінка відносного ризику				39
	(9) Зниження ризиків *Які дії ви зробите, виходячи із загальної оцінки цього ризику?*				
	☐ **прийняти**	☐ **відкласти**	☒ пом'якшити	☐ **Передати**	
	Для ризиків, які ви вирішили знизити, виконайте наступні дії:				
	До якого контейнера ви застосували б елементи управління?	*Які адміністративні, технічні та фізичні заходи контролю ви б застосували до цього контейнеру?*			
	Технічні (внутрішні мережі)	Обмежте мережевий трафік так, щоб він був доступен тільки авторизованим користувачам. Використовуйте протоколи захисту зв'язку, такі як SSL DTLS через UDP. Використовуйте багаторівневі заходи безпеки.			

Фізичні елементи	Зберігайте всі фізичні сховища в надійному місці. Регулярно оновлюйте обладнання, резервні копії всієї важливої інформації.
Люди	Регулярно проводьте програми навчання з питань безпеки для жителів, щоб вони знали про ймовірні ризики безпеки.
Інтернет	Використовуйте безпечний канал зв'язку за допомогою VPN з використанням IPsec, SSL або TLS.

Таблиця 3.13

Ризик інформаційного майна для інформації, яку збирають датчики

<table>
<tr><td colspan="2">Робочий лист Allegro 10a</td><td colspan="4">РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ</td></tr>
<tr><td rowspan="9">Ризик інформаційних активів</td><td rowspan="8">Загроза</td><td>Інформаційний актив</td><td colspan="3">Інформація, що збирається пристроями (датчиками) / інформація про статус розумного будинку</td></tr>
<tr><td>Область інтересів</td><td colspan="3">Система розумного будинку вийшла з ладу</td></tr>
<tr><td>(1) Дійова особа.</td><td colspan="3">Хакер</td></tr>
<tr><td>(2) Засоби.</td><td colspan="3">Збої в енергопостачанні</td></tr>
<tr><td>(3) Мотив.</td><td colspan="3">випадковий</td></tr>
<tr><td>(4) Результат.</td><td colspan="3">☐ розкриття ☐ Руйнування
☐ модифікація ☒ переривання</td></tr>
<tr><td>(5) Вимоги безпеки.</td><td colspan="3">Електроживлення повинно бути доступно цілодобово</td></tr>
<tr><td>(6) Імовірність</td><td>☐ висока</td><td>☒ Середня</td><td>☐ низька</td></tr>
<tr><td colspan="2">(7) Наслідки Які наслідки для організації або інформації власник активів в результаті результату і порушення вимог безпеки?</td><td colspan="3">(8) Серйозність. Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?</td></tr>
</table>

<table>
<tr><td></td><td rowspan="7">Якщо сценарій загрози був реалізований, система розумного будинку стає небезпечною для життя, наприклад, двері і вікна не будуть розблоковані.
Система розумного будинку престає працювати належним чином.</td><td>Область впливу</td><td>Значення</td><td>Оцінка</td></tr>
<tr><td>Репутація(4)</td><td>Середнє (2)</td><td>8</td></tr>
<tr><td>Фінанси (3)</td><td>Високе (3)</td><td>9</td></tr>
<tr><td>Продуктивність (2)</td><td>Низьке (1)</td><td>2</td></tr>
<tr><td>Безпека і здоров'я (5)</td><td>Середнє (2)</td><td>10</td></tr>
<tr><td>Штрафи(1)</td><td>Низьке (1)</td><td>1</td></tr>
<tr><td>Обумовлена користувачем зона впливу</td><td>N / A</td><td></td></tr>
<tr><td colspan="3">Оцінка відносного ризику</td><td>30</td></tr>
<tr><td colspan="4">(9) Зниження ризиків Які дії ви зробите, виходячи із загальної оцінки цього ризику?</td></tr>
<tr><td>☐ прийняти</td><td>☐ відкласти</td><td>☒ пом'якшити</td><td>☐ Передати</td></tr>
<tr><td colspan="4">Для ризиків, які ви вирішили знизити, виконайте наступні дії:</td></tr>
<tr><td colspan="2">На якому контейнері ви б примінили контроль?</td><td colspan="2">Які адміністративні, технічні та фізичні заходи контролю ви б застосували до цього контейнеру?</td></tr>
<tr><td colspan="2">фізичний</td><td colspan="2">У вас повинно бути резервне джерело безперебійного живлення (ДБЖ).</td></tr>
<tr><td colspan="2">люди</td><td colspan="2">Переконайтеся, що у вас є програма підвищення обізнаності користувачів, для того щоб вони знали про важливість справності джерела живлення.</td></tr>
</table>

Таблиця 3.14

Профіль критично важливих інформаційних ресурсів (відеопотік з камер спостереження)

Робочий лист Allegro 8	**КРИТИЧНІ ІНФОРМАЦІЙНІ ПРОФІЛІ АКТИВУ**	
(1) Критичний актив.	**(2) Обгрунтування вибору** *Чому важливий цей інформаційний актив для організації?*	**(3) Опис** *Яке Опис цього інформаційного активу*
Відеопотік камер спостереження	Цей інформаційний актив дуже важливий, тому що камери спостереження є частиною системи розумного будинку, а відеопотік камери спостереження використовується, наприклад, для виявлення незвичайних рухів усередині розумного будинку.	Без цього інформаційного ресурсу система розумного будинку (SHAS) буде неповною
(4) Власник		
Власник системи автоматизації розумного будинку (SHAS), який несе відповідальність за цей інформаційний актив.		
(5) Вимоги безпеки		
☐ **Конфіденційність**	Тільки користувач з достатній рівнем привілей може переглядати цей інформаційний актив	Тільки жителі мають право доступу до цього інформаційного активу.
☐ **чесність**	Тільки користувач з достатній рівнем привілей може змінювати цей інформаційний актив таким чином:	Тільки жителі мають право маніпулювати цим інформаційним активом.

☐ **доступність**	Цей актив повинен бути доступний цього персоналу для виконання своєї роботи	Актив повинен бути доступний для використання, коли він потрібен жителям.
	Цей актив повинен бути доступний 24 години, 7 днів на тиждень, 52 тижні на рік.	Ці інформаційні ресурси повинні бути доступні цілодобово. Він повинен бути доступний користувачеві для функціональних цілей. Короткочасні відключення не викликають серйозних проблем. Тривале переривання роботи (більше 8 годин) може викликати серйозні проблеми.
☐ **інша**	До цього активу пред'являються особливі вимоги щодо захисту відповідності нормативним вимогам	/

(6) Найважливіша вимога безпеки			
☒Конфіденційність	☐ чесність	☒ Наявність	☐ інша

Таблиця 3.15

Карта середовища технічного ризику інформаційних активів для відеопотоку з камер спостереження

Робочий лист Allegro 9a	**КАРТА ТЕХНІЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. розумний ТВ, ПК (робочі станції)	Власник
2. База даних: Інформаційний актив в основному знаходиться в базі даних	Власник
3.Домашня внутрішня мережа. Вся інформація переміщається по цій мережі.	Власник
ЗОВНІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**

4. Інтернет	Користувач розумного будинку
5. Смартфони, планшети, ПК	Користувач розумного будинку

Таблиця 3.16

Карта середовища фізичного ризику інформаційних активів для відеопотоку з камер спостереження

Робочий лист Allegro 9b	**КАРТА ФІЗИЧНИХРИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1.Камери можуть записувати події і зберігати їх на носіях і надіслати копію в базу даних будинка.	жителі
2. DVD, відеокасети	жителі
ЗОВНІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
Резервні носії, які зберігаються за межами розумного будинку	жителі

Таблиця 3.17

Карта середовища людського ризику інформаційних активів для відеопотоку з камер спостереження

Робочий лист Allegro 9c	**КАРТА ЛЮДСЬКИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІ КОРИСТУВАЧІ	
ІМ'Я АБО РОЛЬ	**СИСТЕМА**
Члени сім'ї	Усередині розумного будинку
ЗОВНІШНІ КОРИСТУВАЧІ	
ПОСТАЧАЛЬНИК	**СИСТЕМА**
Гості, Відвідувачі	**Уся система будинку**
Зловмисник, якщо отримає до них доступ	**Уся система будинку**

