Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

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

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Підвищення захищеності елементів розумного будинку за рахунок прогнозування векторів сучасних атак

Виконавець: студент IV курсу, групи КБ-41

_____ **Мирослав ДЗЕКУНОВ**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	**Юрій ЩЕБЛАНІН**	

Нормоконтроль	**Олена БОГУСЛАВСЬКА**	

Київ 2023

Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-41** (група) **Дзекунову Мирославу Андрійовичу**
(прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Підвищення захищеності елементів розумного будинку за рахунок прогнозування векторів сучасних атак

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Безпека розумних будинків, протоколи зв'язку в розумних будинках, технології захисту систем розумного будинку, централізовані і децентралізовані системи.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Аналіз основних підсистем розумного будинку і дослідження історії виникнення систем розумного будинку. Аналіз загальнодоступної інформації про кібератаки. Наведення підходів для запобігання кібератак на системи розумного будинку та

зменшення збитків від інцидентів та витоків інформації.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Результати дослідження важливі для забезпечення кібербезпеки «розумних будинків» та для покращення методів захисту «розумного будинку»

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 12 жовтня 2022 року

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Мирослав ДЗЕКУНОВ (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Отримання завдання	24.10.2022 – 27.11.2022	*виконано*
2	Аналіз літератури	28.11.2022 – 02.01.2023	*виконано*
3	Огляд системи розумний будинок	03.01.2023 – 20.01.2023	*виконано*
4	Збір відомостей щодо системи запобігання вторгненням	21.01.2023 – 26.03.2023	*виконано*
5	Дослідження основних елементів розумного будинку	27.03.2023 – 13.04.2023	*виконано*
6	Аналіз основних вразливостей в технологіях розумного будинку	14.04.2023 – 02.05.2023	*виконано*
7	Написання тексту атестаційної роботи	02.05.2023 – 15.05.2023	*виконано*
8	Оформлення пояснювальної записки	15.05.2023 – 01.06.2023	*виконано*
9	Підготовка та оформлення роботи до захисту	02.06.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Мирослав ДЗЕКУНОВ (ініціали, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 65 сторінки основного тексту, 6 таблиць та 15 рисунків. Список використаних джерел містить 19 найменувань і займає 2 сторінки.

Об'єктом дослідження процес виявлення вразливостей та оцінки захищеності розумного будинку.

Предметом дослідження є елементи розумного будинку відповідальні за захист системи.

Методи дослідження використанні при підготовці кваліфікаційної роботи:

- аналіз наукової літератури;
- експериментальне дослідження;
- порівняння та синтез;
- аналіз даних.

У даній кваліфікаційній роботі проведено комплексне дослідження з можливості підвищення безпеки елементів розумного будинку. По-перше, проведено аналіз наукової літератури, що стосується елементів розумного будинку та систем виявлення та запобігання вторгнень. Це включало вивчення ключових методів та алгоритмів пов'язаних з безпекою розумного будинку.

Результати досліджень можуть застосовуватися в сфері інформаційної безпеки, для покращення методів захисту розумного будинку від кібератак. Наприклад, за допомогою отриманих даних можуть бути розроблені нові методи захисту від кібератак.

Практична цінність отриманих результатів полягає в розробці програмного забезпечення для навчання користувачів системи розумного будинку протидії атак соціальної інженерії.

Напрямки подальших досліджень: розробка нових методів захисту розумного будинку від кібератак на основі отриманих результатів дослідження.

Ключові слова: розумний будинок, методи захисту, аналіз даних, вектор атак, безпека мережі, аналіз даних, захист від фішингу, системи контролю доступу, шкідливі програми, класифікація атак, інформаційна безпека.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

IoT	–	Internet of things
API	–	Application programming interface
HVAC	–	Heating ventilation air-conditioning
SM	–	Smart home
Wi-Fi	–	Wireless fidelity
BLE	–	Bluetooth low energy
IP	–	Internet protocol
VPN	–	Virtual private network
ISP	–	Internet service provider
IT	–	Information Technology
IDS	–	Intrusion detection system
CIA	–	Confidentiality, integrity, availability,
PLS	–	Programmable Logic Controller
CSA	–	Connectivity Standards Alliance
WPAN	–	Wireless personal area network
LAN	–	Local Area Network
SIEM	–	Security Information And Event Management
TCP	–	Transmission Control Protocol
IPv6	–	Internet Protocol version 6
DNS	–	Системи доменних імен
2FA	–	Двохфакторна автентифікацію
SSPSK	–	Spread spectrum phase shift keying
КЦД	–	Конфіденційність, цілісність, доступність
ПК	–	Персональний комп’ютер
MIMO	–	Технологія множинного входу і виходу
ОС	–	Операційна система
ШІ	–	Штучний інтелект

ЗМІСТ

ВСТУП

Актуальність роботи зумовлюється тим, що технологія розумного будинку стала все частіше зустрічатися в українських будинках, що потребує більшої уваги до проблем безпеки, з якими можуть стикатися системи розумного будинку.

Технологія розумного будинку докорінно змінила спосіб взаємодії з нашим житловим простором, пропонуючи комфорт, зручність і навіть віддалений контроль над елементами нашого житла. Від автоматизованого управління освітленням в залежності від температури повітря, або частини дня, до віддаленого управління камерами спостереження та системи домашньої безпеки в цілому – розумні будинки створюють взаємопов'язану та цілісну систему. Однак цей зв'язок також несе в собі потенційні ризики та вразливості, що робить безпеку першим пріоритетом.

Метою роботи є підвищення рівня захищеності систем розумного будинку з урахуванням векторів сучасних атак. Для її досягнення було визначено наступні завдання:

- провести аналітичний огляд систем розумного будинку;
- визначити ризики безпеки методом компанії Microsoft і OCTAVE Allegro;
- проаналізувати вектори кібератак на системи IoT за останні роки;
- розробити програмне забезпечення для навчання користувачів системи розумного будинку орієнтовних на атаки соціальної інженерії.

Об'єктом дослідження є процес виявлення вразливостей та оцінки захищеності розумного будинку.

Предметом дослідження є елементи розумного будинку відповідальні за захист системи.

Методи дослідження використанні при підготовці кваліфікаційної роботи:

- аналіз наукової літератури;
- експериментальне дослідження;
- порівняння та синтез;
- аналіз даних.

РОЗДІЛ 1

ДОСЛІДЖЕННЯ ОСНОВНИХ ЕЛЕМЕНТІВ РОЗУМНОГО БУДИНКУ

1.1 Історія виникнення системи розумного будинку

Концепція розумного будинку з’явилася на початку 20-го століття разом з ідеєю створення автоматизованого житлового простору. Для початку спробую максимально стисло описати ключові моменти виникнення розумного будинку:

- Ранні системи автоматизації (1900-1960 роки)

Ідея автоматизації домашнього простору і створення більш зручного житлового середовища з’явилась ще на початку 1900-х років. Люди з різних професій почали розробляти і покращувати різні системи автоматизації. Так у 1930 році з’явилися перші дистанційно керовані домашні пристрої. До таких пристроїв можна віднести гаражні ворота. Ці ранні системи автоматизації поклали початок розвитку технологій розумного будинку.

- Протокол X10

У 1970 році протокол розробили як стандарт зв’язку для домашньої автоматизації. Цей протокол використовував електричну проводку для передачі сигналів і керування пристроями, дозволяючи власнику керувати освітленням та кухонними приладами. Не дивлячись на те, що цей протокол мав недоліки пов’язані з надійністю та безпекою, він став за основу деяких сучасних протоколів.

- Вплив появи інтернету на розвиток технологій віддаленого керування

Поява інтернету та розвиток IoT стали ключовими моментами в розвитку розумних будинків. Підключення до інтернету зробило можливим віддалене керування домашніми пристроями, що започаткувало нову еру у можливостях систем домашньої автоматизації. Інтеграція датчиків, приводів і технологій бездротового зв’язку дозволила створити взаємопов’язані екосистеми розумних будинків.

У 2010-х роках з’явилися нові комплексні системи екосистем розумних будинків. Великі компанії, як Google, Amazon, Apple та інші розробили власні центральні пункти управління для пристроїв розумного будинку. Ці системи дозволили звичайний користувачам підключати різні пристрої від різних компанії до вибраної платформи.

У теперішній час інтеграція електронних пристроїв для можливості підключення до системи розумного будинку стає все більш поширеною. Освітлення, розумні холодильники, годинники, системи контролю температури та використання енергії дозволяють економити і роблять життя комфортнішим [1].

1.2 Основні підсистеми розумного будинку

Розумний будинок або «інтелектуальний будинок» - це будинок сучасного типу, організований для проживання людей за допомогою єдиної автоматизованої системи управління і моніторингу всіх підсистем безпеки та життєзабезпечення.

Схема основних підсистем розумного будинку, котрі представлені на рисунку1.1.

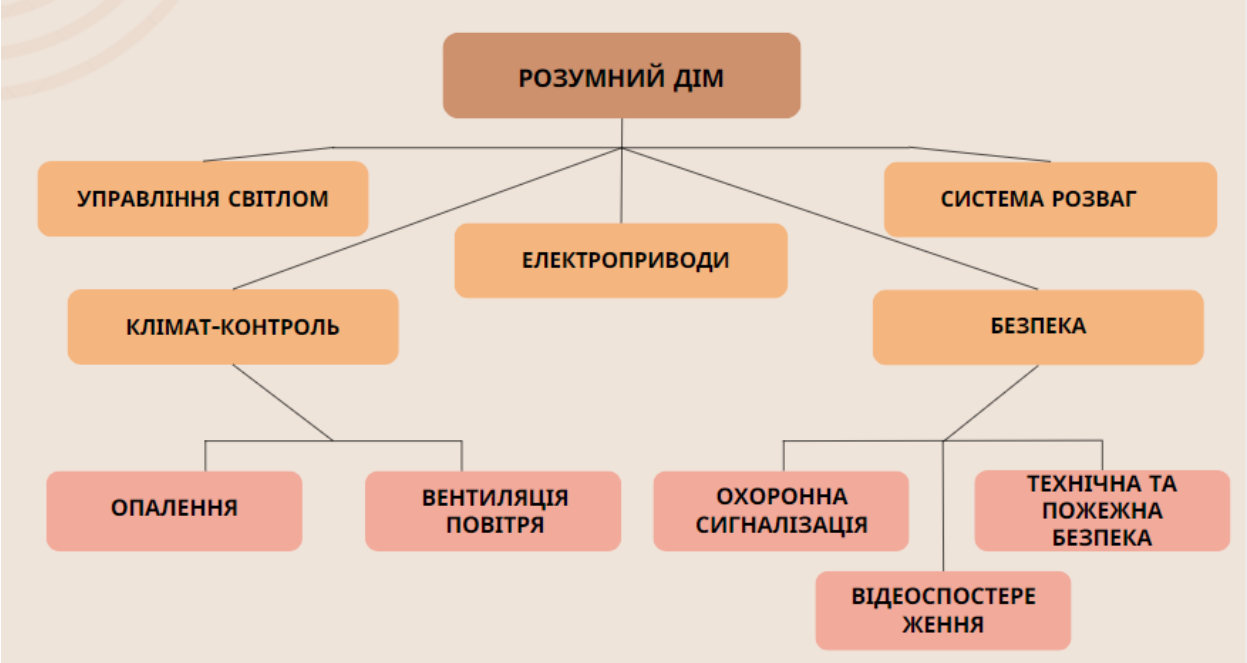

Рисунок 1.1 - Основні підсистеми розумного будинку.

Залежно від того, як організована і побудована система, можна виділити два методи:

- метод децентралізації;
- централізований метод;

Система розумний будинок побудована централізовано, як на рисунку 1.2 і складається з елементів керування, центрального контролера та керованих елементів, а пристрої об’єднані в єдину телекомунікаційну мережу прийому і передачі команд управління.

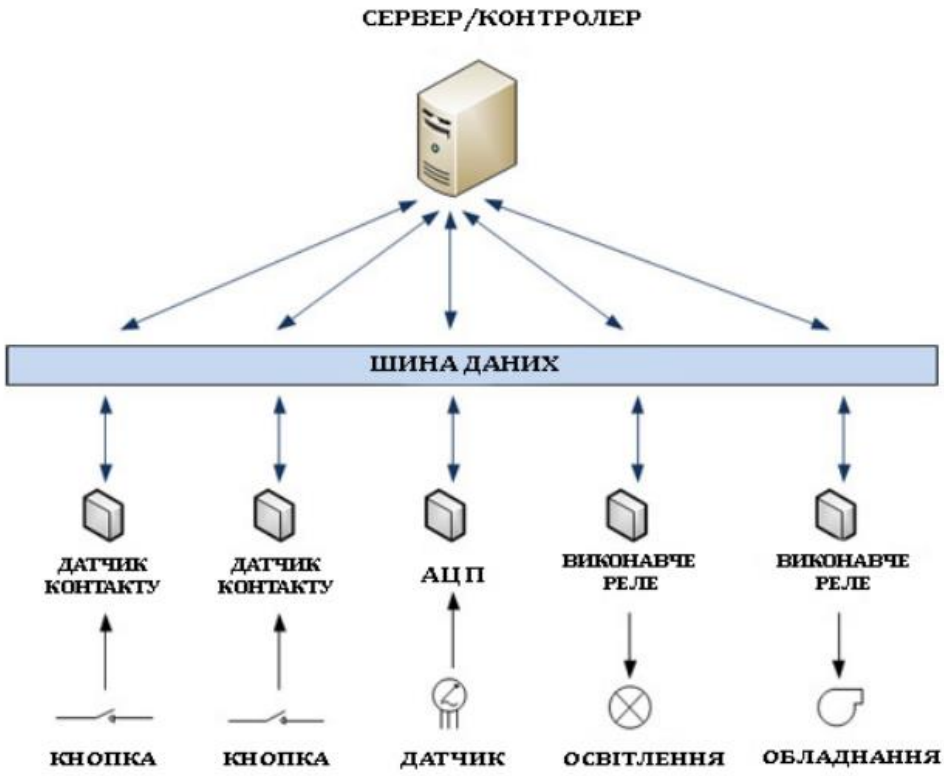

Рисунок 1.2 - Приклад централізованої схеми розумного будинку з головним ПК.

Елемент управління – це обчислювальний або командний пристрій. З його допомогою можна передавати «розумним» системам команди виконання. Елементом управління може бути пульт управління, сенсорна панель, смартфони, та різні датчики. Центральний контролер керує всією системи та кожним її елементом [2].

У порівнянні з централізованим методом, в децентралізованому методі, схему якого зображено на рисунку1.3, немає центрального контролера. В даному випадку

система складається з датчиків і активаторів. За допомогою цих пристроїв виявляються зміни в параметрах контролю будинком і система реагує на ці зміни посилаючи сигнал активаторам.

