МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ім. Ю.М. ПОТЕБНІ

Кафедра мікроелектронних та електронних інформаційних систем
(повна назва кафедри)

Кваліфікаційна робота

другий (магістерський)
(рівень вищої освіти)

на тему Дослідження безпеки систем розумного будинку

Виконав: студент II курсу, групи 8.1710
спеціальності 171 «Електроніка»
(код і назва спеціальності)
освітньої програми Електроніка
(код і назва освітньої програми)
спеціалізації _____
(код і назва спеціалізації)

_____
(ініціали та прізвище)

Керівник к.т.н., доцент Шмалій С.Л.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Рецензент заступник директора п.п. ЖВКФ „Екотех" Шершов С.А.
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Запоріжжя
2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІНЖЕНЕРНИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ім. Ю.М. ПОТЕБНІ

Кафедра мікроелектронних та електронних інформаційних систем
Рівень вищої освіти другий (магістерський)
Спеціальність 171 «Електроніка»
(код і назва)
Освітня програма Електроніка
(код і назва)
Спеціалізація

ЗАТВЕРДЖУЮ
Завідувач кафедри Критська Т.В.
"____" _____ 2021 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТОВІ (СТУДЕНТЦІ)

Панченко Тетяні Павлівни
(прізвище, ім'я, по батькові)

1 Тема роботи (проєкту) Дослідження безпеки систем розумного будинку

керівник роботи к.т.н., доцент Шмалій С.Л.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ЗНУ від "30" 06 2021 року № 974-С

2 Строк подання студентом роботи

3 Вихідні дані до роботи напруга 220 В, модуль Wi-Fi, Bluetooth 2,4 ГГц, 5 ГГц, локальна мережа, Модуль дистанційного керування.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Системи домашньої автоматизації. Основні характеристики безпеки систем розумного будинку. 2 Дослідження шляхів запобігання загрозам безпеки систем розумного будинку. 3 Функції щодо шляхів запобігання загрозам безпеки систем РБ. 4. Методики підходи та критерії вибору параметрів безпеки системи РБ. 5. Економічне дослідження. 6. Охорона праці та Техніка Безпеки на виробництві.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

1. Схематичне зображення системи розумного будинку.
2. Перелік загроз, вразливостей та можливих наслідків в системах розумного будинку
3. Схема передачі даних в системах розумного будинку
4. Схема ієрархії" будинки в системах розумного будинку
5. Розрахунок найбезпечнішої системи розумного будинку
6. Розрахунок економічних показників. 7. Здійснювальний пристрій
8. Схема електрична структурна

6 Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1.	к.т.н., доцент Шмалій С.Л.		
2.	к.т.н., доцент Шмалій С.Л.		
3.	к.т.н., доцент Шмалій С.Л.		
4.	к.т.н., доцент Шмалій С.Л.		
5.	к.т.н., доцент Шмалій С.Л.		
6.	к.т.н., доцент Шмалій С.Л.		

7 Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи магістра	Строк виконання етапів роботи	Примітка
	Розділ 1	1.06.21	
	Розділ 2	15.06.21	
	Розділ 3	20.06.21.	
	Розділ 4	30.06.21	
	Розділ 5	20.11.21	
	Розділ 6	30.11.21	

Студент _____ Панченко К.Г.
(підпис) (прізвище та ініціали)

Керівник роботи (проекту) _____ Шмалій С.Л.
(підпис) (прізвище та ініціали)

Нормоконтроль пройдено

Нормоконтролер _____ Турішев К.О.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Кваліфікаційна робота магістра: 108 сторінок, 27 рисунків, 19 таблиць, 56 наукових джерел.

Об’єкт дослідження: система безпеки розумного будинку.

Предмет Алгоритми, протоколи, схемотехнічні рішення для підвищення рівня безпеки систем розумного будинку.

Мета роботи: дослідження теоретичних засад і розробка практичних рекомендацій вибору оптимального методу забезпечення покращення безпеки систем розумного будинку.

Методи дослідження: систематизація, класифікація, порівняння, розрахунковий метод, математично-психологічний метод, прогнозування на основі факторного аналізу.