Таблиця 3.18

Ризик інформаційних активів для відеопотоку з камер спостереження

<table>
<tr><td colspan="2">Робочий лист Allegro 10</td><td colspan="6">РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ</td></tr>
<tr><td rowspan="10">Ризик інформаційних активів</td><td rowspan="8">Загроза</td><td>Інформаційний актив</td><td colspan="5">Відеопотік камер спостереження</td></tr>
<tr><td>Область інтересів</td><td colspan="5">Неавторизована людина отримує доступ до відеоспостереження.</td></tr>
<tr><td colspan="2">(1) Дійова особа.</td><td colspan="4">Зловмисник</td></tr>
<tr><td colspan="2">(2) Засоби</td><td colspan="4">Зламати приймачі або вкрасти призначений для користувача пульт дистанційного керування.</td></tr>
<tr><td colspan="2">(3) Мотив</td><td colspan="4">Шпигунство, моніторинг за людиною та цікавість</td></tr>
<tr><td colspan="2">(4) Результат</td><td colspan="4">☒розкриття ☐ Руйнування
☐ модифікація ☐ переривання</td></tr>
<tr><td colspan="2">(5) Вимоги безпеки</td><td colspan="4">Трансляції з камери повинні бути захищені від неавторизованих людей. Тільки авторизований користувач повинен їх бачити.</td></tr>
<tr><td colspan="2">(6) Імовірність</td><td>☒ Висока</td><td>☐ Середня</td><td colspan="2">☐ низька</td></tr>
<tr><td colspan="3">(7) Наслідки
Які наслідки для організації або інформації власник активів в результаті порушення вимог безпеки?</td><td colspan="4">(8) Серйозність Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?</td></tr>
<tr><td colspan="3">Якщо сценарій загрози здійснився, зловмисник отримує доступ до системи розумного будинку, а потім вимагає грошовий викуп за інформацію.
Зловмисник може відстежувати жителів розумного будинку, вивчати їх розпорядок дня і записувати їх</td><td>Область впливу</td><td>значення</td><td>оцінка</td></tr>
<tr><td colspan="3"></td><td>Репутація і довіра клієнтів (4)</td><td>Висока (3)</td><td>12</td></tr>
<tr><td colspan="3"></td><td>Фінанси (3)</td><td>Висока (3)</td><td>9</td></tr>
<tr><td colspan="3"></td><td>Продуктивність (2)</td><td>Низьке (1)</td><td>2</td></tr>
<tr><td colspan="3"></td><td>Безпека і здоров'я (5)</td><td>Середнє (2)</td><td>10</td></tr>
<tr><td colspan="3"></td><td>Штрафи(1)</td><td>Низьке (1)</td><td>1</td></tr>
</table>

	поведінку і дії. Таким чином порушується приватність жителів. Успіх дії хакера означає матеріальний збиток власника будинку.	Обумовлена користувачем зона впливу	N / A	
Оцінка відносного ризику				34
(9) Зниження ризиків *Які дії ви зробите, виходячи із загальної оцінки цього ризику?*				
☐ **прийняти**	☐ **відкласти**	☒ пом'якшити	☐ **Передати**	
Для ризиків, які ви вирішили знизити, виконайте наступні дії:				
На якому контейнері ви б застосували контроль?	*Які адміністративні, технічні та фізичні заходи контролю ви б застосували до цього контейнеру?*			
технічний	Обмежте мережевий трафік так, щоб він був доступен тільки авторизованим користувачам. Застосовуйте багаторівневі заходи безпеки.			
фізичний	Зберігайте всі фізичні сховища в надійному місці. Регулярно оновлюйте обладнання, робіть резервні копії для всієї важливої інформації. Встановлюйте камери тільки в безпечних місцях будинку, щоб уникнути несанкціонованого доступу.			
люди	Регулярно проводьте програми навчання з питань безпеки для жителів, щоб вони знали про ймовірні ризики безпеки.			

Підсистема 2 між пристроями і домашнім шлюзом:

- інформаційні ресурси (зображення, документи, музика і т. д.) [Підсистема 1, 2];
- інформація про налаштування розумного будинку [Підсистема 1, 2];
- облікові дані користувача (ім'я користувача і пароль) [Підсистема 2];
- інформація про структуру розумного будинку [Підсистема 1, 2].

Усередині розумного будинку (підрозділ 2) у нас є чотири зазначених вище інформаційних актива. Проаналізуємо їх аспекти безпеки. Після цього описуються аспекти безпеки за межами розумного будинку, пов'язані з підсистемою 3.

Таблиця 3.19

Профіль критично важливих інформаційних ресурсів ((зображення, документи, відео, музика)

Робочий лист Allegro 8	**АКТИВ КРИТИЧНОЇ ІНФОРМАЦІЇ**		
(1) Критичний актив *Що є важливим інформаційним активом?*	**(2) Обгрунтування вибору** *Чому цей інформаційний актив важливий для організації?*	**(3) Опис** *Опис цього інформаційного активу*	
Інформаційні ресурси (зображення, документи, відео, музика і т. Д.)	Цей інформаційний актив важливий, тому що він містить персональні дані про користувачів.	Ця інформація може зберігатися локально або передаватися по локальних мережах. Ці ресурси є приватними і містять приватну інформацію користувачів. Їх можна знайти фізично або в цифровому вигляді.	
(4) Власник			
Власником цієї інформації є жителі.			
(5) Вимоги безпеки			
☐**Конфіденційність**	Тільки користувач з достатній рівнем привілей може переглядати цей інформаційний актив	Жителі можуть переглядати свою конфіденційну інформацію,	
☐ **чесність**	Тільки користувач з достатній рівнем привілей може змінювати цей інформаційний актив таким чином:	Тільки жителі можуть вносити зміни в цю інформацію.	
☐ **доступність**	Цей актив повинен бути доступний персоналу для виконання своєї роботи	Ці інформаційні ресурси повинні бути доступні власникам для повсякденного використання.	
(6) Найважливіша вимога безпеки *Яке найбільш важлива вимога безпеки для цього інформаційного активу?*			
☒ Конфіденційність	☒ Чесність	☒ доступність	☒ інша

Таблиця 3.20

Карта середовища технічних ризиків інформаційних активів для інформаційних ресурсів таких, як зображення, документи, відео, музика і т.д.

Робочий лист Allegro 9a	**КАРТА ТЕХНІЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. ПК	жителі
2. комунікаційні мережі	жителі
3. База даних	жителі

Таблиця 3.21

Карта середовища іфзичних ризиків інформаційних активів для інформаційних ресурсів такиї, як зображення, документи, відео, музика і т. д.

Робочий лист Allegro 9b	**КАРТА ФІЗИЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. фотоальбоми	жителі
2. CD, DVD, USB, резервний носій	жителі
3. Папери, папки	жителі

Таблиця 3.22

Карта середовища людських ризиків інформаційних активів для інформаційних ресурсів таких, як зображення, документи, відео, музика і т.д.

Робочий лист Allegro 9c	**КАРТА ЛЮДСЬКИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІ КОРИСТУВАЧІ	
ІМ'Я АБО РОЛЬ	**БЛОК СИСТЕМИ**
1. жителі	Усередині розумного будинку
ЗОВНІШНІ КОРИСТУВАЧІ	
ПОСТАЧАЛЬНИК	**СИСТЕМА**
1. Гості, Відвідувачі	Обмежений доступ

Таблиця 3.23

Ризик інформаційних активів для інформаційних ресурсів таких, як зображень, документів, відео, музики і т. д.Проблемна область 1

Робочий лист Allegro 10		**РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**	
Ризик інформаційних активів	**Загроза**	**Інформаційний актив**	Інформаційні ресурси (зображення, документи, відео, музика і т. Д.)
		Область інтересів	Сторонні особи можуть переглядати фотографії і особисті документи членів сім'ї розумного будинку
		(1) Дійова особа.	Хакер
		(2) Засоби	Інструменти для злому
		(3) Мотив	цікавість
		(4) Результат	☒**розкриття** ☐ Руйнування ☐ **модифікація** ☐ переривання
		(5) Вимоги безпеки	Тільки авторизовані люди можуть

			переглядати цей інформаційний ресурс.		
		(6) Імовірність	☐ **висока**	☐ **середня**	☒ Низька

(7) Наслідки *Які наслідки для організації або власника інформаційних активів в результаті порушення вимог безпеки?*	(8) Серйозність *Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?*			
Якщо вимоги до безпеки цих інформаційних активів будуть порушені, конфіденційність користувача розумного будинку буде порушена. Репутація жителів постраждає через розкриття активу.	**Область впливу**	**значення**	**оцінка**	
	Впевненість (4)	Високе (3)	12	
	Фінанси (3)	Низьке (1)	3	
	Продуктивність (2)	Низьке (1)	2	
	Безпека і здоров'я (5)	Низьке (1)	5	
	Штрафи (1)	Низьке (1)	1	
	Визначені користувачем області впливу	N / A	0	
Оцінка відносного ризику				23

(9) Зниження ризиків *Які дії ви зробите, виходячи із загальної оцінки цього ризику?*

☐ **прийняти**	☐ **відкласти**	☒ пом'якшити	☐ **Передати**

Для ризиків, які ви вирішили знизити, виконайте наступні дії:

На якому контейнері ви б	*Які адміністративні, технічні та фізичні заходи контролю ви б*

примінили контроль?	*застосували до цього контейнеру?*
технічний	Для регулювання доступу до системи повинна застосовуватися політика контролю доступу.
	Захистіть всі системи, застосувавши кілька рівнів безпеки, таких як шифрування, установіть антивірусну програма в системі
мережа комунікації	Використовувати зашифрований канал зв'язку
фізичний	Використовувати шифрування
люди	Проведення програм з підвищення обізнаності користувачів

Таблиця 3.24

Ризик інформаційних активів для інформаційних ресурсів таких, як зображень, документів, відео, музики і т. д.Проблемна область 2

Робочий лист Allegro 10		**РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**	
Ризик інформаційних активів		**інформаційний актив**	Інформаційні ресурси (зображення, документи, відео, музика і т. Д.)
		Область інтересів	Носії даних (жорсткі диски) будуть недоступні через збій обладнання або відключення живлення. (призводить до відмови в обслуговуванні DoS для користувача.)
	Загроза	(1) Дійова особа.	Постачальник обладнання
		(2)**Засоби**	Втрата потужності при відмові приладів
		(3)**мотив**	випадковий
		(4)**результат**	☐ **розкриття** ☒ Руйнування ☐ **модифікація** ☐ переривання
		(5)**Вимоги безпеки**	Інформаційний актив буде недоступний для авторизованих користувачів.