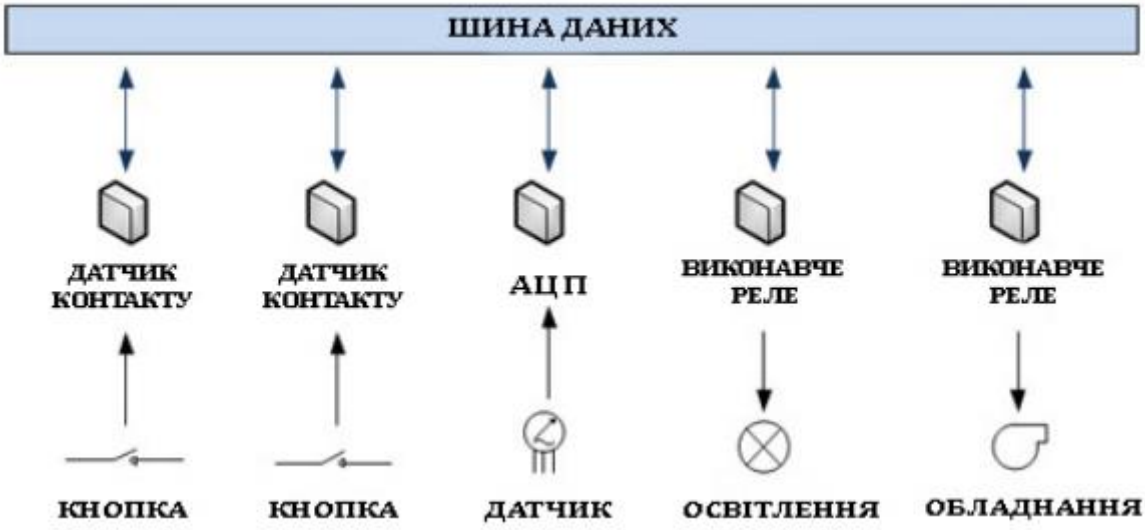

Рисунок 1.3 - Приклад децентралізованої схеми розумного будинку без центрального контролера.

Тепер повернемось безпосередньо до опису кожної з підсистеми розумного будинку, деякі з них представлені на рисунку 1.4.

Рисунок 1.4 - Підсистеми з яких складається розумний будинок.

Отже, розумний дім складається з різних підсистем, які працюють разом щоб забезпечити автоматизацію, контроль і зручність для власників житла. Кожна підсистема фокусується на певному аспекті будинку і призначена для підвищення функціональності та зручності користування. Нижче буде наведений опис кожної підсистеми.

Система освітлення оснащена розумними лампочками, вимикачами і контролерами. Це дозволяє домовласникам дистанційно керувати рівнями освітлення, кольорами та виставляти вмикання і вимикання на певні часові проміжки. Система освітлення може бути інтегрована з іншими підсистемами, такими як датчики руху або системи безпеки, для автоматизації освітлення в залежності від кількості мешканців або потреб безпеки.

Система опалення, вентиляції та кондиціонування (HVAC) в розумному будинку забезпечує інтелектуальний клімат контроль. Термостати можна запрограмувати на автоматичне регулювання температурних параметрів в залежності від потреб мешканців. Цими термостатами можна керувати дистанційно, що дозволяє власникам оптимізувати використання енергії та створювати персоналізовані налаштування комфорту. Також можлива інтеграція з датчиками присутності або технологією геозонування.

Розважальна та аудіосистема зосереджена на створенні захоплюючих аудіовізуальних вражень. Ця підсистема включає в себе смарт-телевізори, потокові пристрої, домашні кінотеатри та аудіоколонки. Смарт- телевізори можуть підключатися до потокових сервісів і надавати доступ до широкого спектру контенту. Аудіосистеми можна розподілити по всьому будинку забезпечуючи синхронізоване відтворення або індивідуальне зонування для різних кімнат. Інтеграція з голосовими асистентами забезпечує управління без допомоги рук і безперешкодну інтеграцію з іншими пристроями [3].

Автоматизовані віконні ролети, такі як моторизовані жалюзі або штори, забезпечують зручність, конфіденційність та енергоефективність. Цими пристроями можна керувати дистанційно або автоматично. Інтеграція з системами освітлення та

клімат-контролю дозволяє координувати автоматизацію, оптимізуючи природне освітлення, надходження тепла та використання енергії.

Підсистеми управління водопостачанням та зрошенням відстежують і контролюють використання води в будинку. Розумні лічильники води надають дані про споживання води в режимі реального часу, виявляючи витоки або ненормоване використання. Системи зрошення коригують графік поливу на основі прогнозів погоди або рівня вологості ґрунту, заощаджуючи води та сприяючи збереженню ландшафту.

1.3 Протоколи зв'язку Smart Home

Протоколи зв'язку відіграють вирішальну роль у забезпеченні безперебійного з'єднання та сумісності між пристроями і системами в межах розумного будинку. Ці протоколи визначають, як пристрої обмінюються даними для забезпечення коректної роботи системи.

Wi-Fi – один із найпопулярніших протоколів зв'язку в «розумних будинках».

Він дозволяє пристроям підключатися до локальної мережі. Це дозволяє запровадити високу швидкість передачі даних, що забезпечує швидкий і надійний зв'язок між пристроями.

До основних версій Wi-Fi, що використовуються в розумних будинках відносяться:

- Wi-Fi 4. Ця версія має вищу швидкість передачі даних і кращу загальну продуктивність у порівнянні з попередніми версіями. Wi-Fi 4 працює в діапазонах 2,4 ГГц і 5 ГГц і підтримує технологію множинного входу і множинного виходу, що дозволяє поліпшити покриття і підвищити пропускну здатність. Він зазвичай використовується для різних пристроїв розумного будинку, таких як смарт-динаміки, пристрої для потокового мовлення та камери безпеки;
- Wi-Fi 5 приніс значний прогрес з точки зору швидкості, пропускної здатності та загальної продуктивності. Він працює виключно в діапазоні частот 5 ГГц і підтримує технології MIMO і формування променя, які забезпечують більш високу

швидкість передачі даних і краще покриття. Wi-Fi 5 добре підходить для вимогливих додатків у розумних будинках, таких як потокове відео високої чіткості, онлайн-ігри та підключення декількох пристроїв.

Bluetooth – це протокол бездротового зв'язку малого радіусу дії, який зазвичай використовується для підключення пристроїв на близькій відстані. Зазвичай використовується в «розумних будинках», для підключення смартфонів, планшетів, смарт-годинників і переносних пристроїв для керування та моніторингу за різними пристроями розумного дому. Bluetooth low energy особливо популярний через низьке енергоспоживання, що робить його придатним для пристроїв, що працюють від акумулятора, таких як датчики та переносні пристрої.

Zigbee – це протокол бездротової стільникової мережі з низьким енергоспоживанням, розроблений для програм із низькою швидкістю передачі даних. Цей протокол працює відповідно до стандарту IEEE 802.15.4, дозволяючи пристроям формувати самовідновлювану мережу. Протокол в основному використовується в системах домашньої автоматизації, таких як системи освітлення, термостатах, інтелектуальних датчиках, де пристрої повинні витрачати на взаємодію небагато енергії і одночасно встановлювати надійне з'єднання.

Коли справа доходить до сітчастої мережі, Zigbee є яскравим прикладом, який використовує топологію сітчастої мережі. Ця топологія дає змогу пристрою спілкуватися з іншими пристроями через кілька стрибків, причому кожен пристрій Zigbee може працювати як маршрутизатор. Завдяки цій стільниковій архітектурі покриття та надійність зв'язку значно покращуються, оскільки повідомлення можуть динамічно маршрутизуватися до місця призначення, навіть якщо пряме з'єднання перешкоджає.

Низьке енергоспоживання Zigbee є однією з його головних переваг. Пристрої, які використовують Zigbee, мають можливість працювати тривали час від обмежених джерел живлення, таких як батареї. Вони роблять це, використовуючи низькі робочі цикли та режими сну, що означає, що вони прокидаються лише тоді, коли це необхідно для економії енергії. Ця функція робить Zigbee чудовим вибором для

розумних домашніх програм, які вимагають тривалого часу автономної роботи, таких як приводи, перемикачі та датчики.

Zigbee надає комплексні функції безпеки для захисту передачі даних у своїй мережі. Він використовує кілька методів безпеки, таких як шифрування, автентифікація та керування ключами, щоб забезпечити захист даних, які спільно використовуються між пристроями Zigbee. Завдяки цим заходам безпеки зберігається конфіденційність і цілісність даних, а також запобігається несанкціонований доступ і втручання.

Масштабованість мереж Zigbee вражає, коливається від декількох пристроїв до тисяч пристроїв. Завдяки сітчастій структурі мережі розширення мережі є легким, оскільки нові пристрої можна вводити, не перешкоджаючи поточній інфраструктурі.

Коли мова заходить про додатки, які потребують керування в реальному або майже реальному часі, Zigbee ідеально підходить завдяки низькій затримці та швидкому часу відгуку. Це особливо важливо в ситуаціях розумного дому, де оперативна реакція на дані датчиків або команди користувача має вирішальне значення. Розумні будинки потребують швидкого керування освітленням, систем безпеки та інтерактивної домашньої автоматизації, які Zigbee ефективно забезпечує.

Z-Wave – протокол, бездротової комірчастої мережі, який широко використовується в «розумних будинках». Так само як і Zigbee, цей протокол працює за стандартом IEEE 802.15.4, але в іншому частотному діапазоні. Протокол відомий своїм великим радіусом дії, низьким енергоспоживанням і сумісністю з великою кількістю пристроїв [4].

Основними характеристиками Z-Wave є те, що цей протокол використовує топологію стільникової мережі, подібну до Zigbee, коли справа доходить до Mesh Networking. Кожен пристрій Z-Wave може діяти як ретранслятор, який може передавати повідомлення на інші пристрої в мережі. Завдяки цій стільниковій архітектурі покриття в середовищі розумного дому одночасно надійне та широке. Повідомлення можна динамічно маршрутизувати між кількома вузлами, підвищуючи надійність зв’язку навіть у великомасштабних розгортаннях.

Основною перевагою Z-Wave є сумісність, яка відрізняє його від інших пристроїв. Z-Wave Alliance, коаліція компаній, гарантує дотримання та сумісність стандартів серед виробників. Це означає, що пристрої Z-Wave від різних брендів можуть без проблем співпрацювати один з одним, дозволяючи власникам нерухомості створювати єдину систему розумного дому, використовуючи продукти різних компаній.

MiWi – це протокол бездротового зв'язку призначений для додатків із низьким енергоспоживанням і низькою швидкістю передачі даних для бездротових сенсорних мереж і пристроїв, що працюють від батарейок, у розумних домашніх умовах. Протокол працює за стандартом IEEE 802.15.4, який визначає фізичній рівень і рівень керування доступом до середовища низькошвидкісної бездротової персональної мережі [5].

Енергоспоживання вузла в мережі підтримується на низькому рівні за допомогою ядер мікроконтролера. Надійність є ключовою особливістю MiWi, протоколу бездротової мережі, який є зручним і зрозумілим. Протокол працює на простій основі, що робить його легким у використанні для тих, хто погано розбирається в технічних аспектах. Незалежно від того, новачок ви чи досвідчений професіонал, цей протокол гарантує безперебійний бездротовий зв'язок, а впровадження вузлів є доступним і бюджетним.

X10 працює через технологію зв'язку по лінії електропередач (PLC), яка використовує наявну в будинку систему електропроводки для передачі керуючих сигналів. X10 відомий своєю простотою використання та економічною ефективністю, що призвело до його широкого використання в ранніх системах домашньої автоматизації.

Основним способом зв'язку системи X10 є використання попередньо існуючої електричної проводки в домогосподарстві для передачі керуючих сигналів. Це досягається за допомогою технології фазової маніпуляції з розширеним спектром (SSPSK) для модуляції цих сигналів в існуючу лінію живлення. Інші пристрої, які підключені до того самого електричного кола, здатні отримувати та інтерпретувати ці сигнали, таким чином забезпечуючи зв'язок і контроль.

Протокол X10 — це проста система, яка використовує нескладні двійкові команди для керування пристроєм. Ці команди складаються з двох компонентів: домашнього коду та коду пристрою, які використовуються для ідентифікації призначеного пристрою. Прикладом команди є "A1 ON", яка вказує на те, що пристрій із кодом будинку A та кодом пристрою 1 слід увімкнути.

Система X10 забезпечує базові можливості керування. Команди для керування можна передавати вручну через контролери X10 або вводити для автоматичного надсилання за розкладом або певними подіями, які їх запускають.

Низька швидкість передачі даних X10 може зробити його вразливим до погіршення сигналу та перешкод. Різні фактори, такі як електричні перешкоди, згасання сигналу та перешкоди від інших електричних пристроїв, можуть значно вплинути на надійність зв’язку X10. Щоб підвищити надійність зв’язку X10 у великих будинках або за умов слабкого сигналу, ретранслятори X10 можна використовувати для збільшення діапазону сигналу та посилення його сили.

Протокол X10 залишається актуальним, незважаючи на появу нових технологій домашньої автоматизації, частково завдяки сумісності його пристроїв і модулів. Домовласники можуть побудувати систему, використовуючи компоненти від багатьох виробників, оскільки вони легко доступні та можуть бездоганно працювати разом. Ця сумісність зіграла важливу роль у довговічності протоколу X10.

Під час свого розквіту протокол X10 вважався новаторським. Однак, якщо порівнювати з сучасними технологіями, у X10 є деякі недоліки. Швидкість передачі даних у нього відносно низька, що робить його не ідеальним для процесів, які потребують режим реального часу для додатків. Крім того, X10 не підтримує двонаправлений зв’язок, що перешкоджає можливості отримувати зворотний зв’язок від пристроїв або виконувати більш складні функції автоматизації.

Короткий опис основних протоколів для «розумних будинків» наведено в таблиці 1.1.

Таблиця 1.1

Основні протоколи

Назва протоколу	Швидкість передачі	Тип передачі	Основні характеристики
Wi-Fi	200+ Мбіт/с		Специфікація IEEE 802.11, високий рівень енергоспоживання. Призначений для частотного діапазону 2.4 Ггц.
Bluetooth	3 Мбіт/с		Частотний діапазон 2.4 Ггц. Низький рівень енергоспоживання. Топологія «зірка». Дальність зв'язку 1-10 м.
Zigbee	20-250 кбіт/с	RF	Працює в різних частотних діапазонах, включаючи 2,4 ГГц, 868 МГц і 915 МГц (Північна Америка). Топологія комірчастої мережі. Низьке енергоспоживання.
Z-Wave	100 кбіт/с	RF	Низьке енергоспоживання. Використовує AES-128 шифрування.
MiWi	20-250 кбіт/с	RF	Мережа, побудована на базі даного протоколу може мати до 1024 вузлів. У ній можуть працювати до 8 координаторів, кожен з яких підтримує до 127 вузлів. MiWi призначений для фізичного і канального рівнів. І потрібний для побудови простих бездротових мереж діапазону 2.4 ГГц.
X10	20 біт/с	PLC, RF	Система віддаленого контролю ламп та побутових приладів, яка використовує технологію X10 wireless technology.