Специфіка даної роботи у вирішені актуальної проблеми пов’язаної з забезпечення безпеки, визначенням поняття та основних характеристик безпеки, у дослідженні шляхів запобігання загрозам безпеки, пропозиції щодо шляхів запобігання загрозам безпеки, запропонуванні методичних підходів та критеріїв вибору параметрів безпеки систем розумного будинку

СИСТЕМИ РОЗУМНОГО БУДИНКУ, БЕЗПЕКА, ДОСЛІДЖЕННЯ, МЕТОДИ ЗАПОБІГАННЯ ЗАГРОЗАМ, КРИТЕРІЇ БЕЗПЕКИ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БР – бажаний результат

БР - бажаний результат;

ЄС – Європейський союз;

ЗІЗ – засоби індивідуального захисту;

ЗНУ – Запорізький національний університет;

ЗП – заробітна плата;

МАІ – метод аналізу ієрархій

НАН – Національна Академія Наук

ОРВ – об’єкт, який робить вибір;

ОУ – об’єкт управління;

РБ – розумний будинок

ТБ – техніка безпеки;

API (скор. із англ. Application Programming Interface) – прикладний програмний інтерфес;

GDPR (скор. із англ. General Data Protection Regulation) – Загальноий регламент захисту даних;

GSM (скор. із англ. Global System for Mobile Communications) - глобальна система мобільного зв'язку;

IEEE (скор. із англ. Institute of Electrical and Electronics Engineers) – інститут інженерів електротехніки та лектроніки;

LAN (скор. із англ. Local Area Network) – локальна мережа;

LoRaWAN (скор. із англ. Long Range wide Area Network) - глобальна мережа далекого радіусу дії

LTE (скор. із англ. Long Term Evolution) – довготерміновий розвиток, назва мобільного протоколу передавання даних;

OSI (скор. із англ. The Open Systems Interconnection model) — модель взаємодії відкритих систем;

PLC (скор. із англ. Power Line Communication) – телекомунікаційна технологія що базується на використанні внутрішньо-будинкових і внутрішньо-квартирних електромереж для високошвидкісного інформаційного обміну;

RTLS (РТЛС) (скор. із англ. Real-time Locating Systems) - система визначення поточного розташування у реальному часі;

TKIP (скор. із англ. Temporary Key Integrity Protocol) — протокол тимчасової цілісності ключів;

VPN (скор. із англ. Virtual Private Network) - віртуальна приватна мережа;

WEP (скор. із англ. Wired Equivalent Privacy) – стандарт захисту бездротового трафіку;

WPA (скор. із англ. Wi-Fi Protected Access) – протокол безпеки для вайфаю.

ЗМІСТ

ВСТУП

Актуальність теми зумовлена популяризацією та збільшенням попиту на автоматизовані системи керування, найпоширеніші з яких – це системи розумного будинку. Проте, незважаючи на зростаючий темп впровадження даних систем в повсякденне життя, серед користувачів систем розумного будинку збільшується кількість переживань щодо забезпечення конфіденційності своїх персональних даних, та взагалі, цілісної безперебійної роботи системи без зовнішнього втручання сторонніх осіб. На сьогоднішній день системи «розумного будинку» не володіють повноцінною захищеністю від атак зловмисників та інших несанкціонованих операцій шляхом використання вразливостей систем, у зв'язку з чим виникає потреба у дослідженні цього питання.

Проблеми розробки та експлуатації систем автоматизації житлових приміщень, зокрема, розумного будинку розглядаються у працях зарубіжних та вітчизняних авторів: А.Дуднік [1], І.О. Дужак [2], С. Міхаел[3], М.Ю. Пантелеєв[4], О.В.Полякова [5], М.Е. Сопер[6], В.Н. Харке [7], Д.Федоров [8], І.О. Фурман[9], Т.Р. Елсенпітер[10] та інші. Проте питання інженерних рішень по забезпеченню безпеки систем розумного будинку досліджено недостатньо та потребує подальших наукових розвідок, що і зумовило вибір теми кваліфікаційної роботи.

Мета роботи: дослідження теоретичних засад і розробка практичних рекомендацій вибору оптимального методу забезпечення покращення безпеки систем розумного будинку.