<table>
<tr><td rowspan="8"></td><td></td><td>(6)імовірність</td><td>☐ висока</td><td>☐ Середня</td><td colspan="2">☒ Низька</td></tr>
<tr><td colspan="2">(7)наслідки Які наслідки для організації або власника інформаційних активів в результаті порушення вимог безпеки?</td><td colspan="4">(8)строгість Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?</td></tr>
<tr><td colspan="2" rowspan="7">Якщо станеться збій системи і немає резервних копій цих інформаційних активів, то вони не будуть відновлені, і ви втратите їх назавжди.</td><td>Область впливу</td><td>значення</td><td>оцінка</td></tr>
<tr><td>Репутація(4)</td><td>Низьке (1)</td><td>4</td></tr>
<tr><td>Фінанси (3)</td><td>Низьке (1)</td><td>3</td></tr>
<tr><td>Продуктивність (2)</td><td>Низьке (1)</td><td>2</td></tr>
<tr><td>Безпека і здоров'я (5)</td><td>Низьке (1)</td><td>5</td></tr>
<tr><td>Штрафи(1)</td><td>Низьке (1)</td><td>1</td></tr>
<tr><td>Вплив, визначений користувачем</td><td>N / A</td><td></td></tr>
<tr><td colspan="5">Оцінка відносного ризику</td><td>15</td></tr>
<tr><td colspan="6">(9) Зниження ризиків
Які дії ви зробите, виходячи із загальної оцінки цього ризику?</td></tr>
<tr><td colspan="2">☐ прийняти</td><td>☐ відкласти</td><td colspan="2">☒ пом'якшити</td><td>☐ Передати</td></tr>
<tr><td colspan="6">Для ризиків, які ви вирішили знизити, виконайте наступні дії:</td></tr>
<tr><td colspan="2">На якому контейнері ви б примінили контроль?</td><td colspan="4">Які адміністративні, технічні та фізичні заходи контролю ви б застосували до цього контейнеру?</td></tr>
<tr><td colspan="2">Жорсткі диски</td><td colspan="4">Обов'язково зробіть резервні копії всіх ваших систем, які містять цінну інформацію. Таким чином ви можете відновити свій інформаційний актив.</td></tr>
<tr><td colspan="2">потужність</td><td colspan="4">Переконайтеся, що у вас є джерело безперебійного живлення (ДБЖ).</td></tr>
</table>

Таблиця 3.25

Профіль критично важливих інформаційних ресурсів (інформація про налаштування розумного будинку або керівництва користувача для побутової техніки)

Робочий лист Allegro 8	**КРИТИЧНИЙ ІНФОРМАЦІЙНИЙ ПРОФІЛЬ АКТИВУ**	
(1) Критичний актив *Що є важливим інформаційним активом?*	**(2) Обгрунтування вибору** *Чому цей інформаційний актив важливий для організації?*	**(3) Опис** *Опис цього інформаційного активу*
Інформація про налаштування Розумного будинку / Інструкції	Цей інформаційний актив дуже важливий, особливо для жителів, тому що без цього активу буде неможливо налаштувати систему розумного будинку або керувати пристроями розумного будинку.	Цей інформаційний актив можна знайти фізично або в цифровому вигляді і зберігати локально або передавати по локальних мережах. Ці ресурси є приватними і містять цінну інформацію про систему розумного будинку. Він може містити докладні інструкції про те, як виконати конкретне завдання або процес. Він містить кроки по налаштуванню або інструкції, які розкажуть, як щось потрібно зробити.
(4) Власник		
Власник розумного будинку Продавець		
(5) Вимоги безпеки		

☐ **Конфіденційність**	Тільки користувач з достатній рівнем привілей може переглядати цей інформаційний актив	Тільки уповноважені особи повинні мати доступ до цих посібників користувача
☐ **чесність**	Тільки користувач з достатній рівнем привілей може змінювати цю інформацію	Ніхто не має права вносити зміни або маніпулювати змістом цього інформаційного активу, крім авторизованого користувача
☐ **доступність**	Цей актив повинен бути доступний цього персоналу для виконання своєї роботи	Інформаційний актив повинен бути доступний при необхідності.

(6) Найважливіша вимога безпеки *Яке найбільш важлива вимога безпеки для цього інформаційного активу?*

☐ Конфіденційність	☒ Чесність	☒ Наявність	☐ інша

Таблиця 3.26

Карта середовища технічних ризиків інформаційних активів для інформації з налаштування розумного будинку / керівництв користувача

Робочий лист Allegro 9a	**КАРТА ТЕХНІЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. Файл даних, що зберігається в системах розумного будинку	жителі

Таблиця 3.27

Карта середовища фізичних ризиків інформаційних активів для інформації про налаштування розумного будинку / керівництв користувача

Робочий лист Allegro 9b	**КАРТА ФІЗИЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. На папері у вигляді книги або керівництва	жителі
2. CD, DVD, резервний носій	жителі
ЗОВНІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1.Є паперові копії активів локально у продавця	Продавець

Таблиця 3.28

Карта середовища людських ризиків інформаційних активів для інформації з налаштування розумного будинку / керівництв користувача

Робочий лист Allegro 9c	**КАРТА ЛЮДСЬКИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІ КОРИСТУВАЧІ	
ІМ'Я АБО РОЛЬ	**БЛОК СИСТЕМИ**
1. Жителі, власник системи	Усередині розумного будинку
ЗОВНІШНІ КОРИСТУВАЧІ	
ПОСТАЧАЛЬНИК	**ОРГАНІЗАЦІЯ**
1. консультант від продавця	Продавець

Таблиця 3.29

Ризик інформаційних активів для інформації про налаштування розумного будинку

Робочий лист Allegro 10		**РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**	
		Інформаційний актив	Інформація про налаштування Розумного будинку / Інструкції

		Область інтересів	Інформація про налаштування Розумного будинку або керівництва користувача		
		(1) Дійова особа.	постачальники-конкуренти		
		(2)**Засоби**	Інструменти для злому		
		(3)**мотив**	Завдавати шкоди системам конкурентів.		
		(4)**результат**	☐ **розкриття** ☐ Руйнування ☒**модифікація** ☐ переривання		
		(5)**Вимоги безпеки**	Тільки авторизований постачальник, який створив актив, може змінювати його вміст з метою оновлення		
		(6)**імовірність.**	☐ висока	☐ середня	☒ низька

(7)**наслідки** *Які наслідки для організації або власника інформаційних активів в результаті порушення вимог безпеки?*	(8)**строгість** *Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?*		
Якщо цей актив буде змінений не уповноваженою особою, це може привести до неправильної роботи різних систем і навіть до того, що хтось отримає травму. Буде складно правильно налаштувати систему розумного будинку, тому станеться збій. Інформаційні активи не захищені від ушкоджень і не можуть використовуватися за призначенням.	**Область впливу**	**значення**	**оцінка**
	Репутація і довіра клієнтів (4)	Високе (3)	12
	Фінанси (3)	Середнє (2)	6
	Продуктивність (2)	Низьке (1)	2
	Безпека і здоров'я (5)	Високе (3)	15
	Штрафи (1)	Низьке (1)	1
	Зона впливу обумовлена користувачем	N / A	

Оцінка відносного ризику	36

(9) Зниження ризиків

Які дії ви зробите, виходячи із загальної оцінки цього ризику?