1.4 Методи оцінки ризиків: OCTAVE Allegro

Оперативно-критична оцінка загроз, активів та вразливостей (OCTAVE) - це методологія оцінки ризиків, розроблена Інститутом програмної інженерії (SEI) Університету Карнегі-Меллона. Вона покликана допомогти організаціям ідентифікувати та визначити пріоритети ризиків інформаційної безпеки для широкого набору активів, включаючи дані, людей та обладнання.

Методологія OCTAVE базується на процесі управління ризиками, який передбачає виявлення, аналіз та систематичне усунення ризиків. Методологія складається з трьох етапів:

Етап 1: На цьому етапі організація ідентифікує активи та визначає їх важливість для досягнення своїх бізнес-цілей. Активами можуть бути будь-яка інформація, роль, особа або місце, критично важливі для діяльності організації, наприклад, люди, технології та дані. Потім організація визначає загрози для цих активів і розробляє їхні профілі.

Етап 2: На цьому етапі організація оцінює вразливості своєї інфраструктури, якими можуть скористатися виявлені загрози. Сюди входить виявлення слабких місць у фізичному, технічному та адміністративному контролі організації.

Етап 3: На цьому етапі організація розробляє стратегію безпеки та план її реалізації для усунення виявлених ризиків. План включає визначення пріоритетності ризиків на основі їхнього впливу на організацію та розробку дорожньої карти для управління ними.

Методологія OCTAVE розроблена таким чином, щоб бути гнучкою для задоволення потреб різних організацій. Використовуючи OCTAVE, організації можуть краще зрозуміти свої ризики інформаційної безпеки та розробити ефективні стратегії для їх зменшення.

SEI Університету Карнегі-Меллона створив OCTAVE Allegro, щоб задовольнити специфічні потреби малих та середніх організацій з обмеженими ресурсами та досвідом у сфері інформаційної безпеки.

До розробки OCTAVE Allegro багато методологій оцінки ризиків були розроблені для великих підприємств зі значними бюджетами та спеціалізованими командами безпеки. Малі та середні організації часто потребують більше ресурсів та досвіду для ефективного впровадження цих методологій, що робить їх вразливими до загроз інформаційної безпеки.

OCTAVE Allegro спрощує методологію оцінки ризиків OCTAVE, щоб зробити її більш доступною для малого та середнього бізнесу. Вона зосереджена на виявленні та зменшенні найбільш критичних ризиків для активів організації, визнаючи при цьому обмеженість ресурсів організації.

Основні зміни в OCTAVE Allegro порівняно з оригінальною методологією OCTAVE такі:

Спрощений процес: Процес оцінки ризиків OCTAVE Allegro є більш простим, ніж оригінальна методологія OCTAVE. Він складається з меншої кількості етапів і розроблений таким чином, щоб бути більш доступним для організацій з обмеженими ресурсами та досвідом у сфері інформаційної безпеки.

Зменшена сфера застосування: OCTAVE Allegro має вужчу сферу застосування, ніж оригінальна методологія OCTAVE. Вона зосереджена на виявленні та визначенні пріоритетності найбільш критичних ризиків для активів організації, а не на проведенні комплексної оцінки всіх ризиків.

Зменшення ресурсних зобов'язань: OCTAVE Allegro фокусується на методах контролю та оцінки, які є менш складними у використанні, легшими у впровадженні, вимагають менше маніпуляцій з даними та спрощують зусилля з ідентифікації та пом'якшення ризиків (особливо ті, що пов'язані з документуванням та аналізом).

Повторюваність: OCTAVE Allegro робить акцент на використанні повторюваних методів і практик, щоб невеликі організації могли з легкістю впроваджувати їх у поточні програми управління ризиками.

Послідовність: Незалежно від зменшення обсягу, ресурсів або складності, мета полягає в тому, щоб результати оцінки ризиків були узгодженими в рамках всього підприємства.

Загалом, зміни в OCTAVE Allegro відображають фокус на простоті, практичності та легкості використання. Це має вирішальне значення для малих і середніх організацій, яким може не вистачати ресурсів і досвіду для впровадження більш складної методології оцінки ризиків.

OCTAVE-S - це варіант методології оцінки ризиків OCTAVE, розроблений, щоб допомогти невеликим командам ідентифікувати та визначити пріоритетність ризиків стратегічного рівня для їхньої місії та бізнес-цілей. OCTAVE-S - це більш стратегічний підхід до оцінки ризиків, ніж оригінальна методологія OCTAVE. Він фокусується на місії, бізнес-цілях та критичних активах організації, а не лише на її інформаційних технологіях.

Методологія складається з 3 етапів:

Етап 1: На цьому етапі команда створює профілі загроз, які можуть визначити критерії оцінки, організаційні активи та організаційні практики. Цей етап виконується виключно командою IT-безпеки з мінімальним залученням або без залучення зовнішніх даних, з розумінням того, що команда має достатні або майже достатні знання для виконання завдання.

Етап 2: На цьому етапі команда проводить огляд IT та обчислювальної інфраструктури на високому рівні. Сюди входить розуміння того, як організація використовує технологію і як користувачі та інші сторони інтегрують безпеку у свої практики.

Етап 3: Нарешті, команда визначає ризики та створює плани реагування на них, включаючи стратегії пом'якшення та відновлення.

Загалом, графік публікації випливає з основних стандартів OCTAVE (для корпоративних організацій) в OCTAVE-S, який містить багато з тих же кроків, що і OCTAVE, але орієнтований на невеликі, вільні організації. Це, в свою чергу, стосується невеликих команд з питань внутрішньої безпеки або IT-стратегії з глибокими знаннями про організацію, які можуть застосувати самостійний підхід до оцінки ризиків. Такі організації можуть бути менш ієрархічними, якщо не зовсім пласкими, і мають меншу потребу в директивах з оцінки, що спускаються зверху вниз.

Нарешті, OCTAVE Allegro - це більш комплексний підхід до оцінки ризиків, який все ще оптимізований для малого та середнього бізнесу, але відповідає потребам більш складної та ієрархічної організаційної структури.

1.5 Методи оцінки ризиків Microsoft

Метод оцінки ризиків Microsoft, відомий також як Microsoft Risk Assessment Methodology (MSRAM), є комплексною системою для ідентифікації, аналізу та управління ризиками в інформаційних системах. Цей метод розроблений командою експертів Microsoft і використовується в компанії для забезпечення безпеки своїх продуктів та послуг, а також надається як інструмент для оцінки ризиків організаціям та іншим зацікавленим сторонам.

MSRAM базується на розширеному циклі оцінки ризиків, що складається з наступних етапів:

- Збір інформації: В рамках цього етапу проводиться збір відповідної інформації про систему, її компоненти, архітектуру, залежності та взаємодії. Це може включати аналіз документації, спілкування з експертами, огляд коду та інших джерел інформації.
- Виявлення загроз: За допомогою методології Threat Modeling проводиться ідентифікація потенційних загроз, шляхів атак та вразливостей системи. Цей етап включає аналіз потенційних сценаріїв атак та визначення можливих наслідків для системи.
- Аналіз ризиків: На основі виявлених загроз проводиться оцінка ризиків, включаючи визначення ймовірності виникнення загрози та впливу на систему. Цей етап допомагає визначити пріоритетність ризиків та встановити необхідні заходи для їх управління.
- Розробка стратегій захисту: На основі аналізу ризиків розробляються стратегії та рекомендації щодо запобігання, виявлення та відповіді на ризики. Це може включати використання захисних механізмів, розробку політик безпеки, проведення навчання та тренінгів для персоналу.

- Реалізація та впровадження заходів: На цьому етапі розроблені стратегії та рекомендації реалізуються в практичні заходи. Це може включати впровадження технічних засобів захисту, налаштування систем, вдосконалення процедур та інших заходів для запобігання ризикам.

- Моніторинг та оновлення: Оцінка ризиків є постійним процесом, тому важливо здійснювати моніторинг і оновлення заходів безпеки на регулярній основі. Це включає аналіз нових загроз та вразливостей, вдосконалення захисних механізмів та впровадження актуальних стратегій захисту.

MSRAM забезпечує систематичний підхід до оцінки ризиків та управління безпекою, дозволяючи ідентифікувати та зменшувати потенційні загрози для інформаційних систем. Цей метод дозволяє компаніям та організаціям ефективно аналізувати, планувати та впроваджувати заходи безпеки, що сприяє забезпеченню надійності, конфіденційності та доступності їх інформаційних ресурсів [6].

1.6 Напрямки прогресу системи розумного будинку

Система розумний дім стрімко розвивається завдяки технологічному прогресу та зростаючому попиту на зручність, комфорт та енергоефективність. Ось деякі напрямки розвитку системи розумного будинку:

- Інтеграція та інтероперабельність: Одним з ключових напрямків прогресу є інтеграція та інтероперабельність різних пристроїв і систем розумного будинку. Основна увага приділяється створенню безперешкодного користувацького досвіду, дозволяючи пристроям від різних виробників гармонійно взаємодіяти і працювати разом. Для полегшення взаємодії використовуються такі стандарти, як Zigbee, Z-Wave і Wi-Fi.

- Голосове управління та штучний інтелект: Голосове управління за допомогою віртуальних помічників, таких як Amazon Alexa, Google Assistant і Apple Siri, набуло значної популярності. Системи "розумного дому" впроваджують технології штучного інтелекту (ШІ), які дозволяють виконувати голосові команди, обробляти природну мову і використовувати можливості машинного навчання. Це

дозволяє користувачам керувати різними пристроями, отримувати доступ до інформації та автоматизувати завдання за допомогою голосових команд.

- Підвищена безпека та конфіденційність: Оскільки системи розумного будинку обробляють конфіденційні дані користувачів і керують критично важливими пристроями, забезпечення безпеки і конфіденційності має першорядне значення. Існує прогрес у розробці надійних заходів безпеки, включаючи надійні протоколи шифрування, безпечні методи автентифікації та оцінки вразливостей. Крім того, розвиваються правила і галузеві стандарти для вирішення проблем конфіденційності, пов'язаних зі збором і використанням даних в розумних будинках.

- Енергоефективність та сталий розвиток: Системи розумних будинків все більше зосереджуються на енергоефективності та сталості. Інтеграція з системами управління енергоспоживанням дозволяє оптимізувати використання енергії, інтелектуально керувати освітленням та автоматизовано регулювати температуру. Інтеграція з відновлюваними джерелами енергії, такими як сонячні панелі та системи зберігання енергії, також набирає обертів, дозволяючи домовласникам зменшити свій вплив на навколишнє середовище та заощадити на витратах на електроенергію.

- Розширене зондування та автоматизація: Системи розумного будинку включають в себе передові датчики та можливості автоматизації. Датчики присутності, освітлення, температури та якості повітря забезпечують персоналізовану та контекстно-орієнтовану автоматизацію. Наприклад, розумні термостати можуть вивчати вподобання користувача і відповідно до них регулювати налаштування температури, а розумні системи освітлення можуть автоматично регулювати яскравість на основі рівнів природного освітлення.

- Моніторинг здоров'я та самопочуття: Системи розумного дому розширюються, включаючи можливості моніторингу здоров'я і благополуччя. Пристрої, такі як розумні ліжка, носимі пристрої та датчики навколишнього середовища, можуть відстежувати режим сну, контролювати життєво важливі показники та виявляти потенційні ризики для здоров'я. Ці дані можуть бути використані для надання персоналізованої інформації, підтримки профілактичної

медицини та дистанційного моніторингу людей, особливо людей похилого віку або тих, хто має хронічні захворювання [7].

- Вдосконалені користувацькі інтерфейси: Користувацькі інтерфейси систем розумного дому стають все більш інтуїтивно зрозумілими та зручними. Мобільні додатки, веб-інтерфейси та спеціальні панелі управління пропонують централізований контроль і моніторинг пристроїв. Поява технологій доповненої реальності і віртуальної реальності відкриває нові можливості для залучення нових технологій для інтерактивного досвіду в екосистемі розумного будинку.

- Аналітика даних і машинне навчання: Зростаюча доступність даних з пристроїв розумного будинку відкриває можливості для аналізу даних і машинного навчання. Аналіз даних, згенерованих різними датчиками та пристроями, може дати цінну інформацію про поведінку користувачів, моделі використання енергії та прогнозоване технічне обслуговування. Алгоритми машинного навчання можуть вчитися на історичних даних для оптимізації енергоспоживання, автоматизації рутинних завдань і персоналізації користувацького досвіду.

- Інтеграція з Інтернетом речей (IoT): Поширення пристроїв Інтернету речей розширює можливості систем розумного будинку. Інтеграція з широким спектром пристроїв Інтернету речей, таких як смарт-прилади, носимі пристрої і системи домашньої безпеки, дозволяє створити більш комплексну і взаємопов'язану екосистему розумного будинку. Ця інтеграція забезпечує розширену автоматизацію, моніторинг у реальному часі та безперебійне керування на різних пристроях і платформах.

- Підключення до хмари та віддалений доступ: Підключення до хмари відіграє вирішальну роль у розвитку систем розумного будинку. Зберігання даних і хостингових сервісів у хмарі забезпечує віддалений доступ і керування пристроями, навіть коли користувачі перебувають поза домом. Хмарні платформи також полегшують синхронізацію даних, управління пристроями та оновлення програмного забезпечення, гарантуючи, що системи розумного будинку залишаються актуальними і безпечними.

- Інтеграція з розумними мережами: Системи розумного будинку інтегруються з технологіями "розумних мереж" для оптимізації енергоспоживання і підтримки програм реагування на попит. Підключившись до електромережі, розумні будинки можуть отримувати інформацію про ціни на енергію в режимі реального часу і відповідно коригувати своє енергоспоживання. Така інтеграція сприяє енергоефективності, балансуванню навантаження та інтеграції відновлюваних джерел енергії в електромережу.

- Дизайн, орієнтований на людину: У системах розумного будинку акцент зміщується в бік дизайну, орієнтованого на людину. Користувацький досвід і дизайн користувацького інтерфейсу стають пріоритетними, щоб гарантувати, що технологія розумного дому є інтуїтивно зрозумілою, доступною та інклюзивною для всіх користувачів. Такі принципи дизайну, як простота, персоналізація та зворотній зв'язок з користувачем, сприяють розробці інтерфейсів розумного будинку, які легко зрозуміти і з якими легко взаємодіяти.

- Екосистемні партнерства та інтеграція: Співпраця та партнерство між виробниками пристроїв для розумного дому, постачальниками послуг та розробниками платформ стають все більш поширеними. Метою є створення комплексних екосистем, які пропонують безперешкодну інтеграцію пристроїв, послуг і додатків. Ці екосистеми надають користувачам уніфікований і цілісний досвід роботи з розумним будинком, дозволяючи їм контролювати і управляти своїми будинками через єдину платформу.