Завдання роботи:

– визначити поняття систем розумного будинку та основні характеристики безпеки систем розумного будинку;

– дослідити шляхи запобігання загрозам безпеки систем розумного будинку;

– зробити пропозиції щодо шляхів запобігання загрозам безпеки систем розумного будинку;

– запропонувати методичні підходи та критерії вибору параметрів безпеки систем розумного будинку;

– провести економічне дослідження, розглянути загальні положення з охорони праці та техніки безпеки на виробництві, та розрахувати заземлюючий пристрій.

Об’єкт дослідження: система безпеки розумного будинку.

Предмет Алгоритми, протоколи, схемотехнічні для підвищення рівня безпеки систем розумного будинку.

Методи дослідження: систематизація, класифікація, порівняння, розрахунковий метод, математично-психологічний метод, прогнозування на основі факторного аналізу.

Наукова новизна одержаних результатів дослідження полягає в удосконалені та розвитку методичних підходів та практичних рекомендацій щодо вибору найоптимальнішого типу систем розумного будинку відносно експертної думки об’єкта, який робить вибір.

Удосконалено: методичні підходи отримання математично-психологічного результату вибору найоптимальнішого типу систем розумного будинку відносно експертної думки об’єкта, який робить вибір.

Обґрунтовано: напрямки удосконалення методичних підходів, зокрема запропоновано використання методу аналізу ієрархій, за допомогою якої можливо отримати математично-психологічний результат вибору найоптимальнішого типу систем розумного будинку відносно експертної думки об’єкта, який робить вибір

Набули подальшого розвитку запропоновані критерії вибору параметрів безпеки систем розумного будинку.

Інформаційна база дослідження. В ході дослідження використано нормативно-правові акти у сфері безпеки та кіберзлочинності, матеріали

конференцій, електроні ресурси, навчальні посібники, монографії, періодичні та аналітичні вітчизняні та зарубіжні матеріали.

Практичне значення одержаних результатів полягає у вирішені актуальної проблеми пов’язаної з забезпечення безпеки систем розумного будинку. Впровадження в практичну діяльність запропонованих інженерних рішень та критерії дозволить спростити вибір типу системи розумного будинку, здійснювати самостійне безкоштовне запобігання загрозам систем розумного будинку, та використовувати готові інженерні рішення для запобігання загрозам систем розумного будинку з точки зору інженера електронника.

Апробація результатів дослідження. Основні теоретичні та практичні положення кваліфікаційної роботи магістра були представлені та отримали позитивну оцінку на 4 науково-практичних конференціях: XXIV Науково-технічна конференція аспірантів, магістрантів, студентів та викладачів Інженерного навчально-наукового інституту ЗНУ (Запоріжжя, 2019 р.), XXIX Міжнародна наукова конференція студентів і молодих вчених. (Запоріжжя, 2020 р.), XIV Конференція студентів, аспірантів, докторантів і молодих вчених «Молода наука-2021» (Запоріжжя, 2021 р.), І Всеукраїнська науково-практична конференція здобувачів вищої освіти, аспірантів та молодих вчених «Актуальні питання сталого науково-технічного та соціального-економічного розвитку регіонів України» (Запоріжжя, 2021 р.).

1. СИСТЕМИ РОЗУМНОГО БУДИНКУ. ОСНОВНІ ХАРАКТЕРИСТИКИ БЕЗПЕКИ СИСТЕМ РОЗУМНОГО БУДИНКУ

1.1. Поняття систем розумного будинку та його головні складові

Розумний будинок (англ. smart home) – сучасний тип житлового будинку, що за допомогою високотехнологічних пристроїв та автоматизації організований для комфортного життя людей. [11]. Для визначення високотехнологічних особливостей приміщення також вживають терміни: intelligent building, smart-house, digital home. Схематичне зображення розумного будинку наведено нижче (Рис. 1.1)[12].