☐ **прийняти**	☐**відкласти**	☒ пом'якшити	☐ **Передати**

Для ризиків, які ви вирішили знизити, виконайте наступні дії:

На якому контейнері ви б примінили контроль?	*Які адміністративні, технічні та фізичні заходи контролю ви б застосували до цього контейнеру?*
технічний	Обмежте мережевий трафік, щоб він був доступний тільки авторизованим користувачам. Використовуйте багаторівневі заходи безпеки.
фізичний	Зберігайте всі фізичні сховища в надійному місці. Регулярно оновлюйте обладнання, робіть резервні копії всієї важливої інформації. Зашифруйте всі дані на фізичних носіях.
люди	Інформуйте користувачів про проблеми з розкриття конфіденційної інформації за допомогою програм підвищення обізнаності та навчання для користувачів.

Таблиця 3.30

Актив критично важливої інформації (облікові дані користувача)

Робочий лист Allegro 8	**КРИТИЧНО ІНФОРМАЦІЙН АКТИВИ**	
(1) Критичний актив *Що є важливим інформаційним активом?*	**(2) Обгрунтування вибору** *Чому цей інформаційний актив важливий для організації?*	**(3) Опис** *Опис цього інформаційного активу*
Облікові дані користувача	Цей інформаційний актив важливий, тому що він потрібен для аутентифікації користувача	Зазвичай складається з ідентифікатора користувача і пароля для ідентифікації та перевірки користувача.
(4) Власник (и)		

Власником цього інформаційного активу є авторизований користувач			
(5) Вимоги безпеки			
☐ **Конфіденційність**	Тільки користувач з достатній рівнем привілей може переглядати цей інформаційний актив		Тільки жителі, яким дозволено користуватися системою автоматизації розумного будинку.
☐ **чесність**	Тільки користувач з достатній рівнем привілей може змінювати цей інформаційний актив		Тільки жителі, які є власником цього активу, можуть періодично змінювати ці облікові дані.
☐ **доступність**	Цей актив повинен бути доступний персоналу для виконання своєї роботи		Цей актив повинен бути доступний весь час, щоб мати можливість отримати доступ до систем.
(6) Найважливіша вимога безпеки *Яке найбільш важлива вимога безпеки для цього інформаційного активу?*			
☒ Конфіденційність	Чесність	☒ Наявність	☐ інша

Таблиця 3.31

Карта середовища технічних ризиків інформаційних активів для облікових даних користувача

Робочий лист Allegro 9a	**КАРТА ТЕХНІЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. Підсистема 2 (призначений для користувача інтерфейс)	жителі

Таблиця 3.32

Карта середовища фізичних ризиків інформаційних активів для облікових даних користувача

Робочий лист Allegro 9b	**КАРТА ФІЗИЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. На папері	жителі

Таблиця 3.33

Карта середовища людських ризиків інформаційних активів для облікових даних користувача

Робочий лист Allegro 9c	**КАРТА ЛЮДСЬКИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІ КОРИСТУВАЧІ	
ІМ'Я АБО РОЛЬ	**БЛОК СИСТЕМИ**
1. жителі	Уся система будинку

Таблиця 3.34

Ризик інформаційних активів для облікових даних користувача.

Проблемна область 1

Робочий лист Allegro 10		**РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**	
Ризик інформаційних активів	**Загроза**	**Інформаційний актив**	Облікові дані користувача
		Область інтересів	Неавторизована особа отримує ці облікові дані і може отримати доступ до системи розумного будинку.
		(1) Дійова особа.	Зловмисник

		(2) Засоби	– Використання методів соціальної інженерії – Перебирає паролі за замовчуванням, які зазвичай використовуються в такому обладнанні. – Атака методом грубої сили – Використання програм для моніторингу робочого столу – Використання різноманітних програм для пошуку пароля		
		(3) Мотив	Фінанси		
		(4) Результат	☒**розкриття** ☐ Руйнування ☐ **модифікація** ☐ переривання		
		(5) Вимоги безпеки	Ці облікові дані повинні бути тільки у авторизованого користувача.		
		(6) Імовірність	☐**висока**	☒ **Середня**	☐ **низька**

(7) Наслідки *Які наслідки для організації або власника інформаційних активів в результаті результату і порушення вимог безпеки?*	(8) Серйозність *Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?*

Зловмисник отримує доступ до основної системи розумного будинку і вимагає гроші. Хакер має можливість здійснювати несанкціоновані операції.	**Область впливу**	**значення**	**оцінка**
	Репутація (4)	Високе (3)	12
	Фінанси (3)	Високе (3)	9
	Продуктивність (2)	Середнє (2)	4
	Безпека і здоров'я (5)	Високе (3)	15
	Штрафи(1)	Низьке	1

			(1)	
		Обумовлена користувачем зона впливу	N / A	
Оцінка відносного ризику				41
(9) Зниження ризиків *Які дії ви зробите, виходячи із загальної оцінки цього ризику?*				
☐ **прийняти**	☐ **відкласти**	☒ пом'якшити	**Передати**	
Для ризиків, які ви вирішили знизити, виконайте наступні дії:				
На якому контейнері ви б примінили контроль?	*Які адміністративні, технічні та фізичні заходи контролю ви б застосували до цього контейнеру?*			
технічний	Не використовуйте зламані пристрої для доступу до систем розумного будинку. Заблокуйте доступ до систем за допомогою сканеру відбитків пальців.			
фізичний	Не пишіть на папері складні ідентифікатори користувача і паролі і не ховайте їх поруч з робочою станцією			
люди	Переконайтеся, що у вас є програма підвищення обізнаності користувачів, щоб вони знали про ризики соціальної інженерії			

Таблиця 3.35

Ризик інформаційних активів для облікових даних користувача

Проблемна область 2

Робочий лист Allegro 10		**РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**	
Ризик інформаційних активів		**Інформаційний актив**	Облікові дані користувача
		Область інтересів	Стороння людина отримує доступ до системи розумного будинку і може управляти розумним будинком.
	Загроза	(1) Дійова особа.	Зловмисник
		(2) Засоби	Знаходить або краде мобільний пристрій, який вже підключений до системи розумного будинку

		(3) Мотив	Шкідливий намір, фінансові вигоди, цікавість		
		(4) Результат	☐ **розкриття** ☒ Руйнування ☐ **модифікація** ☐ переривання		
		(5) Вимоги безпеки	Ці облікові дані повинні бути тільки у авторизованого користувача.		
		(6) Імовірність	☐ **висока**	☒ **Середня**	☐ **низька**

	(7) Наслідки *Які наслідки для організації або власника інформаційних активів в результаті результату і порушення безпеки* *вимоги?*	(8) Серйозність *Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?*		
	Зловмисник отримує контроль або доступ до основної системи розумного будинку і вимагає грошей (викуп), відстежує всі дії користувачів і пред'являє безліч інших вимог. Зловмисник може, наприклад, отримати доступ до системи опалення розумного будинку і включити воду або цвімкнути і вимкнути світло.	**Область впливу**	**значення**	**оцінка**
		Репутація (4)	Високе (3)	12
		Фінанси (3)	Високе (3)	9
		Продуктивність (2)	Середнє (2)	4
		Безпека і здоров'я (5)	Високе (3)	15
		Штрафи(1)	Низьке (1)	1
		Обумовлена користувачем зона впливу	N / A	
Оцінка відносного ризику				41

(9) Зниження ризиків

Які дії ви зробите, виходячи із загальної оцінки цього ризику?

☐ **прийняти**	☐ **відкласти**	☒ пом'якшити	☐ **Передати**

Для ризиків, які ви вирішили знизити, виконайте наступні дії:

На якому	*Які адміністративні, технічні та фізичні заходи контролю ви*

контейнері ви б примінили контроль?	*б застосували до цього контейнеру? які*
технічний	Не використовуйте зламані пристрої для доступу до систем розумного будинку.
фізичний	Зберігайте свій мобільний пристрій в надійному місці
люди	Пам'ятайте про крадіжки.

Таблиця 3.36

Профіль критично важливих інформаційних активів та інформація про структуру розумного будинку

Робочий лист Allegro 8	**КРИТИЧНО ІНФОРМАЦІЙН АКТИВИ**	
(1) Критичний актив *Що є важливим інформаційним активом?*	**(2) Обгрунтування вибору** *Чому цей інформаційний актив важливий для організації?*	**(3) Опис** *Опис цього інформаційного активу*
Структура розумного будинку / Інформація про прилади	Цей інформаційний актив важливий, тому що документ містить детальну інформацію про системи, прилади і пристрої розумного будинку. Інвентаризація розумного будинку не тільки допомагає користувачеві створити докладний список вмісту розумного будинку, але і надає йому / їй інтерактивний метод для документування та обслуговування систем розумного будинку.	Інвентаризація розумного будинку може бути створена, почавши з перерахування всіх основних приладів, пристроїв і систем в розумному будинку і документування всієї інформації про них. Наявність документу корисне у цілях страхування майна.