- Технологія блокчейн: Технологія блокчейн стає потенційним рішенням для підвищення безпеки, конфіденційності та довіри до систем "розумного будинку". Вона пропонує децентралізоване і захищене від несанкціонованого доступу зберігання транзакційних даних, забезпечуючи надійну автентифікацію і цілісність даних.

Ці напрямки прогресу відображають постійні інновації та розвиток в області систем розумного будинку, пропонуючи користувачам більшу зручність, комфорт, енергоефективність, безпеку і можливості кастомізації [8].

Висновки за розділом 1

У першому розділі кваліфікаційної роботи розглядаються найважливіші аспекти системи розумний будинок. Концепція розумного будинку почала свій шлях ще з ранніх систем автоматизації і еволюціонувала з появою комунікаційних протоколів, ПК, підключення до інтернету, штучного інтелекту. Оскільки в наш час технології розвиваються все більш активніше, розумні будинки мають величезний потенціал для покращення нашого життя. Так, вже зараз ця технологія може запропонувати персоналізований досвід, оптимізацію енергоспоживання та багато іншого.

При розгляді я перерахував основні підсистеми, які складають структуру та функціональність розумного будинку. Важливість кожної підсистеми важко недооцінити, оскільки всі вони сприяють безпеці, енергоефективності та загальному комфорту розумного будинку. Досліджуючи ці підсистеми я отримав уявлення про те, як вони взаємодіють одна з одною.

Аналіз також містить в собі перевірку протоколів зв’язку, які використовуються в системах розумного будинку. Кожен із цих протоколів характеризується відмінними рисами та перевагами, які впливають на швидкість передачі даних, надійність, енергозбереження та сумісність з іншими пристроями. Завдяки ретельному вивченню цих протоколів я зміг оцінити їхні відповідні переваги та недоліки.

Перший розділ став початком для дослідження та розширення теми «розумного будинку». Це дозволило отримати уявлення про історію розробки, ключові підсистеми та протоколи зв’язку, які є невід’ємними компонентами розумного будинку. Ці знання будуть особливо корисними, для переходу до наступних розділів кваліфікаційної, де я зосереджусь на аналізі останніх векторів атак і формулюванні стратегій для підвищення безпеки елементів розумного будинку.

РОЗДІЛ 2

СУЧАСНІ ВРАЗЛИВОСТІ ТА ВЕКТОРИ АТАК НА СИСТЕМИ РОЗУМНОГО БУДИНКУ

2.1 Кібератаки на системи розумного будинку

У жовті 2016 року Dyn, основний постачальник DNS, став жертвою колосальної DDoS-атаки (розподілена відмова в обслуговуванні). Наслідки цієї атаки зазнали на собі численні відомі веб-сайти, у тому числі підключені до систем розумного дому. Зловмисники використовували Mirai, ботнет, який заволодів тисячами пристроїв IoT, багато з яких були конфігураціями розумного будинку з неадекватними налаштуваннями безпеки. Зловмисний трафік, який було випущено, перевантажив сервери Dyn, спричинивши значні перебої в роботі послуг, що сильно вплинуло на користувачів, які покладалися на системи розумного дому.

Системи дзвінка в двері, які зазвичай використовуються для безпеки будинку, постраждали від багатьох випадків несанкціонованого доступу з боку хакерів.

У цих конкретних випадках зловмисникам часто вдавалося отримати доступ до облікових записів Ring, використовуючи слабкі паролі або повторно використовуючи облікові дані, отримані в результаті витоку даних. Опинившись усередині, вони могли переглядати відеозаписи в реальному часі, спілкуватися з користувачами за допомогою функції двостороннього аудіозв’язку та навіть надсилати підроблені екстрені сповіщення за допомогою зламаних пристроїв. Ці події висвітлили питання безпеки щодо пристроїв розумного дому та підкреслили важливість використання надійних єдиних у своєму роді паролів разом із двофакторною автентифікацією.

За останні кілька років дослідники виявили слабкі місця в широко використовуваному протоколі бездротового зв’язку Zigbee, який часто використовується в гаджетах розумного будинку, які надають такі послуги, як інтелектуальне керування освітленням і домашня автоматизація. Ці вразливості

дозволили хакерам перехопити та підробити зв’язок, що відбувається між пристроями з підтримкою Zigbee. Використання цих слабких місць у системі дозволяє хакерам отримати контроль над інтелектуальними пристроями без належного дозволу. Це вторгнення потенційно може поставити під загрозу конфіденційність, безпеку та безпеку дому користувача. Проте з тих пір виробники випустили виправлення та оновлення для усунення цих вразливостей і запобігання подальшому несанкціонованому доступу [9].

Експлойт, націлений на технологію Bluetooth. BlueBorne — це набір вразливостей, які впливають на пристрої, які мають можливості Bluetooth, наприклад системи домашньої автоматизації. Ці недоліки дозволяють хакерам виконувати довільний код на вразливих пристроях без будь-якого втручання користувача, просто використовуючи протоколи Bluetooth. Використовуючи BlueBorne, зловмисники можуть заволодіти розумними домашніми пристроями, що може поставити під загрозу їх продуктивність і надати хакерам доступ до конфіденційної інформації користувачів. У результаті багато хто стурбований безпекою систем домашньої автоматизації з підтримкою Bluetooth, і стало ясно, що необхідні швидкі оновлення безпеки та виправлення.

Ботнети Інтернету речей, такі як Mirai та його похідні, використовувалися в численних кібератаках на системи розумного дому. Ці ботнети використовують скомпрометовані пристрої Інтернету речей, в тому числі пристрої розумного дому, для проведення масштабних атак, таких як DDoS-атаки та підробка облікових даних. В атаках підміни облікових даних хакери можуть використовувати раніше витоки комбінацій імен користувачів і паролів, щоб отримати несанкціонований доступ до облікових записів користувачів, пов'язаних з системами розумного будинку. Після компрометації вони можуть змінювати налаштування обладнання, отримувати доступ до особистої інформації та займатися шкідливою діяльністю.

Ці приклади ілюструють еволюцію загроз для систем розумного дому і вказують на необхідність впровадження надійних заходів безпеки, включаючи регулярне оновлення програмного забезпечення, надійні механізми автентифікації,

безпечні мережеві налаштування і навчання користувачів найкращим практикам кібербезпеки.

2.2 Найпопулярніші кібератаки на системи IoT за час пандемії COVID-19

На сьогоднішній день, деякі атаки на системи розумного будинку виявляються більш вірогідними і популярними, оскільки вони використовують вразливості, які є поширеними серед таких систем. Ось деякі атаки, які згідно останніх спостережень являються найбільш вірогідними:

- Атаки на безпеку мережі (Network Security Attacks).

Це включає атаки на безпеку мережі Wi-Fi або інших мережевих протоколів, що використовуються в системах розумного будинку. Зловмисники можуть намагатися перехоплювати мережевий трафік, зламувати паролі Wi-Fi або використовувати розширений перехоплювач для отримання доступу до системи.

- Вразливості в програмному забезпеченні (Software Vulnerabilities).

Багато систем розумного будинку використовують програмне забезпечення з вразливостями, які можуть бути використані зловмисниками для злому системи. Це можуть бути недоліки в коді, недостатні заходи безпеки або застарілі версії програмного забезпечення.

- Фішингові атаки (Phishing Attacks).

Зловмисники можуть намагатися отримати доступ до облікових записів користувачів системи розумного будинку. Вони можуть надсилати підроблені електронні листи або створювати фальшиві веб-сайти для введення користувачів в оману та отримання їхніх облікових даних.

- Атаки на дистанційне керування (Remote Control Attacks).

Деякі системи розумного будинку мають можливість дистанційного керування, що може бути скомпрометовано зловмисниками. Вони можуть використовувати недоліки в програмному забезпеченні або підроблені облікові дані, щоб отримати доступ до системи та керувати пристроями в будинку.

- Атаки на фізичний доступ (Physical Access Attacks).

Це атаки, які вимагають фізичного доступу до пристроїв системи розумного будинку. Зловмисники можуть намагатися отримати доступ до пристроїв шляхом зламу дверей, вікон або інших механізмів безпеки.

- Атаки на голосові помічники (Voice Assistant Attacks)

Зловмисники можуть використовувати голосові помічники, такі як Amazon Echo або Google Home, для здійснення атак на систему розумного будинку. Вони можуть надсилати фальшиві голосові команди, використовувати служби розпізнавання голосу для підміни ідентифікації користувача або навіть зламати захист голосового помічника.

Таблиця 2.1

Найчастіші кібератаки на період пандемії covid-19

Кібератаки	Опис кібератак
Фішинг	Фішинг з такими заголовками : Оновлення щодо коронавірусу Спалах коронавірусу у вашому місті
Шкідливе програмне забезпечення	BabyShark Mirai Rammit Matsnu Necurs DirCrypt
Програма-вимагач	CovidLock Netwalker
Атаки мережевого рівня	Спроби перехопити мережевий трафік, зламати паролі Wi-Fi або використовувати вразливості мережевих протоколів.

2.3 Проблеми з безпекою в застосунках розумних будинків

У додатках для розумних будинків існує безліч загроз від внутрішніх до зовнішніх типів, при цьому в більшості випадків, в внутрішні загрози, наприклад, пов'язані з тим, що мешканці недостатньо кваліфіковані в питаннях безпеки і рішень для своїх власних будинків, крім того, існують компанії, які виробляють або надають послуги для додатків для розумних будинків, які не пересвідчуються у використанні вимог безпеки, щоб уникнути атак. У цьому дослідженні ми проаналізували деякі найпоширеніші проблеми з безпекою проблеми з безпекою в додатках для розумних будинків.

Сьогодні в розумних будинках використовуються розумні пристрої, які оснащені різними видами програм, необхідних для запуску пристроїв, отже, ці різні програми створюються людьми, що в певний момент робить їх вразливими до помилок, які залишать можливість хакерам отримати доступ до будинків, маніпулюючи зламаним програмним забезпеченням у визначеному місці. Атака на вразливе програмне забезпечення може зайняти короткий або тривалий час, в залежності від того, як довго хакер буде добре поінформований про проблеми в програмному забезпеченні, які має певна будівля або пристрої. Така вразливість програмного забезпечення може виникнути в додатках для розумних будинків, таких як лікарнях, тому що дані пацієнтів є конфіденційними і хакери можуть використати їх для того, щоб хакери можуть використати це, щоб зіпсувати репутацію лікарні. Школи або університети - це місця, які також можуть постраждати від програмних атак і можуть втратити дані студентів, або ж інформація може бути змінена. Важливо пам'ятати, що в розумних будинках мешканці зазвичай створюють нові коди для своїх приладів, таких як двері, сигналізація, замки до головних воріт, аудіо- та відеозаписи всього, що відбувається всередині або зовні. І якщо хакери отримають доступ до програмного забезпечення-шлюзу, то всі дані можуть бути викрадені. Атака на програмне забезпечення може відбуватися багатьма шляхами.

Зловмисники можуть почати стежити за кожною дією у певній мережі і підслуховувати всі дані або вміст які їх цікавлять. Це дуже небезпечно для

користувачів, тому що зловмисники можуть мати всю інформацію про них протягом багатьох років.

На етапі модифікації даних хакери можуть змінити паролі або навіть місцезнаходження передавача або приймача і викрасти потрібну кількість даних. яку вони забажають. У розумних будинках або будівлях державних установ дані можуть бути змінені або видалені.

Маючи паролі, хакери можуть змінювати назви списків, адреси мереж, видаляти минулу мережеву інформацію, змінювати конфігурацію пристроїв тощо. У випадку з лікарнями, лікарі контролюють прийом ліків пацієнтами, стан їхніх хвороб, рівень цукру або кров'яного тиску за допомогою датчиків, встановлених у тілі пацієнта і якщо хакери володіють базою даних, вони можуть маніпулювати всіма цими даними і надсилати фальшиві дані як лікарям, так і пацієнтам[10].

Виправлення вразливостей пов'язане з програмним забезпеченням пристроїв, яке потребує частого оновлення, але коли відбувається збій, то важко розпізнати, чи це керується хакерами, чи це звичайний збій звичайним збоєм, і в такому випадку розумні будинки можуть постраждати від модифікації даних. Отримання виправлень - дуже складне завдання, і це також дуже складна робота для компаній, які працюють безпосередньо з розумними будинками. Компанії, що працюють з бездротовими сенсорними технологіями, щоб надсилати виправлення мешканцям, а з іншого боку, ці виправлення мають бути з іншого боку, ці виправлення повинні бути встановлені, як тільки вони виходять, отже, існує ризик того, що вони будуть скасовані користувачами, тому що під час оновлення цих патчів мешканці можуть використовувати або робити важливі речі зі своїми приладами у розумних будинках. Ці патчі, як правило, виготовляються з програмного забезпечення на апаратне, і це є ризиком, тому буде більш ефективніше, якщо це робиться автоматично. Збій в отриманні розумних будинків, які отримують виправлення, часто трапляються в таких будівлях, як таких будівлях, як лікарні, школи, банки, промислові підприємства, урядові будівлі, де зберігаються найважливіші дані і так далі [11].

Кількість пристроїв всередині розумного будинку величезна, для безпеки мешканці вважають за краще встановлювати різні паролі, це найкращий спосіб

зберегти будинок в безпеці, але може бути небезпечним у випадку, якщо ви забудете ці паролі або передасте їх комусь хто може отримати доступ до будинку в будь-який час. Крім того, пристрої всередині та ззовні постійно обмінюються даними один з одним, так що бувають випадки, коли власник будинку може отримати відбитки пальців на свій мобільний телефон, щоб підтвердити, чи може камера на дверях на дверях може дати доступ до дверного замка або підключити термостат, наприклад, в цей момент, як пристрої і власники будинку будуть знати, що це не власники будинків будуть знати, що це не хакер, який просить і не хакер, який просить і надсилає відбитки пальців, щоб отримати доступ до будинку. Заходи для зменшення ризиків таких атак зменшити ризики таких атак включають захист розумних приладів і пристроїв надійним паролем, використання шифрування, якщо це можливо, та підключення до мережі лише надійних пристрої до своєї мережі.

Це одна з великих проблем в розумних будинках, компанії, які купують розумні пристрої, повинні гарантувати, що параметри добре дотримуються, а дані зберігаються в безпеці від хакерів. Велика проблема в компаніях насправді полягає в тому, як ідентифікувати, захистити, відреагувати або відновити реагувати або відновлювати дані після пошкодження, коли це необхідно.

Існує небагато способів дізнатися, коли хакери атакують тому такі помилки, як втрата пристрою, що містить дані, можуть бути фатальними для компанії або розумного будинку. В інших руках компанії, які несуть відповідальність за збереження даних, можуть втратити дані від своїх співробітників, які можуть викрасти їх без відома інших. За своєю природою ми люди, іноді люди надсилають певну кількість даних за неправильною адресою і складність полягає в тому, як відновити ці втрачені дані

У деяких країнах Європи, Азії та Америки управління даними здійснюється відповідно до державних стандартів, тому існують неурядові організації, які не дотримуються цих правил, ставлячи під загрозу конфіденційність даних своїх клієнтів, або піддаються численним кібератакам з боку сусідів, які знають про ці вразливості.