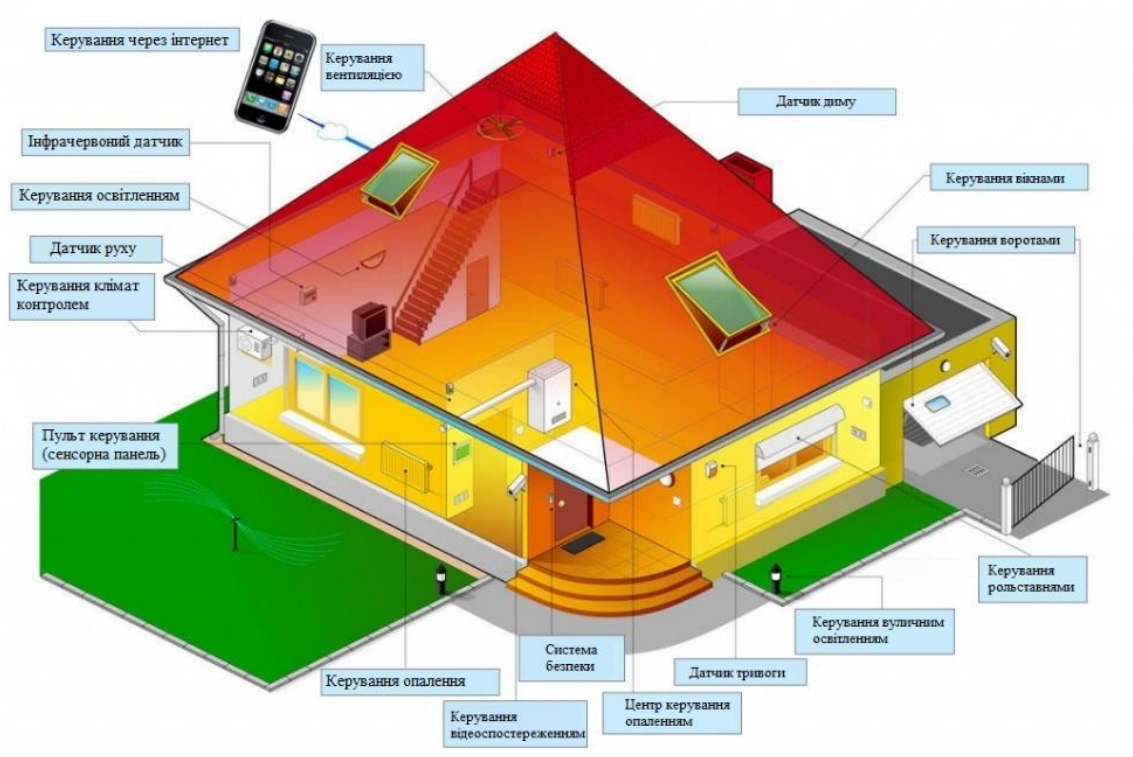

Рисунок 1.1 – Схематичне зображення системи розумного будинку

Під терміном «розумний» будинок слід розглядати систему, що може повністю забезпечити комфорт, безпеку та, звісно, ресурсозбереження для всіх користувачів.

У найпростішому вигляді вона повинна вміти розпізнавати стандартизовані ситуації, що мають місце в конкретному будинку, реагувати на них відповідним чином, наприклад: окрема система може керувати поведінкою будь-яких інших за попередньо розробленими алгоритмами [11].

«Розумний будинок» – це високоавтоматизована система, що призначена для керування компонентами інфраструктури будинка. Вона поєднує в собі високотехнологічне обладнання, що здатне перетворити звичайну кімнату в інтелектуальну, що може підлаштовуватися відповідно до настрою та бажань власника.

Суттєвою перевагою розумного будинку є те, що всі ці автоматизовані системи можна поєднати в тісно взаємодіючу автоматичну систему.

За допомогою спеціального обладнання, системою може бути розпізнано ситуації типого плану та відредаговано на них, за допомогою підключення того чи іншого компоненту. При цьому, системою розумний будинок буде повністю контролюватися робота кожного приладу і не допускатися нераціональне їх використання.

Автоматизувати можна все – освітлення, опалення, полив кімнатних рослин, систему відеоспостереження, охорони і т.і.

Наприклад, освітленням в будь-якій кімнаті є можливість керувати за допомогою: вимикача, комп'ютера, телефону, планшета, за часовою програмою, датчиком руху, датчиком відкриття дверей або будь-яким іншим зручним способом.

Елементи , що використовуються в системах розумного будинку, можна поділити умовно на три групи:

– елементи отримання інформації. До цієї групи можна віднести: датчики газу, води, руху, температури, диму, вологості, світла, яскравості, відкриття дверей, розбиття вікон та багато інших.