(4) Власник (и)			
Власник розумного будинку			
(5) Вимоги безпеки			
☐ **Конфіденційність**	Тільки користувач з достатній рівнем привілей може переглядати цей інформаційний актив.	Власник розумного будинку і страхова компанія мають право переглянути цей інформаційний актив.	
☐ **чесність**	Тільки користувач з достатній рівнем привілей може змінювати цей інформаційний актив.	Тільки власник розумного будинку має право змінювати цей інформаційний актив для оновлення системи і оновлення списку.	
☐ **доступність**	Цей актив повинен бути доступний цього персоналу для виконання своєї роботи.	Актив повинен бути доступний при необхідності як власнику розумного будинку, так і страхової компанії.	
(6) Найважливіша вимога безпеки *Яке найбільш важлива вимога безпеки для цього інформаційного активу?*			
☒ Конфіденційність	☒ Чесність	☐ доступність	☐ інша

Таблиця 3.37

Карта середовища технічних ризиків інформаційних активів

Робочий лист Allegro 9a	**КАРТА ТЕХНІЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**	
ВНУТРІШНІЙ		
ОПИС КОНТЕЙНЕРА		**ВЛАСНИК**
1.	Робочі станції ПК	власник SHAS
2.	База даних будинку	власник SHAS
3.	Внутрішня домашня комунікаційна мережа	власник SHAS

Таблиця 3.38

Карта середовища фзичних ризиків інформаційних активів для інформації про структуру розумного будинку

Робочий лист Allegro 9b	**КАРТА ФІЗИЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. На папері	Користувач
2. CD, DVD	Користувач
3. Внутрішні носії резервного копіювання	Користувач
ЗОВНІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
1. Зовнішні носії резервного копіювання	Користувач

Таблиця 3.39

Карта середовища людських ризиків інформаційних активів для інформації про структуру розумного будинку

Робочий лист Allegro 9c	**КАРТА ЛЮДСЬКИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІ КОРИСТУВАЧІ	
ІМ'Я АБО РОЛЬ	**БЛОК**
1. Власник розумного будинку	Система керування
2. жителі	Система керування
ЗОВНІШНІ КОРИСТУВАЧІ	
ПОСТАЧАЛЬНИК	**ОРГАНІЗАЦІЯ**
1. співробітники в страховій компанії	Страхова компанія

Таблиця 3.40

Ризик інформаційних активів для інформації про структуру розумного будинку

<table>
<tr><td colspan="2">Робочий лист Allegro 10</td><td colspan="5">РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ</td></tr>
<tr><td rowspan="11">Ризик інформаційних активів</td><td rowspan="9">Загроза</td><td>інформаційний актив</td><td colspan="4">Інформація про структуру розумного будинку / інвентаризація</td></tr>
<tr><td>Область інтересів</td><td colspan="4">Хакери можуть отримати доступ до цього інформаційного активу і знайти конкретний пристрій з відомими уразливими, щоб атакувати пристрої системи.</td></tr>
<tr><td colspan="2">(1) Дійова особа.</td><td colspan="3">конкуренти</td></tr>
<tr><td colspan="2">(2) Засоби</td><td colspan="3">Злом
Пошук носіїв, які містять цей актив
Соціальна інженерія</td></tr>
<tr><td colspan="2">(3) Мотив</td><td colspan="3">Отримує актив, щоб знайти спосіб атакувати систему розумного будинку і завдати шкоди.</td></tr>
<tr><td colspan="2">(4) Результат</td><td colspan="3">☒розкриття ☐ Руйнування
☐ модифікація☐ переривання</td></tr>
<tr><td colspan="2">(5) Вимоги безпеки</td><td colspan="3">Інформація про інвентаризацію повинна залишатися конфіденційною, і тільки уповноважені особи можуть отримати доступ до неї.</td></tr>
<tr><td colspan="2">(6) Імовірність</td><td>☒ Висока</td><td>☐ Середня</td><td>☐ низька</td></tr>
<tr><td colspan="3">(7) Наслідки
Які наслідки для організації або власника інформаційних активів в результаті порушення вимог безпеки?</td><td colspan="3">(8) Серйозність
Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?</td></tr>
<tr><td colspan="3" rowspan="3">Якщо конфіденційність інформаційного активу порушена, зловмисник знаходить найслабший</td><td>Область впливу</td><td>значення</td><td>оцінка</td></tr>
<tr><td>Репутація (4)</td><td>Високе (3)</td><td>12</td></tr>
<tr><td>Фінанси (3)</td><td>Високе (3)</td><td>9</td></tr>
</table>

	пристрій з відомими уразливими і атакує його. З його допомогою він може знайти спосіб отримати доступ до основної системи і керувати нею. якщо це станеться, то він може робити все, що захоче, в залежності від свого наміру. Розумний будинок буде як мінімум небезпечний для проживання.	Продуктивність (2)	Низьке (1)	2
		Безпека і здоров'я (5)	Високе (3)	15
		Штрафи (1)	Низьке (1)	1
		Визначені користувачем області впливу	N / A	
Оцінка відносного ризику				39

(9) Зниження ризиків

Які дії ви зробите, виходячи із загальної оцінки цього ризику?

☐ **прийняти**	☐ **відкласти**	☒ пом'якшити	☐ **Передати**

Для ризиків, які ви вирішили знизити, виконайте наступні дії:

До якого контейнера ви застосували б елементи управління?	*Які адміністративні, технічні та фізичні заходи контролю ви б застосували до цього контейнеру? Який залишковий ризик як і раніше приймає організація?*
технічний	Обмежте мережевий трафік так, щоб він був доступен тільки авторизованим користувачам. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Використовуйте механізми шифрування Використовуйте IDS (система виявлення вторгнень) / IPS (система запобігання вторгнень)
Інтернет	Використовуйте безпечний канал зв'язку за допомогою VPN з використанням IPsec, SSL або TLS.
фізичний	Регулярно оновлюйте все обладнання, робіть резервні копії всієї важливої інформації. Тримай всі свої резервні носії в безпечних місцях як всередині, так і за межами розумного будинку.
люди	Проведення програм навчання обізнаності для жителів для того, щоб вони знали про загрози безпеки і соціальну інженерію.

Таблиця 3.41

Профіль активу критично важливої інформації (інформація журналів)

Робочий лист Allegro 8	**КРИТИЧНО ІНФОРМАЦІЙН АКТИВИ**	
(1) Критичний актив *Який криничний інформаційний актив?*	**(2) Обгрунтування вибору** *Чому цей інформаційний актив важливий для організації?*	**(3) Опис** *опис цього інформаційного актив?*
інформація журналів	Цей інформаційний актив дуже важливий, тому що реєстрація подій безпеки, які відбуваються в мережі розумного будинку - це єдиний спосіб визначити, чи знаходиться система в процесі злому або була зламана. Тільки знаючи, що відбувається в мережі, можна правильно захиститися від атак.	Події безпеки повинні реєструватися, а доступ до журналів повинен бути задокументован і захищен від розголошення неавторизованих користувачам.
(4) Власник (и)		
Власнику розумного будинку		
(5) Вимоги безпеки		
☐ **Конфіденційність**	Тільки користувач з достатній рівнем привілей може переглядати цей інформаційний актив	Власник розумного будинку (адміністратор) має право переглядати цю інформацію
☐ **чесність**	Тільки користувач з достатній рівнем привілей може змінювати цей	Тільки власник розумного будинку має

	інформаційний актив таким чином:	право змінювати цю інформацію.
☐ **доступність**	Цей актив повинен бути доступний для виконання своєї роботи	Цей актив повинен бути доступний при необхідності власнику розумного будинку.

(6) Найважливіша вимога безпеки *Яке найбільш важлива вимога безпеки для цього інформаційного активу?*			
☒ Конфіденційність	☒ Чесність	☐ доступність	☐ інша

Таблиця 3.42

Карта середовища технічних ризиків інформаційних активів для інформації журналів

Робочий лист Allegro 9a	**КАРТА ТЕХНІЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
▪ Робочі станції ПК	власник будинку
▪ База даних будинку	власник будинку
▪ Внутрішня домашня комунікаційна мережа	власник будинку
ЗОВНІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
▪ Зовнішня комунікаційна мережа	власник будинку

Таблиця 3.43

Карта середовища іфзичних ризиків інформаційних активів для інформації журналів

Робочий лист Allegro 9b	**КАРТА ФІЗИЧНИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
• CD, DVD, USB	власник будинку
• Внутрішні носії резервного копіювання	власник будинку
ЗОВНІШНІЙ	
ОПИС КОНТЕЙНЕРА	**ВЛАСНИК**
• Зовнішні носії резервного копіювання	власник будинку

Таблиця 3.44

Карта середовища людських ризиків інформаційних активів для інформації журналів

Робочий лист Allegro 9c	**КАРТА ЛЮДСЬКИХ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА**
ВНУТРІШНІ КОРИСТУВАЧІ	
ІМ'Я АБО РОЛЬ	**ВЛАСНИК**
• Власник розумного будинку (системний адміністратор)	власник будинку

Таблиця 3.45

Ризик інформаційних активів для інформації журналів

Робочий лист Allegro 10		**РОБОЧА ТАБЛИЦЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ**	
Ризик інформаційних активів	**Загроза**	Інформаційний актив	інформація журналів
		Область інтересів	Зловмисник може отримати доступ до даних журналів і отримати з них корисну інформацію, наприклад конфігурацію системи, що є серйозним недоліком безпеки, що дозволяє йому атакувати систему розумного будинку.