Різноманітність є великою проблемою для безпеки розумного будинку оскільки всі підключені пристрої в розумному будинку походять від різних виробників, і кожен виробник має різні стандарти безпеки в своєму програмному забезпеченні, а також надійність та якість пристроїв досить сильно відрізняються один від одного[12].

2.4 Загрози інформації в системах розумного будинку

Метою цього розділу є спочатку зібрати всі загрози безпеці, виявлені під час проведення інформаційної оцінки ризиків інформаційної безпеки за методологією OCTAVE Allegro. Результати цього дослідження представлені в таблицях 2.2 і 2.3, які дають кращий огляд виявлених загроз безпеці та потенційні ризики в середовищі розумного будинку. Обидві таблиці показують інформаційні активи, які були виявлені та використані в процесі оцінки ризиків, загрози, пов'язані з ними, а також наслідки або потенційні впливи у вигляді конкретних ризиків.

У таблиці 2.2 показані загрози, виявлені в результаті дослідження всієї системи розумного будинку на основі IoT з точки зору кібернетичної та фізичної перспективи.

Виявлені ризики охоплюють автентифікацію користувача, поведінку користувача, пристрої розумного будинку та обмін даними між домашніми пристроями через Інтернет. У Таблиці 2.3 наведено можливі впливи або потенційні ризики визначені та пов'язані з активами та загрозами, згаданими в Таблиці 2.2.

У таблиці 2.2 показано випадок імітації автентичного домашнього користувача, коли зловмисник намагається діяти замість справжнього домашнього користувача. Щоб досягти успіху, зловмиснику може знадобитися доступ до даних облікового запису резидента, які зазвичай включають ідентифікатор користувача та пароль. Для отримання такого доступу можна використовувати соціальну інженерію або перехоплення звичайних даних.

Таблиця 2.2

Загрози безпеці, виявлені шляхом проведення оцінки інформаційних ризиків з точки зору можливих загроз, пов'язаних з інформаційними активами.

Інформаційний актив	Можливі загрози безпеці
Облікові дані користувача	Видавання себе за користувача Крадіжка особистих даних та облікових даних
Мобільні персональні дані та додатки	Впровадження шкідливого коду в додатки, встановлені на телефоні
Інформація, зібрана пристроями. Інформація про стан розумного будинку	Атаки на відмову в обслуговуванні (DoS) Компрометація пристроїв або датчиків Інформація про стан розумного будинку Розголошення інформації Переривання функцій
Структура розумного будинку. Інформація про інвентаризацію	Отримати доступ до інвентаризаційної інформації для пошуку конкретного пристрою з відомими вразливостями для атак на розумні будинки
Інформація про журнал	Отримання доступу до даних журналів та отримання корисної інформації уможливлення можливих атак на систему розумного будинку
Інформація, що передається через шлюз	Викрадення інформації з пакетів, що передаються через шлюз
Відео з камер спостереження	Взлом камер, щоб стежити за користувачами та шпигувати за ними
Інформація про відстеження місцезнаходження	Спостереження за трафіком даних про місцезнаходження
Інформаційні ресурси (наприклад, фотографії, документи та музика)	Викрадення приватної інформації Зробити носій інформації недоступним через збій обладнання

Таблиця 2.3

Заходи протидії загрозам безпеці в середовищах розумного будинку

Приклади з реального життя	Можливі підходи до пом'якшення наслідків
Неавторизований користувач отримує необхідні облікові дані і може увійти в головну систему розумного будинку.	Контролювати доступ до системи за допомогою ефективних біометричних ідентифікаторів. Впровадити програму інформування користувачів про соціальну інженерію. Впровадити багатофакторну автентифікацію.
Законний користувач втрачає свій мобільний пристрій або його викрадають, а потім маніпулюють додатками для розумного дому.	Уникайте використання незахищеного Wi-Fi, який дає хакерам доступ до персональних даних. Налаштуйте безпечну мережу перед використанням програми для домашньої автоматизації. Пам'ятайте про вкрадені або загублені пристрої.
Глушіння і втручання на фізичному рівні в роботу датчиків і лічильників можуть перешкодити виявляти ризики такі як пожежа, повінь або неочікуваний рух. Скомпрометований датчик руху може бути використаний для визначення наявності людей вдома. Статуси дверних замків і систем сигналізації можуть бути використані, щоб визначити, коли розумний будинок зайнятий.	Використовуйте безпечний канал зв'язку, використовуючи захищену віртуальну приватну мережу (VPN). Обмежте мережевий трафік так, щоб він був доступний лише авторизованим користувачам. Розрбіть навчальну програму з безпеки для мешканців розумного будинку.

Продовження Таблиці 2.3

Заходи протидії загрозам безпеці в середовищах розумного будинку

Зловмисники можуть отримати доступ до інформаційного ресурсу, отримавши незашифровані носії резервних копій або за допомогою атаки соціальної інженерії.	Використовувати систему виявлення вторгнень / систему запобігання вторгненням. Використовувати механізми шифрування для передачі даних.
Шлюз не захищений належним чином, наприклад, відкрита Wi-Fi мережа. Зловмисник може перехопити Wi-Fi з'єднання, впровадити шкідливий код і отримати контроль над системою розумного будинку.	Використовувати товарне обладнання та програмне забезпечення для збору та дослідження мережевого трафіку. Завжди відстежуйте продуктивність системи, шукайте інциденти неправильної поведінки.
Атака через передачу застосунків на аутсорсинг (сторонньому постачальнику послуг).	Обмежте фізичний доступ до пристроїв лише автентифікованими особами. Уникайте аутсорсингу інфраструктури стороннім постачальникам послуг.
Інформація надсилається з системи стеження на пристрій підслуховування у відкритому вигляді та перехоплена зловмисником.	Вимкніть непотрібні сервіси відстеження місцезнаходження на пристроях. Відстежуйте поведінку системи, щоб виявити будь-які підозрілі витоки інформації.
До інформації можуть отримати доступ сторонні особи, якщо інформація не зберігається належним чином і безпечно.	Використовуйте лише надійні та автентичні мережі. Обережно та обмежено діліться інформацією. Використовуйте тільки перевірених провайдерів для отримання технічної підтримки в разі збоїв обладнання в розумному будинку.

Ситуації, коли пристрої можуть бути скомпрометовані, можуть призвести до того, що датчики не зможуть визначити фізичні небезпеки, такі як пожежа, повінь або будь-які незвичайні рухи в будинку. Крім того, якщо хакер отримує доступ до даних, зібраних встановленими датчиками, він може впровадити шкідливі коди, віруси або черв'яків у мережевий трафік, який потім може бути випущений у систему або мобільні програми. Це може призвести до інтенсивного використання системних ресурсів під час самовідтворення коду, що зрештою призведе до нездатності системи досягти запланованої мети, що зробить систему розумного дому непридатною для використання.

Якщо зловмисник отримує інформацію про місцезнаходження за допомогою GPS або мобільних пристроїв, він може зробити висновок про відсутність власника розумного будинку, що призведе до серйозних наслідків, наприклад фінансової шкоди, спричиненої зломом [13].

У таблиці 2.3 перераховані можливі контрзаходи, які можна застосувати для захисту інформаційних активів і підвищення безпеки розумного будинку.

У таблиці 2.3 запропоновані заходи протидії загрозам і ризикам безпеки тісно пов'язані між собою. Перший запропонований контрзахід — впровадження надійного методу автентифікації, наприклад біометричних ідентифікаторів. Біометричні характеристики охоплюють низку фізичних характеристик, включаючи відбитки пальців, геометрію руки, сканування сітківки та райдужної оболонки ока та аналіз підпису. Біометричну технологію хвалять за її потужні можливості автентифікації як у цивільних, так і в судово-медичних установах. Крім того, це сприймається як підхід, який підходить для людей з когнітивними порушеннями, яким важко запам'ятати свої облікові дані. Біометрія також надає чудову можливість для впровадження на апаратних платформах. Одним із ефективних способів інформування користувачів про проблеми безпеки є пропонування постійних програм підвищення обізнаності та навчання. Багатофакторна автентифікація - це процес ідентифікації користувача шляхом перевірки двох або більше тверджень, представлених користувачем, кожне з яких належить до різних категорій факторів, які включають те, що ви знаєте, те, що ви маєте, або те, ким ви є.

Використання захищених Wi-Fi з'єднань в середовищі розумного будинку не дозволяє зловмиснику перехопити мережеве з'єднання перехопити мережеве з'єднання, а отже, зменшує можливість доступу до конфіденційних даних шляхом прослуховування мережевого трафіку, що проходить через нього, або впроваджуючи шкідливі коди в систему. Перехоплення бездротового з'єднання створює вразливість, де зловмисник може впровадити шкідливий код, який може бути виконаний деякими мобільними додатками. Зловмисники можуть використовувати готові інструменти, такі як WebView API, для вбудовування веб-вмісту в мобільні додатки.

Використовуючи захищені канали зв'язку, обмежуючи доступ до трафіку лише авторизованим користувачам, а також проводячи заходи безпеки, зловмисники можуть

доступу до трафіку лише авторизованим користувачам, а також проведення тренінгів з безпеки, модифікації інформації, розголошення інформації, а також компрометації пристроїв або датчиків можна уникнути. Це має зменшити потенційні ризики маніпуляцій з пристроями а отже, зменшити фінансові втрати.

Постійне вивчення мережевого трафіку, забезпечення доступу до конфігурацій системи та моніторинг поведінки системи повинні запобігти крадіжці інформації через мережі розумного будинку. Це, в свою чергу, має зменшити час простою системи, знизити ймовірність вичерпання ресурсів системи, а також зменшити ймовірність появи нових вразливостей в системі розумний дім.

Виконання частого резервного копіювання та архівування даних дозволяє зберігати копії конфіденційних даних і захищає їх як від фізичного, так і від технічного пошкодження. Захист носіїв резервних копій повинен бути забезпечуватися наявністю та застосуванням політики безпеки, наданням прав доступу до програмного забезпечення для резервного копіювання лише уповноваженим особам авторизованим особам, зберігання резервних копій за межами офісу, контролю фізичного доступу до місця зберігання резервних копій, використання захищених носіїв інформації.

Зберігання резервних копій, використання вогнетривкого сейфу з відповідним носієм інформації, а також використання захищених паролем і зашифрованих резервних копій.

Необхідно звернути увагу на захист фізичного розташування та доступу до інтерфейсів конфігурації пристроїв.

Очікується, що використання уніфікованого методу автентифікації як для логічного, так і для фізичного контролю доступу в системі розумного будинку підвищить економічну ефективність.

Важливо визнати, що запропоновані методи пом’якшення не дають абсолютної відповіді на ідентифіковані небезпеки та ризики. Скоріше контрзаходи служать засобом стримування загроз безпеці та зменшення серйозності ризиків і наслідків, що виникають. Однак суворе дотримання контрзаходів безпеки може мати негативний вплив на зручність використання системи. Повне вимкнення служби визначення місцезнаходження може допомогти захистити конфіденційність користувача, але це може значно перешкодити користуванню пристроєм. Тому вкрай важливо знайти баланс між безпекою системи та простотою використання, яку вона забезпечує.

Як частину стратегій пом’якшення, посилення заходів безпеки та конфіденційності для мобільних пристроїв можна розглядати як основу.

Один із підходів до пом’якшення, наведених у таблиці 2.3, передбачає ретельний вибір надійних постачальників для пристроїв Інтернету речей і компонентів системи. Пристрої IoT, придбані від ненадійних постачальників, можуть містити шкідливий код або неправильні конфігурації, які можуть підірвати будь-які впроваджені заходи безпеки. Крім того, щоб підтримувати стабільність і продуктивність системи, періодичне технічне обслуговування, перевірки конфігурації та виправлення помилок повинні проводитися автентифікованим і відповідно навченим персоналом.

Домашнє середовище на основі Інтернету речей (IoT) зазвичай охоплює безліч пристроїв, послуг і постачальників. Пристрої розумного дому разом із відповідними постачальниками можна класифікувати на шість різних категорій. Ці категорії включають розподіл електроенергії, контролери розумного дому, будівельні

програми, побутову техніку, комунікаційні пристрої, а також постачальників IT і телекомунікацій.

Конструкція розумного дому, підключеного до Інтернету речей (IoT), складається з трьох основних рівнів: рівня сприйняття, також відомого як рівень пристроїв, рівня мережі та рівня додатків. На малюнку 2.1 представлено візуальне представлення стандартного налаштування розумного дому на основі IoT і потенційних загроз безпеці, присутніх у середовищі. Ці ризики можуть охоплювати кілька рівнів архітектури IoT. Наприклад, ризик невиправданого проникнення може бути присутнім як у доступі до основних конфігурацій системи, так і в доступі до шлюзу IoT. Тому надійний метод автентифікації повинен бути впроваджений у всіх цих точках. Технологія біометрії може бути вбудована в багатофакторну автентифікацію для створення надійного механізму автентифікації користувачів.

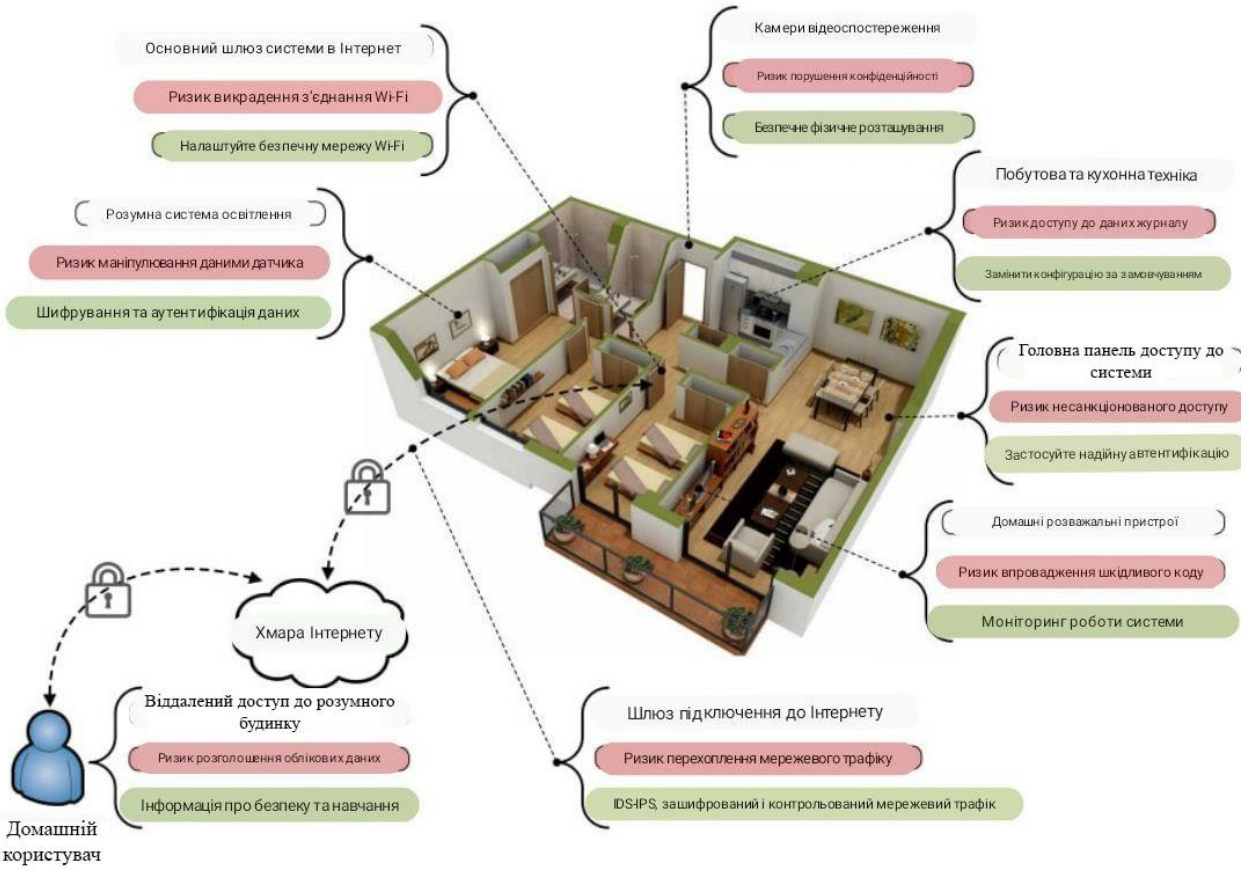

Рисунок 2.1 - Ризики безпеки та підходи до їх зменшення.