– елементи отримання команд. До них можна віднести пристрої, через які користувач розумного будинку передає команди розумного будинку.

Це різноманітні кнопки, вимикачі, сенсорні панелі, пристрої отримання голосових команд, персональні комп'ютери, смартфони, планшети та інше.

– виконавчі модулі. Це прилади, які виконують команди розумного будинку: релейні блоки, пристрої керування жалюзі, димери, аудіомодулі, відеомодулі, модулі передачі інфрачервоних команд.

Система розумного будинку включає три типи пристроїв:

– контролери;

– датчики або сенсори;

– актуатори.

Контролер – керуючий пристрій, що з'єднує всі елементи системи один з одним і зв'язує їх із зовнішнім світом (рис. 1.2).

Рисунок 1.2 – Зображення контролеру системи розумного будинку

Центральний контролер або «Хаб» систем розумного будинку це найголовніший приймач інформації від датчиків або сенсорів. Отриману інформацію контролер оброблює та надсилає керуючі сигнали до актуаторів.

Найбільш сучасніші контролери мають особистий «штучний інтелект». Він програмує контролер йти за певним «сценарієм», тобто виконувати певні дії, без залучань користувачів системи розумного будинку. Наявність в контролері системи розумного будинку «штучного інтелекту» дає змогу

набагато краще аналізувати вимоги та звички користувачів системи та налаштовуватися відповідно до їх персональних потреб.

Датчики та сенсори – пристрої, які отримують інформацію про зовнішні умови (рис. 1.3) [13].

Рисунок 1.3 – Зображення найпоширеніших датчиків реалізованих в системах розумний будинок

Робота систем розумного будинку заснована на комплексній роботі датчиків, які аналізують та відсліджують певні параметри навколишнього середовища. Усе це різноманіття розумних приладів умовно можна розділити на дві окремі групи:

– детектори руху або присутності;

– датчики зчитування параметрів.

Незважаючи на величезне конструкційне та функціональне різноманіття, всі датчики та сенсори функціонують за одним принципом -

передача даних на базовий контролер або керуючий модуль. Найчастіше для передачі даних використовуються системи Wi-Fi, Bluetooth, Z-Big, Z-Wave, GSM-net.

Одним з найзатребуваніших датчиків серед користувачів, на сьогоднішній дань, є – smart sockets або «розумні розетки» (рис. 1.4).

Рисунок 1.4 – Зображення датчику «Smart socket»

Головною функцією розумної розетки – є з’єднання або роз’єднання ланцюга електроживлення. Це може відбуватися як локально, тобто безпосередньо на пристрої, так і дистанційно, автоматично.

Також, окрім цієї функції, розумні розетки оснащують й іншими функціями:

– відсвіжування параметрів мережі, такі як напруга, сила струму, або навіть, температура електропроводки, тощо;

– діагностика вірогідності короткого замикання;

– ввімкнення або вимкнення приладів згідно певного заданого розкладу. Це можливо або за допомоги вмонтування таймера, або за допомогою програмування певного складного «сценарію» через базовий модуль;

– інколи влаштовують функцію електролічильника.

Нижче наведено таблицю найпопулярніших моделей розумних розеток, таблиця 1.1.

Таблиця 1.1 – Таблиця найпопулярніших моделей smart розеток

Модель	Спосіб передачі даних	Кількість каналів	Максимальна потужність	Дальність прийому сигналу
Trust APA3-1500R	Радіосигнал	3	1,5 кВт	30м
Trust AGDR-3500	Радіосигнал	6	3,5 кВт	70м
Телеметрика Т-40	GSM	4	3,5 кВт	—
ELANG PowerControl	GSM	1	2,6 кВт	—
IQSocket Mobile	GSM	1	3,5 кВт	—

Наступний датчик, який користується великим попитом серед користувачів – датчик витіку газу.

Витік газу – це не лише загроза цілісності будинку, а й життю самих володарів. Більшість датчиків витіку газу оснащено детектором виявлення метану у повітрі, який надсилає сигнал небезпеки при виявлені концентрації метану в повітрі в розмірі 3-4%. Найпоширенішими моделями датчиків витоку газу є – Rubetek KRGD13, Mijia Honeywell (рис. 1.5).