		(1) Дійова особа.	Конкуренти Хакери		
		(2) Засоби	Злом системи (бекдори, троянські коні, тощо)		
		(3) Мотив	Зловмисна мета Завдати шкоди		
		(4) Результат	☒**розкриття** ☒ Руйнування ☒**модифікація** ☐ переривання		
		(5) Вимоги безпеки	Інформація журналів повинна бути конфіденційною, і тільки уповноважені особи можуть отримати доступ до неї.		
		(6) Імовірність	☒ Висока	☐ **Середня**	☐ **низька**

(7) Наслідки *Які наслідки для організації або власника інформаційних активів в результаті порушення вимог безпеки?*	(8) Серйозність *Наскільки серйозні ці наслідки для організації або власника активу в залежності від області впливу?*		
Якщо конфіденційність інформаційного активу порушена, зловмисник знаходить спосіб отримати доступ до основної системи і контролювати її. Якщо це станеться, то він зможе робити все, що захоче, в залежності від свого наміру. Розумний будинок буде як мінімум небезпечний для проживання.	**Область впливу**	**значення**	**оцінка**
	Репутація і впевненість клієнтів (4)	Високе (3)	12
	Фінанси (3)	Високе (3)	9
	Продуктивність (2)	Низьке (1)	2
	Безпека і здоров'я (5)	Високе (3)	15
	Штрафи (1)	Низьке (1)	1
	Визначені користувачем області впливу	N / A	
Оцінка відносного ризику			39

(9) Зниження ризиків

Які дії ви зробите, виходячи із загальної оцінки цього ризику?

☐ **прийняти**	☐ **відкласти**	☒ пом'якшити	☐ **Передати**

Для ризиків, які ви вирішили знизити, виконайте наступні дії:

На якому контейнері ви б примінили контроль?	*Які адміністративні, технічні та фізичні заходи контролю ви б застосували до цього контейнеру?*
технічний	Обмежте мережевий трафік так, щоб він був доступен тільки авторизованим користувачам. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Журнали повинні бути анонімними Уникайте реєстрації інформації, яка може дати зловмисникові корисну інформацію. Обмежте доступ до журналів, застосувавши механізми контролю доступу. При відправці до віддаленої системи, журнали повинні бути захищені криптографічними механізмами. Застосовуйте багаторівневі заходи протидії для захисту всіх систем.
Інтернет	Використовуйте безпечний канал зв'язку за допомогою VPN з використанням IPsec, SSL або TLS.
фізичний	Регулярно оновлюйте все обладнання, робіть резервні копії всієї важливої інформації. Тримай всі свої резервні носії в безпечних місцях як всередині, так і за межами розумного будинку.
люди	Проведення програми навчання для власника системи та інших користувачів

Висновки за розділом 3

В даному розділі проведена комплексна оцінка ризиків безпеки за допомогою методології OCTAVE Allegro.

Визначено десять найважливіших інформаційних активів, для яких необхідно виконати оцінку.

РОЗДІЛ 4
РЕЗУЛЬТАТИ ВИКОНОЇ РОБОТИ

4.1 Результати роботи

Метою цього розділу є, по-перше, опис всіх ризиків безпеки, які були виявлені шляхом проведення оцінки ризиків інформаційної безпеки з використанням методології OCTAVE Allegro, а по-друге, первірка того, чи були досягнуті раніше поставлені цілі.

Результати роботи були коротко описані у вигляді таблиці, щоб краще зрозуміти виявлені ризики безпеки в типовому розумному будинку. У таблиці 4.1 буде показано, які інформаційні активи ідентифікуються і використовуються в процесі оцінки ризиків, пов'язані з ними ризики, наслідки загроз і можливі заходи протидії, що можуть бути використані з метою захисту інформаційних активів і підвищення безпеки розумного будинку.

Таблиця 4.1

Результат дослідження з оцінки інформаційного ризику

№	Інформаційні активи	Загрози	Вплив	Ризик	Контрзаходи
			Датчики		Обмежте мережевий трафік так, щоб він

1	Інформація, що збирається пристроями та датчикам. Інформація про статус розумного будинку	Зміна даних DoS-атаки Компрометація пристрою або датчика Розкриття інформації Переривання функції	не реагуються на такі ризики, як пожежа, повінь або будь-які дивні рухи всередині будинку. Інсує можливість скомпроментувати датчик, щоб проникнути в систему з невірними обліковими даними, наприклад, щоб викликати певні небажані дії. Фінансові втрати Якщо хакери дізнаються, що вас немає вдома, вони можуть спланувати проникнення в будинок.	39	був доступен тільки авторизованим користувачам. Використовуйте протоколи захисту зв'язку, такі як SSL або DTLS через UDP. Підтримуйте обслуговування апаратного забезпечення Використовуйте резервні копії Проводьте програму навчання жителів з питань безпеки Використовуйте безпечний канал зв'язку за допомогою VPN з використанням IPsec, SSL або TLS. Використовуйте системи з джерелами безперебійного живлення (ДБЖ). Використовуйте багаторівневі заходи безпеки.

2	Відеопоток камер спостереження	Камери спостереження, що фиконують функцію моніторингу	Порушення конфіденційності користувача Фінансові збитки	34	Обмежте мережевий трафік так, щоб він був доступен тільки авторизованим користувачам. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Використовуйте брандмауер і IDS (систему виявлення вторгнень) / IPS (систему запобігання вторгнень) Встановлюйте камери тільки в безпечних місцях будинку, щоб уникнути несанкціонованого доступу.
					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 всі системи, застосувавши кілька рівнів безпеки, таких як шифрування, установка антивірусної програми в систему, або встановіть системи виявлення вторгнень. Використовуйте джерело безперебійного живлення (ДБЖ)
3	Інформаційні ресурси (зображення, документи музика і так далі.)	Крадіжка приватної інформації Відмова в роботі апаратного забезпечення	Порушення конфіденційності користувача Фінансові втрати Збиток репутації тягне за собою втрату інформації	23	

4	Інформація про налаштування розумного будинку або керівництва по експлуатації побутової техніки	Модифікація інформації	Складність у правильній настройці системи розумного дому, отже, можуть виникати несправності. Неправильне використання систем SH. Фінансові збитки.	36	Обмежте мережевий трафік так, щоб він був доступен тільки авторизованим користувачам. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Використовуйте багаторівневі заходи безпеки.
5	Облікові дані користувача (ім'я користувача і пароль)	Видавання себе за іншого користувача та викрадення облікових даних	Несанкціонований доступ до основної системи розумного будинку. Несанкціоноване виконання операцій. Втрата контролю над SHAS Фінансові втрати	41	Заблокуйте доступ до систем за допомогою біометрії (сканери відбитків пальців). Впровадження багатофакторної аутентифікації Забезпечення суворої політики паролів Захистіть всі системи, застосувавши кілька рівнів безпеки, таких як шифрування,

					установка антивірусної програми. Не пишіть паролі на папері і не залишайте їх поруч з робочою станцією або системою. Користуйтесь програмою підвищення обізнаності користувачів, щоб ознайомити їх з соціальною інженерією. Уникайте використання зламаних пристроїв для доступу до систем розумного будинку. Пам'ятайте про можливі крадіжки.

6	Структура розумного будинку	Хакери можуть отримати доступ до інформаційного активу і знайти конкретний пристрій з відомими уразливими, щоб атакувати систему розумного будинку.	Зловмисник знаходить найслабший пристрій з відомими уразливими і атакує його. Потім бере під свій контроль SHAS. В результаті виникають фінансові втрати	39	Обмежте мережевий трафік так, щоб він був доступен тільки авторизованим користувачам. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Використовувати механізми шифрування Робіть резервні копії Застосовуйте багаторівневі засоби захисту для всіх систем. Використовуйте IDS (система виявлення вторгнень) / IPS (система запобігання вторгнень) Використовуйте безпечний канал зв'язку VPN з використанням IPsec, SSL або TLS.