Пристроям Інтернету речей, встановленим у розумних будинках, не вистачає високої обчислювальної потужності, великого простору для зберігання даних і великого обсяг пам'яті. Тому впровадження потужних рішень для забезпечення безпеки може бути недоступним варіантом.

Забезпечити безпечне з'єднання між пристроями Інтернету речей та шлюзом в середовищі розумного будинку, розподілений механізм шифрування або енергоефективне шифрування даних, побудоване за принципом трикутника на основі алгоритму безпеки, який використовує ефективну генерацію ключів.

На межі мережевого рівня шлюз IoT працює як посередник між пристроями IoT та зовнішньою мережею. Шлюз IoT вразливий до різних атак на безпеку, таких як атака "man in the middle" та можливість збору даних з пристроїв IoT. Тому безпека шлюзу є критично важливою потребою для захисту потоку даних всередині і зовні середовища розумного будинку. Безпечний шлюз може бути побудований за допомогою ефективних алгоритмів безпеки, таких як криптографія еліптичних кривих та використання надійних підходів до автентифікації користувачів.

Для досягнення високого рівня безпеки на всьому шляху передачі даних, від пристрою IoT до домашнього користувача на віддаленого користувача, мережеве з'єднання з інтернет-провайдером (ISP) повинно бути захищеним. Поширені механізми мережевої безпеки, такі як віртуальні приватні мережі (VPN), повинні бути реалізовані для забезпечення зашифрованого з'єднання з провайдером. Розподілена система виявлення вторгнень (IDS) для мереж IoT повинна бути розгорнута. Крім того, збір та моніторинг трафіку з використанням товарного обладнання та програмного забезпечення можна розгорнути для побудови системи раннього попередження для виявлення будь-якої аномальної поведінки в мережевому трафіку.

2.5 Соціальна інженерія по відношенню до систем розумних будинків

Соціальна інженерія в контексті розумних будинків є критично важливим аспектом кібербезпеки, який потребує уваги та обізнаності. Оскільки наші будинки стають все більш підключеними та автоматизованими, ризики, пов'язані з атаками

соціальної інженерії, зростають. Соціальна інженерія - це маніпулювання та використання людської поведінки з метою обману для розкриття конфіденційної інформації або вчинення дій, які ставлять під загрозу їхню безпеку.

У контексті розумних будинків атаки соціальної інженерії можуть мати серйозні наслідки. Зловмисники можуть використовувати різні тактики, щоб отримати несанкціонований доступ до систем розумного будинку, керувати підключеними пристроями або отримати особисту інформацію. Одним із поширених методів є фішинг, коли зловмисники надсилають оманливі електронні листи, повідомлення або телефонні дзвінки, які виглядають легітимними і виманюють у користувачів облікові дані для входу в систему або конфіденційні дані. Такі спроби фішингу можуть бути дуже переконливими, часто з використанням складних технологій і створенням відчуття терміновості або страху, що спонукає до негайних дій.

Видавання себе за іншу особу - ще один метод соціальної інженерії, поширений у розумних будинках. Зловмисники можуть видавати себе за сервісних техніків, працівників служби доставки або навіть друзів і членів сім'ї, щоб отримати фізичний доступ до розумного будинку. Потрапивши всередину, вони можуть маніпулювати пристроями, встановлювати шкідливе програмне забезпечення або збирати інформацію, яка може бути використана для подальших атак або несанкціонованих дій.

Зловмисники створюють фальшиві сценарії або приводи, щоб обманом змусити людей розкрити конфіденційну інформацію. Наприклад, зловмисник може видавати себе за представника постачальника послуг для розумного дому, стверджуючи, що вирішує технічну проблему або пропонує оновлення. Увійшовши в довіру, зловмисник може переконати власника будинку надати облікові дані доступу або іншу конфіденційну інформацію.

Щоб завоювати вашу довіру, зловмисник надає точну інформацію про ваші пристрої розумного будинку, наприклад, номери моделей або нещодавні покупки. Він може навіть посилатися на нещодавні новини про порушення безпеки, щоб зробити свою історію більш переконливою. Потім зловмисник просить вас надати йому ваші

облікові дані для входу, стверджуючи, що ця інформація потрібна йому для віддаленого оновлення ваших пристроїв.

Взаємопов'язаність пристроїв розумного будинку також створює нові вразливості для атак соціальної інженерії. Голосові помічники, розумні колонки та інші взаємопов'язані пристрої можуть бути використані зловмисниками для маніпулювання користувачами, щоб змусити їх розкрити конфіденційну інформацію або виконати дії, які ставлять під загрозу їхню приватність і безпеку.

Щоб зменшити ризики соціальної інженерії в розумних будинках, дуже важливо вживати активних заходів безпеки. Користувачі повинні проявляти обережність, відповідаючи на небажані повідомлення, і самостійно перевіряти автентичність джерела, перш ніж ділитися будь-якою конфіденційною інформацією. Важливо перевіряти особу осіб, які називають себе постачальниками послуг або технічними спеціалістами, а власникам будинків слід звертатися безпосередньо до відповідних компаній, щоб підтвердити їхню легітимність.

Безпека паролів і облікових даних - ще один важливий аспект безпеки розумного будинку. Для всіх пристроїв розумного будинку і пов'язаних з ними облікових записів слід використовувати надійні, унікальні паролі. Також бажано використовувати двофакторну автентифікацію для підсилення захисту. Дуже важливо інформувати членів сім'ї про ризики соціальної інженерії та просувати культуру обізнаності в питаннях кібербезпеки.

Регулярне оновлення прошивки та програмного забезпечення пристроїв розумного дому має вирішальне значення для усунення відомих вразливостей і захисту від потенційних зловмисників. Крім того, користувачі повинні з обережністю ставитися до надання фізичного доступу до своїх розумних будинків і усвідомлювати, кого вони впускають до своїх приміщень.

Отже, соціальна інженерія становить значну загрозу для безпеки розумних будинків. Розуміючи тактику зловмисників та впроваджуючи активні заходи безпеки, користувачі можуть зменшити ризики, пов'язані з атаками соціальної інженерії. Побудова надійного захисту від соціальної інженерії має важливе значення для

збереження особистої інформації, захисту підключених пристроїв і підтримки конфіденційності та безпеки систем розумного будинку.

Протидія атакам соціальної інженерії на розумні будинки вимагає поєднання активних заходів і практик безпеки. Ось кілька методів, які можуть допомогти зменшити ризики та захиститися від атак соціальної інженерії.

Навчайтеся: Ознайомтеся з різними методами соціальної інженерії, такими як фішинг, підставні повідомлення та імітація. Будьте в курсі останніх тенденцій атак і методів, які використовують зловмисники для обману власників житла. Розуміння цих тактик може допомогти вам розпізнати потенційні загрози та відреагувати на них.

Перевіряйте особу: Завжди перевіряйте особу людини, перш ніж надавати їй доступ до пристроїв вашого розумного будинку або ділитися конфіденційною інформацією. Будьте обережні з несподіваними відвідувачами, які представляються технічними спеціалістами або представниками компанії. Попросіть пред'явити належне посвідчення або зв'яжіться з відповідним постачальником послуг напряму, щоб перевірити їхні повноваження.

Використовуйте надійні паролі: Переконайтеся, що всі ваші пристрої розумного будинку та пов'язані з ними облікові записи захищені надійними та унікальними паролями. Не використовуйте паролі за замовчуванням або ті, що легко вгадуються. Розгляньте можливість використання менеджера паролів для створення та безпечного зберігання складних паролів для кожного пристрою або служби.

Увімкніть двофакторну автентифікацію: Увімкніть 2FA, де це можливо, щоб додати додатковий рівень безпеки до ваших облікових записів розумного будинку. Це вимагає додаткового етапу перевірки, наприклад, унікального коду, надісланого на ваш мобільний пристрій, перед наданням доступу до облікового запису. Навіть якщо зловмисникові вдасться отримати ваші облікові дані для входу, йому все одно знадобиться додаткова перевірка, щоб отримати доступ.

Регулярно оновлюйте прошивку та програмне забезпечення: Оновлюйте пристрої, програми та прошивку вашого розумного будинку найновішими виправленнями безпеки. Виробники часто випускають оновлення, які усувають

вразливості та підвищують безпеку системи. Регулярно перевіряйте наявність оновлень і своєчасно застосовуйте їх, щоб зменшити ризик експлуатації.

Захистіть свою мережу Wi-Fi: Захистіть домашню мережу Wi-Fi, використовуючи надійне шифрування (WPA2 або вище) та унікальний складний пароль. Змініть ім'я мережі за замовчуванням (SSID) і вимкніть функції віддаленого керування, щоб запобігти несанкціонованому доступу до вашої мережі та пристроїв.

Будьте обережні з підозрілими повідомленнями: Будьте обережні при отриманні небажаних електронних листів, телефонних дзвінків або повідомлень, які запитують конфіденційну інформацію або спонукають до негайних дій. Остерігайтеся несподіваних повідомлень про призи, термінових запитів на надання особистої інформації або пропозицій, які здаються занадто хорошими, щоб бути правдою. Завжди самостійно перевіряйте легітимність таких повідомлень за допомогою перевірених каналів.

Переглядайте дозволи додатків: Регулярно переглядайте та коригуйте дозволи, надані додаткам, пов'язаним з пристроями вашого розумного будинку. Обмежуйте непотрібний доступ до особистої інформації та функцій. Пам'ятайте про дані, які збирають додатки, і враховуйте репутацію та практику безпеки розробників додатків, перш ніж надавати їм дозволи.

Заходи фізичної безпеки: Захистіть фізичний доступ до пристроїв вашого розумного будинку, убезпечивши свій будинок і переконавшись, що сторонні особи не можуть отримати фізичний доступ до ваших пристроїв. Встановіть системи безпеки, використовуйте надійні замки і подумайте про відеоспостереження, щоб відлякувати потенційних зловмисників.

Регулярний моніторинг та аудит: Регулярно відстежуйте пристрої розумного будинку та пов'язані з ними облікові записи на предмет будь-якої незвичної активності або несанкціонованого доступу. Переглядайте журнали активності, налаштовуйте сповіщення про підозрілу поведінку та оперативно розслідуйте будь-які аномалії. Регулярно проводьте аудит і видаляйте з мережі невикористовувані пристрої або облікові записи.

Висновки за розділом 2

Застосування технології Інтернету речей у розумних будинках відкриває як нові можливості, так і ризики для безпеки. Розумні будинки на основі Інтернету речей розумні будинки дуже вразливі до різних загроз безпеці як зсередини, так і ззовні. Якщо безпека розумного будинку або розумного пристрою буде порушена, під загрозою опиняться конфіденційність користувача, його особиста інформація і навіть безпека користувача опиняться під загрозою. Тому необхідно вжити відповідних заходів, щоб зробити розумні будинки більш безпечними і придатними для життя.

Застосунки, які використовуються для керування системами «розумного будинку», також стикаються зі значними проблемами безпеки. Багато з цих застосунків мають вразливості, які можуть бути використані зловмисниками для зламу інформації. Недостатні заходи захисту, незашифровані з'єднання і неналежне управління доступом можуть піддати ризику конфіденційні дані користувачів. Це ставить під загрозу приватність і безпеку власників «розумних будинків».

Ретельна оцінка ризиків безпеки повинна передувати будь-якому впровадженню системи безпеки, щоб гарантувати, що спочатку будуть виявлені всі відповідні проблеми, що лежать в її основі.

У цій роботі була успішно проведена комплексна оцінка ризиків безпеки з використанням методу OCTAVE. Як результат дослідження було виявлено приблизно 15 ризиків для безпеки, що походять як зсередини, так і ззовні розумних будинків.

Наслідки або вплив цих ризиків були описані, виходячи з припущення, що загрози реалізуються. Були запропоновані відповідні контрзаходи для зниження ризиків до прийнятного рівня.

Це дослідження було зосереджене виключно на виявленні загроз безпеці, їхніх наслідків або ризиків, а також відповідних контрзаходів для розумних будинків на основі Інтернет речей.

РОЗДІЛ 3

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ В СЕРЕДОВИЩІ РОЗУМНОГО БУДИНКУ З УРАХУВАННЯМ ОЦІНКИ РИЗИКІВ

3.1 Оцінка ризиків методикою компанії Microsoft

В цій роботі ми будемо визначати термін «загроза інформаційній безпеці» як сукупність обставин і факторів, що створюють потенційну небезпеку порушення безпеки інформації. Вразливість — властива інформаційним системам властивість, яка впливає на ймовірність того, що загрози безпеці інформації, що обробляється, стануть реальністю.

Базові загрози інформаційній безпеці розумного будинку:

- порушення конфіденційності
- порушення цілісності
- порушення доступності

В межах теми «розумних будинків» під конфіденційністю інформації розумітимемо стан управління системами «розумного будинку, при якому відсутня можливість витоку інформації через підсистеми.

Цілісність інформації означає точність і повноту даних, зібраних системою з різних встановлених датчиків і пристроїв. Наприклад, у ситуаціях, коли отримано неправильний сигнал щодо присутності людини в кімнаті, це може призвести до помилкового спрацьовування системи контролю доступу.