Рисунок 1.5 – Зображення датчику виявлення витоку газу «Mijia Honeywell»

Датчики руху є невід’ємною часткою системи розумного будинку, особливо для власників приватних будинків. Частіше за все, для забезпечення безпеки та ще більшої охороняємості, ці датчики використовуються разом в системами відеоспостереження розумного будинку, активуючи їх, якщо було виявлено рух на охоплюємій датчиком території.

Сучасні датчики руху оснащено спеціальними інфрачервоними сенсорами, це дозволяє запобігти «фальшивим» спрацьовуванням системи безпеки, якщо, наприклад відбувся рух фіранки через порив вітру, тощо.

В якості представника даного виду датчиків можна взяти датчик руху від компанії Xiomi, Aqara Motion Sensor (рис. 1.6).

Рисунок 1.6 – Зображення датчику руху Aqara Motion Sensor

До наступного класу датчиків, необхідних для володарів систем розумного будинку можна віднести датчики протікання води. Такі датчики здатні розпізнати потоп у ванній кімнаті, або на кухні, та вчасно відключити водопостачання. Несправність кранів, прорив у водопроводі, засмічення каналізації – все це може призвести до значних витрат на новий ремонт не тільки у вашій квартирі, але і в квартирах ваших сусідів знизу.

До бюджетних та якісних датчиків протікання води можна віднести такі – Kerui JY50001, Topvico TP-206W-3, Wofea ZC-S018, HEO COOLCAM NAS-WS01Z. На рисунку 1.7 зображено датчик протікання води Kerui JY50001.

Рисунок 1.7 – Зображення датчику протікання води «Kerui JY50001»

Для забезпечення безпеки житлового приміщення, також можна додати до системи розумний будинок датчик пожежної сигналізації, а саме датчик виявлення задимленості або датчик швидкого підвищення температури приміщення. Вони можуть оснащуватися такими елементами:

– температурне реле;

– фотоелементи, які реагують на задимленість;

– газоаналізаторами, які реагують на наявність у повітрі чадного газу.

Ось перелік датчиків пожежної сигналізації, які можна додати до системи розумний будинок – Rubetek KR-SD02, Xiaomi Mijia Honeywell, «Ростелеком» PSG01.

Нижче наведено зображення датчику пожежної сигналізації Rubetek (рис. 1.8).

Рисунок 1.8 – Зображення датчику пожежної сигналізації «Rubetek KR-SD02»

Ще один датчик, який користується найбільшим попитом серед користувачів систем розумний будинок є – датчик відкриття та закриття вікон та дверей.

Такі датчики працюють за принципом розмикання контактів при відкритті або закриті вікон. При розмиканні контактів датчик посилає «знак тривоги» на керуючий пристрій, а той в свою чергу віддає сигнали керування на актуатори.

Пристрої, залежно від набору функціональних можливостей, можуть надсилати сповіщення власнику системи розумний будинок у вигляді SMS повідомлення, або одночасно подавати сигнал працівникам охоронної організації, також отримавши повідомлення про проникнення у житлове приміщення може бути надісланий сигнал ввімкнення сирени та/або аварійного освітлення.

Датчики відкриття можна встановити на будь-які двері, віконні стулки, гаражні та вуличні ворота. До найпопулярніших моделей можна віднести наступні датчик – комплект SkyGuard RG-SK31S, Xiaomi smart mi, Invin SC-4.

Нижче наведено рисунок 1.9 – датчик відкриття вікон «Xiaomi smart mi».

Рисунок 1.9 – Зображення датчику відкриття вікон «Xiaomi smart mi»

Ще одна група датчиків без якої просто неможливо уявити сучасну систему розумного будинку – це датчики освітлення та температури. Їх головною задачею являється створення максимально комфортного мікроклімату для користувача системи розумний будинок.

Наприклад, постійна підтримка комфортної температури приміщення виконується за допомогою теплових індикаторів, які вбудовано в датчики температури. Отримуючи сигнал від теплового індикатору, система подає керуючий сигнал до обігрівача або кондиціонеру для налаштування температури навколишнього середовища. Нижче зображено датчик температури Tuya Smart Life Wi-Fi (рис. 1.10).