7	Інформація про журнали	Зловмисник може отримати доступ до даних журналів і отримати з них корисну інформацію (конфігурацію системи), що є серйозним недоліком безпеки і дозволяє йому атакувати розумний будинок.	Зловмисник знаходить спосіб отримати доступ до основної системи і в подальшому має можливість контролювати її. Це призводить до фінансових втрат	39	Обмежте мережевий трафік так, щоб він був доступе тільки авторизованим користувачам. Використовуйте протоколи захисту зв'язку, такі як SSL / TLS через TCP / IP або DTLS через UDP. Уникайте розповсюдження інформації, яка може дати зловмисникові корисну інформацію про систему. Обмежте доступ до журналів, застосувавши механізми контролю доступу. Під час відправки в віддалену систему журнали повинні бути захищені криптографічними механізмами.

8	Інформація та дані, що передаються через домашній шлюз	Зловмисник може вкрасти інформацію та дані, що передаються через домашній шлюз.	Зловмисник може додати код вірусу до пакету даних, який потім надсилається до системи, цей пакет може вижирати системні ресурси за допомогою постійного самовідтворення шкідливої програми, так що система не може виконати відповідну роботу, і це призводить до того, що система остаточно стає непридатною для використання.	39	Захистіть мережевий рівень за допомогою служб мережевої безпеки і контролю доступу, таких як обмеження IP-адреси, шифрування мережевого рівня і 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, наприклад SSL. Виконайте управління конфігурацією маршрутизатора. Впровадити чорний список доменів і IP-адрес.

9	Мобільні персональні дані і додатки	Хакери можуть отримати доступ до смартфону (віддалене управління) і встановити шкідливе програмне забезпечення.	Завдяки цьому смартфон може вез вашого відома таємно робити фотографії, записувати розмови і відстежувати ваше місце розташування. Таким чином зловмисник може відстежувати ваше пересування, перехоплювати SMS-повідомлення та телефонні дзвінки, отримувати списки контактів і електронні листи. крім того, він може використовувати ваш мікрофон і камеру. Зловмисник може додати інтерфейс управління і контролю, який дозволить йому дистанційно керувати смартфоном. Зловмисник може навіть відправляти текстові повідомлення, здійснювати дзвінки або	41	Не використовуйте загальнодоступний Wi-Fi. Перед використанням програми для домашньої автоматизації, переуонайтесь, що ви підключені до безпечної мережі. Пам'ятайте про ймовірну крадіжку вашого ристрою.

10	Інформація для відстежування місцеположення	Зловмисник може спостерігати за даними про місцезнаходження користувача	Зловмисник може зробити висновок, що власник Розумного будинку покинув будинок та зпланувати проникнення в розумний будинок, якщо він залишився без нагляду.	34	Обмежте мережевий трафік так, щоб він був доступен тільки авторизованим користувачам. 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 відправлятися у вигляді відкритого тексту, і, отже, в SHAS необхідно використовувати протокол зв'язку для шифрування трафіку між системою відстеження та пристроєм-приймачем. Необхідно мати багаторівневі заходи безпеки.

Висновки за розділом 4

Як було заявлено раніше, технологія Інтернету речей зробила великий вклад в розробку розумних будинків, які принесуть комфорт і ефективність в наше повсякденне життя і наші оселі.

Безпека - одна з цілей розумного будинку на основі IoT, але, ґрунтуючись на тому, які потенційні ризики безпеки було виявлено в результаті дослідження, очевидно, що ці технології можуть бути дуже вразливі для різних атак, які роблять цю технологію небезпечною для життя, якщо достатній рівень безпеки не буде дотримано. Отже, необхідно оцінити ризики безпеки, щоб судити про доцільність використання розумних будинків.

Розумний будинок - це місце, де живуть люди, і він повинен бути безпечним і надійним, для життя. Він повинен забезпечувати достатню безпеку і гарантії конфіденційності. Підключення всіх інтелектуальних об'єктів в будинку до Інтернету і один до одного призводить до потенційних проблем з безпекою, цілісністю та конфіденційністю даних. Ризики безпеки необхідно досліджувати і усувати, як це було зроблено в цій роботі.

Можна зробити висновок, що безпека є критичним фактором і до неї необхідно ставитися дуже серйозно, в іншому випадку можуть виникнути фатальні наслідки, а також усі ризики, зазначені в роботі стануть актуальними.

З метою отримання відповідей на питання дослідження була проведена комплексна оцінка ризиків безпеки з використанням методології OCTAVE Allegro для оцінки ризиків безпеки в типовому розумному будинку.

Були виявлені загрози безпеки і запропоновані заходи протидії виявленим проблемам, що задовольняють більшості з вимог безпеки.

В ході цієї роботи було визначено десять критичних інформаційних активів, для яких була проведена оцінка ризиків безпеки з метою підвищення

їх захисту. Близько п'ятнадцаті ризиків були виявлені в різних частинах або підсистемах розумного будинку.

Пропонуються різні плани щодо зниження цих ризиків або, принаймні, їх зниження до прийнятного рівня. Людський фактор дуже важливий, і до нього потрібно ставитися серйозно. Навчання користувачів необхідно для того, щоб зацікавлені сторони, зокрема жителі, знали про різні проблеми безпеки, особливо про можливості соціальної інженерії.

В процесі виконання роботи були досягнути поставлені цілі та отримані відповіді на питання дослідження. Також був складений список з ризиками безпеки в розумному будинку, впливами та відповідними контрзаходами. Список буде корисним внеском, який може бути використаний в якості основи для специфікації вимог безпеки в розумному будинку.

Для майбутньої роботи оцінка може бути розширена для того, щоб включити набагато більше ризиків безпеки і навіть розглянути інші типи розумних будинків, як було зазначено раніше.

РОЗДІЛ 5
РЕКОМЕНДАЦІЇ ЗАЦІКАВЛЕНИМ СТОРОНАМ

5.1 Рекомендації комерційним зацікавленим сторонам

1) Існує велика потреба в інтеграції безпеки на етапах проектування і розробки.

2) Всі продукти і послуги, що впливають на життя і безпеку жителів, повинні мати високий рівень безпеки.

3) Повинна бути реалізована система блокування доступу до сторінки входу до систему на деякий час після послідовних невдалих спроб входу в систему. Це захищає систему від атак методом перебору і атак за словником.

4) Потрібно вимагати від споживачів змінити паролі за замовчуванням в процесі настройки.

5) Необхідна юридична підтримка в забезпеченні конфіденційності в середовищах IoT, і конфіденційність слід враховувати вже при проектуванні систем IoT.

6) Краще протестувати заходи безпеки перед запуском своїх рішень.

7) Компаніям слід продовжувати усувати відомі уразливості протягом усього життєвого циклу продуктів.

8) Будьте прозорі і розкажіть своїм клієнтам, як саме ви плануєте використовувати їх конфіденційну інформацію.

5.2 Рекомендації некомерційно зацікавленим сторонам

1) Вкрай важливо встановити безпечні імена користувачів і паролі для кожної з систем, а не залишати їх за замовчуванням.

2) Використовуйте довгі паролі з великими та малими літерми, цифрами і спеціальними символами. Часто змінюйте їх на всіх своїх системах і пристроях.

3) Не використовуйте повторно вже використані паролі. Будьте в курсі останніх подій і встановлюйте всі оновлення прошивки або програмного забезпечення, доступні для ваших пристроїв.

4) Споживачі повинні вибирати свої системи і пристрої від відомих постачальників з хорошою репутацією, а не від постачальників з обмеженим досвідом в області безпеки.

5) Якщо у вас є вибір, не вибирайте зручність і простоту використання нехтуючи безпекою.

6) Правильно налаштуйте свій маршрутизатор.

7) Періодично виконуйте тестування на проникнення, щоб гарантувати безпеку ваших систем.

8) Ризики і загрози постійно змінюються, тому важливо, щоб користувач періодично робив оцінку можливих ризиків і переглядав ефективність обраних контрзаходів.

9) Програма навчання з безпеки є обов'язковою умовою для мешканців будинку для того, щоб вони знали про правильні методи забезпечення безпеки.

10) Мобільний телефон використовується як пристрій дистанційного керування. Тому вкрай важливо, щоб він завжди залишався під пильною увагою.

11) Профілактика проблеми краще, ніж її вирішення. Тримайте зловмисників подалі від ваших систем тому що, як тільки вони проникнуть, їх буде складно ідентифікувати.

12) Важливо відзначити, що процес управління ризиками є ітеративним. Оцінка ризиків повинна бути актуальною. Ризики необхідно постійно оцінювати.

13) Пам'ятайте про методи соціальної інженерії. Не довіряйте всім підряд.

14) Забезпечте повну безпеку своїх мереж Wi-Fi. Використовуйте пристрої, які використовують Advanced Encryption Standard (AES) з розміром ключа не менше 128 біт.

Висновки за розділом 5

Мета цього розділу полягала в тому, щоб надати деякі рекомендації комерційним зацікавленим сторонам таким, як постачальникам програмного і апаратного забезпечення, та некомерційним зацікавленим сторонам, таким, як урядовим установам і кінцевим користувачам з метою покращення безпеки цієї технології.