Доступність інформації - це стан інформації або ресурсів IT-системи, при якому суб'єкти або сама система, що мають права доступу, можуть реалізувати різні дії відповідно до сценарію роботи (вимикати / вмикати датчики, відкривати замки і т.д .). Приклад реалізації даної загрози - виведення з ладу комунікаційного обладнання системи.

За природою виникнення загрози інформаційній безпеці прийняти розділяти на штучні та природні.

До природних відносять загрози, які викликані впливом на інформаційне середовище природних явищ або фізичних процесів без участі людини.

Штучні же в свій час поділяються на ненавмисні і навмисні. Навмисні загрози в основному пов'язані з умисними погрозами, оскільки вони є найчастішою причиною злочинів і правопорушень. Прикладами ненавмисних помилок є помилки програмного забезпечення та персоналу, збої в системі, збої в комп'ютерному та комунікаційному обладнанні, серед інших подібних інцидентів.

Спосіб реалізації виділяє саме загрози першої групи.

Умисні дії мають цілеспрямований характер.

«Ненавмисне» — синонім «випадкового».

У таблиці наведено кілька ілюстрацій вищезазначених небезпек у розділі 3.1. Важливо визнати, що екологічні загрози другої категорії неможливо передбачити, і вони зазвичай включають природні катаклізми.

Таблиця 3.1

Класифікація загроз безпеки інформації в межах систем розумних будинків

Цілеспрямовані	Випадкові	Загрози середовища
Модифікація інформації	Помилки ПО	Пожежа
Розкрадання обладнання	Помилки при обслуговуванні	Блискавка
Хакерська атака	Апаратні відмови	Землетрус
Шкідливе програмне забезпечення (ПО)	Помилки маршрутизації	Екстремальні величини температури і вологості
Перехоплення інформації	Помилки користувача	Затоплення

Основне занепокоєння щодо IT-систем у розумних будинках — потенційні загрози інформаційній безпеці. На ідентифікацію потенційної небезпеки впливає конструкція пристрою. Це життєво важливий аспект оцінки ймовірності небезпеки.

Найбільш вірогідний аспект, який ми розглянемо, це безпека інформації в розумному будинку.

Підхід Microsoft до оцінки ризиків передбачає використання методології оцінки ризиків. Для цього складемо зведену таблицю, в якій оцінимо:

- ймовірність реалізації загрози виходячи з частоти її реалізації за певний період, де висока - ймовірність реалізації однієї або декількох загроз в межах року, середня - виникнення загрози в межах 2-3 років, і низька – малоймовірна поява загрози в межах 4 років;
- рівень схильності впливу, за наступною шкалою: високий – велика кількість збитків для активу, середній - середній або обмежений збиток, низький – невеликий збиток (або його повна відсутність);
- клас активу, за наступною шкалою: високий – вплив на КЦД

Таблиця 3.2

Рівень ризику для загроз розумного будинку

Загроза	Імовірність реалізації	Рівень схильності впливу	Клас активу	Рівень ризику
Атаки на центральний сервер	Висока	Високий	Високий	Високий
Впровадження шкідливого коду	Висока	Високий	Високий	Високий
Атаки соціальної інженерії	Висока	Середній	Середній	Високий
Помилки користувача	Середня	Середній	Середній	Середній

Продовження таблиці 3.2

Рівень ризику для загроз розумного будинку

Доступ до мережі нелегітимних користувачів	Висока	Середній	Середній	Середній
Використання механізмів розробника	Висока	Високий	Середній	Високий
Доступ до захищених файлів з середини компанії	Висока	Середній	Середній	Висока
Відключення контрольних датчиків	Висока	Середній	Середній	Високий
Подолання фізичного захисту об'єкта	Середня	Високий	Високий	Високий
Крадіжка апаратури або носіїв інформації	Середня	Високий	Високий	Висока
Знищення апаратури або носіїв інформації	Середня	Високий	Високий	Середній
Стихійні лиха	Низька	Середній	Високий	Середній

Ґрунтуючись на результатах оцінки ризиків, найбільш небезпечними загрозами є:

- атаки на центральний сервер;
- впровадження шкідливого коду або програми;
- атаки соціальної інженерії;
- крадіжка апаратури або носіїв інформації;
- доступ до захищених файлів з середини компанії;
- подолання фізичного захисту об'єкта.

Існують значні небезпеки, пов’язані з потенційними несправностями в системах електропостачання, а також потенційними помилками користувачів або програмного забезпечення. Тому необхідно вжити захисних заходів, щоб зменшити ризики, пов’язані з цими загрозами. Для мінімізації таких ризиків необхідно вжити наступних заходів:

- впроваджується використання механізмів ідентифікації та аутентифікації користувачів.
- необхідно впровадження механізмів шифрування та заходів для забезпечення цілісності даних, що передаються.
- рекомендується використовувати антивірусне програмне забезпечення.
- система контролю доступу вимагає ретельної організації та планування.
- використання механізмів розподілу навантажень.
- необхідно регулярно перевіряти роботу всіх компонентів системи.
- включення додаткового джерела живлення для цілей резервного живлення.

Щоб захистити користувачів від атак соціальної інженерії, можна вжити наступні заходи:

- Навчання свідомості: Надати користувачам інформацію про потенційні загрози соціальної інженерії та навчити їх розпізнавати ознаки шахрайства. Це можна зробити шляхом проведення тренінгів, семінарів або надання інструкцій.
- Посилення інформаційної безпеки: Налагодити політику безпеки, яка включатиме в себе вимоги щодо сильних паролів, двофакторної автентифікації та

обмеження прав доступу. Також рекомендується нагадувати користувачам про регулярну зміну паролів та уникання використання одного пароля для кількох облікових записів.

- Перевірка ідентифікації: Вимагати додаткову перевірку ідентифікації перед розголошенням чутливої інформації або здійсненням фінансових операцій. Це може включати використання підтвердження через SMS, вводу додаткового коду або відбитка пальця.

Підозрілі ланки та вкладення: Навчити користувачів не клікати на посилання в непідтверджених електронних листах або не відкривати вкладення з незнайомих джерел. Рекомендується використовувати антивірусне програмне забезпечення та спам-фільтри, щоб запобігти отриманню шкідливих повідомлень.

3.2 Розробка програмного забезпечення для навчання користувачів систем розумного будинку протидії атак соціальної інженерії

Як ми бачимо з попереднього розділу одними із найбільших ризиків є атаки соціальної інженерії спрямовані на співробітників, які відповідають за системами розумного будинку, або на користувачів які мають доступ до системи.

Тому я пропоную запровадити програму для навчання і тестування користувачів, які хочуть отримати доступ до систем розумного будинку.

Програму я буди писати на python і для цього потрібно для початку встановити потрібну бібліотеку python-pptx. Для роботи з презентаціями, процес встановлення представлений на рисунок 3.1.

```
C:\Users\MSI>pip install python-pptx
Collecting python-pptx
  Downloading python-pptx-0.6.21.tar.gz (10.1 MB)
     |████████████████████████████████| 10.1 MB 3.3 MB/s
Collecting lxml>=3.1.0
  Downloading lxml-4.9.2-cp39-cp39-win_amd64.whl (3.9 MB)
     |████████████████████████████████| 3.9 MB ...
Requirement already satisfied: Pillow>=3.3.2 in c:\python39\lib\site-packages (from python-pptx) (8.3.1)
Collecting XlsxWriter>=0.5.7
  Downloading XlsxWriter-3.1.2-py3-none-any.whl (153 kB)
     |████████████████████████████████| 153 kB 6.4 MB/s
Using legacy 'setup.py install' for python-pptx, since package 'wheel' is not installed.
Installing collected packages: XlsxWriter, lxml, python-pptx
    Running setup.py install for python-pptx ... done
Successfully installed XlsxWriter-3.1.2 lxml-4.9.2 python-pptx-0.6.21
WARNING: You are using pip version 21.1.3; however, version 23.1.2 is available.
You should consider upgrading via the 'c:\python39\python.exe -m pip install --upgrade pip' command.
```

Рисунок 3.1 - Встановлення бібліотеки python-pptx.

Для того щоб після запуску роботи програму одразу відкривалась презентація з навчальним матеріалом додам функцію open_presentation, як представлено на рисунку 3.2.

```python
import random
import os
import subprocess

# Функція для відкриття презентації
def open_presentation():
    try:
        subprocess.call(["start", "C:\\Users\\MSI\\Desktop\\Соціальнаінженерія.pptx"], shell=True)
    except Exception as e:
```

Рисунок 3.2 - Функція для відкриття презентації.

Спробую реалізувати генерації тестових запитань на основі заданого тексту. Для цього я знайшов на просторах інтернету API, який може це зробити. Реєструюсь на їхньому сайті для того щоб отримати ім’я хосту і ключ до нього. І додаю ключ до програмного коду, як представлено на рисунку 3.3.

temp.py 1.py

```python
import requests

url = "https://prepai-generate-questions.p.rapidapi.com/getQuestions"

payload = {
  "topic": "Make Money in Stock Market",
  "content": "Making money in the stock market is not as complicated or r
}
headers = {
  "content-type": "application/x-www-form-urlencoded",
  "X-RapidAPI-Key": "5535c88dddmsh0ea324057476ca3p1afb66jsnc5e3302c3f6a",
  "X-RapidAPI-Host": "prepai-generate-questions.p.rapidapi.com"
}

response = requests.post(url, data=payload, headers=headers)

print(response.json())
```

Рисунок 3.3 - Програма для генерації тестових запитань.

Нажаль програма генерує лише текст англійською мовою і в незручному для подальшого використання форматі, як видно на рисунку 3.4. А подібні їй аналоги доступні лише з платними підписками.

```
In [8]: runfile('C:/Users/MSI/.spyder-py3/temp.py', wdir='C:/Users/MSI/.spyder-py3')
{'code': 200, 'message': 'Questions generated successfully.', 'response': [{'topic': 'Make Money in Stock Market',
'category_type': 5, 'question': ['Ques  : What is perceived to be simpler and less risky than many people assume?'],
'options': [' Making money in the stock market'], 'help_text': 'Making money in the stock market is not as complicated or
risky as many people think.'}, {'topic': 'Make Money in Stock Market', 'category_type': 5, 'question': ['Ques  : What should
be known about a company before investing in it?'], 'options': [' Financial statements, the competitive landscape, the
company s management, and the risks involved'], 'help_text': 'This includes understanding the financial statements, the
competitive landscape, the company s management, and the risks involved.'}, {'topic': 'Make Money in Stock Market',
'category_type': 1, 'question': ['Ques  : What is perceived to be simpler and less risky than many people assume?'],
'options': [' Making money in the stock market *', ' Taking risks', ' Trading stocks', ' Investing in the stock market'],
'help_text': 'Making money in the stock market is not as complicated or risky as many people think.'}, {'topic': 'Make Money
in Stock Market', 'category_type': 2, 'question': ['Ques  : What is perceived to be simpler and less risky than many people
assume?', ' I. Making money in the stock market ', ' II. Taking risks', ' III. Investing in the stock market', ' IV. Trading
stocks', 'Which of the options given above is/are correct:'], 'options': [' I only.*', ' IV only.', ' III and II only.', '
I, III and II only.'], 'help_text': 'Making money in the stock market is not as complicated or risky as many people
think.'}, {'topic': 'Make Money in Stock Market', 'category_type': 4, 'question': ['Ques  : Making money in the stock market
is perceived to be simpler and less risky than many people assume.'], 'options': [' True*', '  False'], 'help_text': 'Making
money in the stock market is not as complicated or risky as many people think.'}, {'topic': 'Make Money in Stock Market',
'category_type': 4, 'question': ['Ques  : Read the following statements carefully:', ' Statement I:  Investing in the stock
market is perceived to be simpler and less risky than many people assume.', ' Statement II: Making money in the stock market
```

Рисунок 3.4 - Результат генерації тестових питань через програму.

Оскільки в мене не вийшло за допомогою програмного коду згенерувати потрібний меті формат запитань. Я скористаюсь сайтом для створення тестових запитань на основі тексту, як показано на рисунку 3.5.

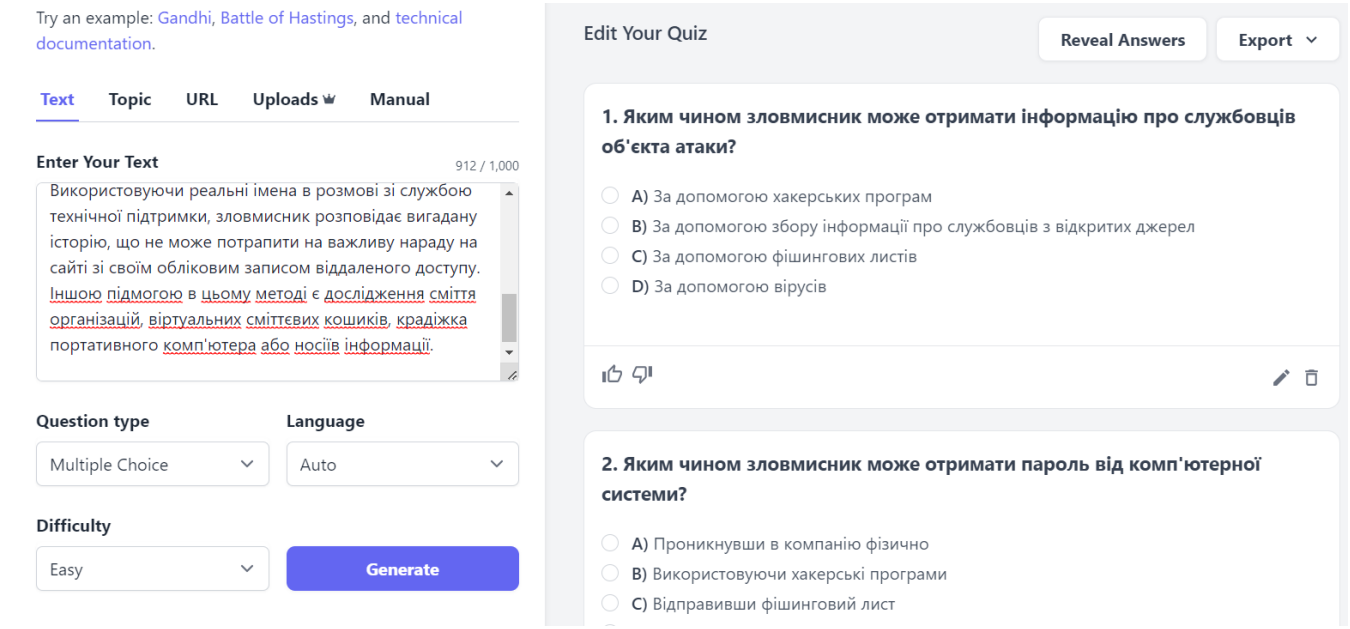

Рисунок 3.5 - Результат генерації тестових питань через сайт.

Далі додам ці питання в код моєї програми для тестування, як видно на рисунку 3.6.

```
# Тестові питання та відповіді
questions = [
    {
        'question': 'Яка важливість розуміння та застосування основних принципів безпеки в "розумному
        'answers': ['Немає значення', 'Це допомагає запобігти потенційним загрозам', 'Це робить систе
        'correct_answer': 2
    },
    {
        'question': 'Які рекомендації щодо створення надійних паролів ви можете навести?',
        'answers': ['Використовуйте прості паролі', 'Використовуйте унікальні та складні паролі', 'Па
        'correct_answer': 1
    },
    {
        'question': 'Який метод захисту безпроводової мережі може бути використаний для запобігання н
        'answers': ['Шифрування Wi-Fi', 'Використання сильних паролів', 'Відключення мережі'],
        'correct_answer': 2
    },
    {
        'question': 'Чому важливо оновлювати програмне забезпечення пристроїв "розумного" будинку?',
        'answers': ['Не має значення', 'Оновлення поліпшує функціональність пристроїв',
                    'Оновлення виправляє вразливості та забезпечує безпеку'],
        'correct_answer': 2
    },
    {
        'question': 'Які налаштування можна використовувати для збереження конфіденційності особистих
        'answers': ['Встановлення паролів на пристрої', 'Обмеження доступу до особистих даних',
```

Рисунок 3.6 - Вигляд згенерованих питань в програмі для тестування.

Додам в код перемішування порядку питань і варіантів відповіді, як видно на рисунку 3.7. Це потрібно для того щоб користувач при повторному проходженні не міг просто відтворити попередні відповіді.

```
# Функція для перемішування варіантів відповіді
def shuffle_answers(answers):
    random.shuffle(answers)
    return answers

def run_test():
    score = 0
    random.shuffle(questions)
```

Рисунок 3.7 - Цей рядок змішує порядок елементів у списку questions, тобто перемішує питання перед кожним новим проходженням тесту.

Тепер повернемося до головної ідеї цієї програми. Я хотів реалізувати програму, яка спочатку відкриває навчальний матеріал про соціальну інженерії для ознайомлення і одразу запускає згенеровані за допомогою штучного інтелекту тестові запитанні. Всього програма генерує 5 тестових запитань. Для успішного проходження потрібно набрати більше 4 тестових балів. У разі успішного складання програма надає користувачу доступ до розумного будинку у вигляді логіну і паролю до системи. У разі неуспішного складання програма запропонує вам пройти тест ще раз. Результат реалізації даного рішення наведено на рисунках 3.8-3.10.

```
In [1]: runfile('C:/Users/MSI/.spyder-py3/temp.py', wdir='C:/Users/MSI/.spyder-py3')
Питання 1: Чому важливо оновлювати програмне забезпечення пристроїв "розумного" будинку?
1. Оновлення виправляє вразливості та забезпечує безпеку
2. Не має значення
3. Оновлення поліпшує функціональність пристроїв
Виберіть відповідь (введіть номер варіанту): 1
Неправильна відповідь!

Питання 2: Які рекомендації щодо створення надійних паролів ви можете навести?
1. Паролі не важливі
2. Використовуйте унікальні та складні паролі
3. Використовуйте прості паролі
Виберіть відповідь (введіть номер варіанту): 1
Правильна відповідь!

Питання 3: Яка важливість розуміння та застосування основних принципів безпеки в
"розумному" будинку?
1. Немає значення
2. Це допомагає запобігти потенційним загрозам
3. Це робить систему повільнішою
Виберіть відповідь (введіть номер варіанту): 1
Неправильна відповідь!

Питання 4: Який метод захисту безпроводової мережі може бути використаний для запобігання
несанкціонованому доступу?
```

Рисунок 3.8 - Вивід тестових запитань на екран.

```
Ваш результат: 2/5
Ви не пройшли тест успішно.
Бажаєте спробувати знову? (так/ні):
```

Рисунок 3.9 - Результат виконання програми при неуспішному проходженні тесту.

```
Виберіть відповідь (введіть номер варіанту): 1
Правильна відповідь!

Ваш результат: 5/5
Вітаємо! Ви пройшли тест успішно.
login:admin, password:qwerty123
```

Рисунок 3.10 - Результат виконання програми при успішному проходженні тесту.

Висновки за розділом 3

На основі результатів оцінки ризиків була розроблена програма, яка поєднує навчальний матеріал про соціальну інженерію та тестування користувачів. Програма спочатку відкриває навчальний матеріал, який допомагає ознайомитись з основами соціальної інженерії та розуміти її потенційні загрози. Після цього програма автоматично генерує тестові запитання, які перевіряють розуміння користувача на предмет соціальної інженерії.

Для успішного проходження тесту користувачеві потрібно набрати задану кількість тестових балів. Це створює вимогу до користувачів мати достатні знання та розуміння, щоб ефективно захищатись від атак соціальної інженерії. У разі успішного складання тесту програма надає користувачу доступ до розумного будинку, представляючи логін та пароль до системи.

У випадку, якщо користувач не успішно складає тест, програма пропонує йому пройти тест знову. Це надає можливість користувачам покращити свої знання та вміння в галузі соціальної інженерії та підвищити рівень своєї безпеки.

Цей підхід з навчання та тестування також дозволяє запобігти знаходженню в системі користувачів, які можуть стати жертвами атак соціальної інженерії.

Програма допомагає користувачам вчасно розпізнати спробу атаки соціальної інженерії, розуміти підвищений ризик психологічного маніпулювання та уникати небажаних дій, що можуть призвести до компрометації безпеки системи розумного будинку. Це сприяє підвищенню свідомості користувачів і допомагає їм приймати обґрунтовані рішення, що знижує ймовірність потрапляння під вплив атак соціальної інженерії.

Загалом, поєднання навчання, тестування та свідомого підходу до захисту від атак соціальної інженерії дозволяє зберегти безпеку та конфіденційність користувачів системи розумного будинку, уникнути потенційних проблем та зберегти їх приватні дані та ресурси в безпеці.

ВИСНОВКИ

У ході дипломної роботи було проведено дослідження основних елементів системи розумного будинку. Розглянуто історію виникнення таких систем, а також вивчено основні підсистеми та протоколи зв'язку, що використовуються в сучасних розумних будинках. Були розглянуті напрямки прогресу, спрямовані на поліпшення функціональності та зручності використання систем розумних будинків.

Однак, разом із зростанням популярності систем розумних будинків зростає й ризик кібератак на такі системи. В розділі про випадки кібератак були розглянуті приклади реальних інцидентів, які відбулися з системами розумного будинку. Такі атаки можуть мати серйозні наслідки, зокрема, компрометацію безпеки житлових приміщень, доступ до приватної інформації та порушення приватності користувачів.

Проблеми з безпекою в застосунках розумних будинків є однією з найбільш актуальних тем сьогодення. У розділі про проблеми з безпекою було розглянуто вразливості та ризики, пов'язані з використанням систем розумних будинків. Зокрема, були висвітлені питання недостатньої захищеності мережі, слабких паролів та недостатньої уваги до приватності та захисту особистих даних користувачів.

З метою запобігання ризикам інформаційної безпеки в системах розумного будинку була розроблена програма, яка спочатку надає навчальний матеріал про соціальну інженерію для ознайомлення користувачів з цим типом атак. Після цього програма автоматично запускає тестові запитання, згенеровані за допомогою штучного інтелекту. У разі успішного складання тесту програма надає користувачу доступ до системи розумного будинку за допомогою логіна і пароля. У разі невдалого проходження тесту програма запропонує здати його ще раз.

Застосування цієї програми дозволяє ефективно навчити користувачів розпізнавати та уникати атак соціальної інженерії, тим самим запобігаючи потенційному потраплянню в систему розумного будинку шкідливих елементів, що можуть завдати шкоди безпеці та конфіденційності. Це сприяє забезпеченню безпеки користувачів та збереженню їх приватної інформації та ресурсів.

Отже, на основі проведених досліджень можна зробити висновок, що зростання популярності систем розумного будинку потребує посилення заходів забезпечення інформаційної безпеки. Програми, спрямовані на навчання та свідоме управління ризиками, є важливим кроком у забезпеченні безпеки користувачів. Такий підхід дозволяє підвищити обізнаність користувачів, розпізнавати загрози та приймати обґрунтовані рішення, забезпечуючи безпеку, приватність та надійність систем розумного будинку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Моделювання розумного будинку в середовищі Cisco Packet Tracer – Київ: Хома В.В., Кеньо Г.В., 2018.

2. Проектування систем автоматизації – Київ: В.Г. Трегуб, 2015

3. Що таке розумний будинок і навіщо він потрібен? [Електронний ресурс] // stylus.ua – Режим доступу до ресурсу: https://stylus.ua/uk/articles/528.html.

4. Home Automation & Wiring 1st Edition – 1999. – 322 с.

5. Система автоматизації роботи інженерних систем та окремих приладів будинку [Електронний ресурс] // domos.ua/. – 2019. – Режим доступу до ресурсу: https://domos.ua/.

6. Що таке розумний будинок: функції, види, складові та екосистеми [Електронний ресурс] // ek.ua. – 2018. – Режим доступу до ресурсу: https://ek.ua/ua/post/1990/618-chto-takoe-umnyy-dom-funkcii-vidy-sostavlyayuschie-i-ekosistemy/.

7. Єрохін С. Д. Штучний інтелект для інформаційної безпеки. В:2020 Системи генерування та обробки сигналів у сфері бортового зв'язку. IEEE, 2020.с.1-4.

8. Системи безпеки розумного будинку [Електронний ресурс] // exposervice. – 2020. – Режим доступу до ресурсу: https://exposervice-p.com.ua/sistemi-bezpeki-rozumnogo-budinku/ .

9. Smart speaker ownership hit 60M US adults [Електронний ресурс] // Marketing Dive. – 2019. – Режим доступу до ресурсу: https://www.marketingdive.com/news/smart-speaker-ownership-hit-60m-us-adults-in-2019/570186/.

10. Enabling Applicability of Energy Saving Applications on the Appliances of the Home Environment [Електронний ресурс] // Spyridwn Tombros, Nikolaos Mouratidis, Maurice Draaijer, Andreas Foglar. – 2010. – Режим доступу до ресурсу: https://www.researchgate.net/publication/224088473_Enabling_Applicability_of_Energy_Saving_Applications_on_the_Appliances_of_the_Home_Environment.

11. Performance analysis for ZigBee under WiFi interference in smart home [Електронний ресурс] // Haoran Jiang, Bin Liu, Chang Wen Chen. – 2017. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7997161.

12. A Novel Secure IoT-based Smart Home Automation System using a Wireless Sensor Network, 2016.

13. Secure biometric template generation for multi-factor authentication [Електронний ресурс] // Salman H. Khan a, M. Ali Akbar b, Farrukh Shahzad b, Mudassar Farooq b, Zeashan Khan c. – 2015. – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/abs/pii/S0031320314003392.

14. SPE: Security and Privacy Enhancement Framework for Mobile Devices [Електронний ресурс] // Brian Krupp, Nigamanth Sridhar;, Wenbing Zhao. – 2017. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7182290.

15. Computer Security: Principles and Practice – New York: Stallings, W., Brown, L, 2014.

16. Fast Fingerprint Orientation Field Estimation Incorporating General Purpose GPU. In Soft Computing Applications; Advances in Intelligent Systems and Computing; Balas – Switzerland: Awad, A.I., 2016. – 891 c.

17. Smart Home Definition and Security Threats. In Proceedings of the 2015 Ninth International Conference on IT Security Incident Management IT Forensics – Magdeburg, Germany: Schiefer, M., 2015. – 114 c.

18. Challenges in Middleware Solutions for the Internet of Things. In Proceedings of the 2012 International Conference on Collaboration Technologies and Systems – Denver, CO, USA: Chaqfeh, M.A.; Mohamed, N, 2012. – 21 c.

19. Дзекунов М.А., Щебланін Ю.М. Аналіз алгоритму X-10, як найпоширенішої технології реалізації розумного будинку / Ю.М. Щебланін, М.А. Дзекунов // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 27-28 жовтня 2022 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко. (голова) та ін. –К.: ВПЦ "Київський університет", 2022. – С.122-123.

ДОДАТОК А
ЛІСТИНГ ПРОГРАМИ

```
import random
import os
import subprocess

# Функція для відкриття презентації
def open_presentation():
    try:
        subprocess.call(["start", "C:\\Users\\MSI\\Desktop\\Соціальнаінженерія.pptx"], shell=True)
    except Exception as e:
        print("Не вдалося відкрити презентацію. Перевірте, чи є файл presentation.pptx в поточній папці.")
        print(f"Помилка: {str(e)}")

# Тестові питання та відповіді
questions = [
    {
        'question': 'Яка важливість розуміння та застосування основних принципів безпеки в "розумному" будинку?',
        'answers': ['Немає значення', 'Це допомагає запобігти потенційним загрозам', 'Це робить систему повільнішою'],
        'correct_answer': 2
    },
    {
        'question': 'Які рекомендації щодо створення надійних паролів ви можете навести?',
        'answers': ['Використовуйте прості паролі', 'Використовуйте унікальні та складні паролі', 'Паролі не важливі'],
```

```
            'correct_answer': 1
        },
        {
            'question': 'Який метод захисту безпроводової мережі може бути використаний для запобігання несанкціонованому доступу?',
            'answers': ['Шифрування Wi-Fi', 'Використання сильних паролів', 'Відключення мережі'],
            'correct_answer': 1
        },
        {
            'question': 'Чому важливо оновлювати програмне забезпечення пристроїв "розумного" будинку?',
            'answers': ['Не має значення', 'Оновлення поліпшує функціональність пристроїв',
                        'Оновлення виправляє вразливості та забезпечує безпеку'],
            'correct_answer': 2
        },
        {
            'question': 'Які налаштування можна використовувати для збереження конфіденційності особистих даних?',
            'answers': ['Встановлення паролів на пристрої', 'Обмеження доступу до особистих даних',
                        'Видалення всіх даних'],
            'correct_answer': 1
        }
    ]

    # Функція для перемішування варіантів відповіді
    def shuffle_answers(answers):
        random.shuffle(answers)
```

```
    return answers

# Функція для проведення тестування
def run_test():
    score = 0
    random.shuffle(questions)

    for index, question in enumerate(questions, start=1):
        print(f"Питання {index}: {question['question']}")
        answers = shuffle_answers(question['answers'])
        for i, answer in enumerate(answers, start=1):
            print(f"{i}. {answer}")

        user_answer = int(input("Виберіть відповідь (введіть номер варіанту): "))

        if user_answer == question['correct_answer']:
            score += 1
            print("Правильна відповідь!")
        else:
            print("Неправильна відповідь!")

        print()

    print(f"Ваш результат: {score}/{len(questions)}")

    if score >= 4:
        print("Вітаємо! Ви пройшли тест успішно.")
        print("login:admin, password:qwerty123")
    else:
        print("Ви не пройшли тест успішно.")
```

```
        retry = input("Бажаєте спробувати знову? (так/ні): ")
        if retry.lower() == "так":
            run_test()

# Головна функція
def main():
    open_presentation()
    run_test()

# Виклик головної функції
main()
```