ВИСНОВКИ

Цілі даної роботи полягали в тому, щоб описати можливість застосування Інтернету речей для створення розумних будинків, що забезпечують комфорт, безпеку та поліпшення якості життя.

Впровадження технологій Інтернету речей в будинок створює нові проблеми з безпекою, тому розумні будинки на основі Інтернету речей вимагають дотримання вимог з безпеки.

Сучасні технології збільшують наші можливості з одного боку, і підвищують ризики безпеки з іншого. Система розумного будинку дуже вразлива для різних загроз безпеки як всередині, так і за межами будинку і тому у разі, якщо вона була скомпрометована, конфіденційність користувача, особиста інформація і навіть безпека жителів опиниться під загрозою.

Безпека розумного будинку і його інформаційних активів має вирішальне значення для безпеки і захисту жителів. Отже, необхідно вжити відповідні заходи, щ обули описані в роботі для того, щоб зробити розумний будинок більш безпечним і придатним для життя.

У дослідженні було зроблено:

1. Проведена комплексна оцінка ризиків безпеки за допомогою методології OCTAVE Allegro.

2. Визначено десять найважливіших інформаційних активів, для яких необхідно виконати оцінку.

3. Процес оцінки ризиків пройшов успішно і привів до виявлення близько п’ятнадцяти загроз безпеки як всередині, так і за межами розумного будинку, як показано в таблиці 4.1.

4. Були запропоновані відповідні контрзаходи для зниження ризиків до прийнятного рівня, оскільки сто відсотковий рівень безпеки ніколи не буде досягнуто.

Оцінка ризиків встановлена для виявлення найбільш серйозних потенційних небезпек. Ризики для обладнання, пов'язані з крадіжкою і дефектом, маніпуляціями і саботажем різних пристроїв, що використовуються в SHAS, також вимагають особливої уваги. Основні ризики мережі пов'язані з невірною автентифікацією і відсутністю безпечного каналу зв'язку та шифрування.

Найбільш серйозним ризиком є людський фактор, тому що недотримання правил людьми стає найголовнішою проблемою в системах автоматизації розумного будинку.

Для майбутньої роботи оцінка ризиків безпеки може буде розширена, щоб розглянути інші види областей застосування розумних будинків, такі як розумні будинки для людей похилого віку, розумні будинки для охорони здоров'я, розумні будинки для догляду за дітьми, тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ештон, К. (2009). «Інтернет речей». Журнал РФіД, 22 (7), 97-114.
2. Чи С., Та Сюй Л. і Чжао С. (2015). Інтернет речей: огляд. Межі інформаційних систем, 17 (2), 243-259.
3. Чжун, Ю. (2015) .IoT: Advanced Direction of the Internet of Things
4. Міллер, М. (2015). Інтернет речей: як смарт-телевізори, розумні автомобілі, розумні будинки і розумні міста змінюють світ. Pearson Education.
5. Н.К. Сурядевара і СК Мухопадхьяй, Розумні будинки: проектування, реалізація і проблеми
6. Чи, Дж., Хуанг, З., і Ван, Х. (2011 р, травень). Повідомлення про відкликання Дослідження контрзаходів про розвиток економіки Інтернету речей
7. Аль-фукаха, Аледхарі М.(2015). Інтернет речей 17 (4), 2347-2376.
8. Кук Д. і Дас С. (2004). Інтелектуальні середовища: технології, протоколи і додатки (Том 43). Джон Вілі і сини.
9. Харпер, Р. (2003). Усередині розумного будинку: ідеї, можливості і методи. Усередині розумного будинку (стр. 1-13).
10. Марцано, С. (2003). Погляди на навколишній інтелект. 010 Видавництва.
11. Нуньєс, Р. Дж., І Дельгадо, Дж. (2000). Інтернет-додаток для домашньої автоматизації.
12. Каусар, Ф., Аль-Ейса, Е., і Бахши, І. (2012). Інтелектуальний домашній моніторинг з використанням RSSI в бездротових сенсорних мережах. Міжнародний журнал комп'ютерних мереж і комунікацій, 4 (6), 33.
13. Саад аль-Сумайті, і Салама, М.М. (2014 року). Розумний будинок: огляд літератури. Компоненти і системи електроенергетики, 42 (3-4), 294-305.

14. Zupic, D. (2014 року). Управління енергоспоживанням розумного будинку в контексті активності мешканців. (стор. 127-132).

15. Nutihouse. (2016).:http://nutihouse.com/

16. Стейнберг, Джозеф. (2014 року). «Ці пристрої можуть шпигувати за вами (навіть у вашому власному домі)».

17. Еванс, Д. (2011). Інтернет речей. Як наступна еволюція Інтернету змінює все. Cisco Internet Business Solutions Group (IBSG).http://www.cisco.com/c/ IoT_IBSG_0411FINAL.pdf

18. Монтано, К., Лундмарк, М., & Мер, В. (2006). Найважливіші фактори розумного будинку

19. Мадакам С., Рамасвамі Р. і Тріпаті С. (2015). Інтернет речей (IoT): огляд літератури. Журнал комп'ютерів і комунікацій, 3 (05), 164.

20. Гранцер В., Кастнер В., Нойгшвандтнер Г. і Праус Ф. (2006). Безпека в мережевих системах автоматизації будівель.

21. Аль-Кутайрі (2010). Інтегровані бездротові технології для додатків розумних будинків.

22. Де Сілва, Петра, І.М. (2012). Сучасні розумні будинки.

23. Інженерні програми штучного інтелекту, 25 (7), 1313-1321.

24. Кяс, О. (2013). Розумний будинок.

25. Yoo, DY, S (2007, грудень). Модель безпеки домашньої мережі в повсякденному середовищі.

26. Ricquebourg, D., DurandB., Delahoche, (2006, грудень). Концепція розумного будинку: наше найближче майбутнє. (стор. 23-28).

27. Чонг, Г., Чжіхао, Л., Іфен, Ю. (2011, вересень). Дослідження та впровадження системи розумного будинку на основі Інтернету речей. (стор. 2944-2947).

28. Бінг, К., Фу, Л., Чжуо, Ю., і Янлей, Л. (2011, липень). Проектування системи розумного будинку на основі Інтернету речей. стор. 921-924).

29. Дарьянян, М.(2008 г., грудень). Розумний будинок, мобільні системи і послуги Інтернету речей на основі RFID., 2087-2092.

30. Модель безпеки домашньої мережі в повсякденному середовищі.

31. Ніксон, РА, Wagealla, W., English, C., & Terzis, S. (2004). Проблеми безпеки, конфіденційності та довіри в інтелектуальних середовищах. Інтелектуальні середовища: технології, протоколи і додатки.

32. Шифер, М. (2015 року, травень). Визначення розумного будинку і загрози національній безпеці. (стор. 114-118).

33. Пападопулос К., Захаріадіс Т., Лелігу Н. і Воліотіс С. (2008, квітень). Проблеми безпеки сенсорних мереж в домашньому середовищі. (стор. 1-4).

34. Джан О. і Сахінгоз О (2015 року, травень). Огляд систем виявлення вторгнень в бездротових сенсорних мережах. (стор. 1-6).

35. Роблес, Р. (2010). Огляд безпеки в розробці розумного будинку. Міжнародний журнал передових наук і технологій, (стор. 15).

36. Оцінка вразливості і технології захисту для кібербезпеки розумного будинку з урахуванням ціноутворення кібератак. (стор. 183-190).

37. Ян Л.(2006, жовтень). Безпека і надійність віддаленого моніторингу та управління інтелектуальною домашньою системою. (том 2, стор. 1149-1153).

38. Манторо, (2014 року, квітень). Забезпечення аутентифікації і цілісності повідомлень для Розумного будинку за допомогою смартфона. (стор. 985-989).

39. Тонг, (2013, травень). Модель безпеки інформаційних потоків для домашньої мережі smart grid. (стор. 456-461).

40. Маластров С. , (2005). Вбудоване розпізнавання осіб в режимі реального часу для розумного будинку. 183-190.

41. Essaaidi, M(2010). Інтелектуальні розподілені обчислення

42. Караллі, Р.А., Стівенс, Дж. Ф., Янг, Л. Р., і Вілсон, В. Р. (2007). Allegro: Поліпшення процесу оцінки ризиків інформаційної безпеки.

43. Гері, С., Аліса, Г., і Алексіс, Ф. (2002). Спеціальна публікація NIST 800-30: Керівництво з управління ризиками для систем інформаційних технологій.

44. Падяб А.М., Пайварінта Т. і Харнеск Д. (2014 року, січень). Жанрова оцінка ризиків інформаційної безпеки. (стор. 3442-3451).