Рисунок 1.10 – Зображення датчику температури «Tuya Smart Life Wi-Fi»

А, ось, датчик освітленості в свою чергу окрім установлення комфортного середовища для користувача виконує й іншу функцію – функцію економії електроживлення. Якщо, наприклад, користувачі забули вимкнути світло вранці, то пристрій автоматично проаналізує рівень освітленості та вимкне надмірне світло. До таких датчиків можна віднести Xiaomi Smart Home Light Sensor (рис. 1.11).

Рисунок 1.11 – Зображення датчик освітленості «Xiaomi Smart Home Light Sensor»

Актуатори – виконавчі пристрої, які безпосередньо виконують команди. Це найчисленніша група, до яких відносяться розумні (автоматичні) сирени, клапани для труб, вимикачі та інше.

У більшості сучасних розумних будинків з’єднання контролеру з іншими пристроями системи відбувається через радіосигнали. До найпоширеніших типів сигналів передачі інформації відносять:

– Wi-Fi;
– Bluetooth.
– Z-Wave;
– Zigbee;

Найпоширеніші стандарти радіозв'язку для домашньої автоматизації – «Z-Wave» , але частота залежить від країни: в Європі – 868 МГц, а Україні – 869 МГц, «Wi-Fi» з частотою 2,4 ГГц, «ZigBee» з частотою 868 МГц або 2,4 ГГц та «Bluetooth» - також 2,4 ГГц.

Шифрування даних, що майже всі вони використовують - це «AES-128», в системах, які використовують «Wi-Fi» застосовується шифрування «WPA», «WPA2» або «WEP».

WPA - це один з протоколів безпеки, що створений для захисту бездротових мереж. Використовуэться на заміни застарілому протоколу WEP. Завдяки TKIP він ефективно вирішує проблему — повторне використання ключів шифрування, що було головною причиною вразливості WEP. Для «спілкування» із зовнішнім світом контролер, частіш за все використовує Інтернет[14].

1.2. Ланцюг системи розумного будинку. Елементи комутації.

Для вмикання, вмикання, вимикання, або перемикання елементів систем розумного будинку, для зміни параметрів елементів кола і т. п., використовується комутація ланцюга.

Комутація – це миттєва зміна параметрів електронного ланцюга. Без неї, повноцінне функціонування систем розумного будинку майже неможливе.

Під поняттям комутації ланцюга варто розглядати замикання або розмикання електричного ланцюга, а також регулювання напруги та електричного струму.

Існування системи розумного будинку (як, фактично, і іншої будь-якої електропровідної системи), не можливе без наступних елементів комутації:

– блок живлення;
– перетворювач або трансформатор;
– регулятор напруги, наприклад освітлення;
– автоматичний вимикач ;
– реле, тощо.

На рисунку 1.12 зображено елементарну блок-схему системи розумного будинку у склад якої входить контролер, елементи комутації та елементарні споживачі [15].

Рисунок 1.12 – Блок-схема елементарної системи розумного будинку

Елементи комутації, окрім основної функції, мають також функцію захисту. Наприклад, система знаходиться під мережним навантаженням занадто великим для неї, або буде ризик короткого замикання, тоді елементи комутації розімкнуть контакти, таким чином, перервавши ланцюг живлення системи і врятувавши її від руйнації.

1.3. Дослідження тенденцій впровадження цифрових технологій в житлові приміщення

Впровадження цифрових технологій або діджиталізація – це поширення використання по всьому світу електронно-цифрових пристроїв, засобів, систем та налагодження електронного та комунікаційного обміну між ними. Це фактично створює можливість інтегральної взаємодії віртуального та фізичного світів, тобто формує кіберфізичний простір [16].

З кожним днем все більше набуває популярності використання цифрових технологій в житлових приміщеннях. Система автоматизації «Розумний будинок» давно широко використовується за кордоном. На даний момент приблизно 10% домогосподарств в США і 3% домогосподарств в Європі мають встановлені системи розумного будинку, кількість яких має подвоїтися чи навіть потроїтися протягом найближчих декількох років.

Компанія Twitter спільно з Bosch провели аналіз попиту в світі на технології розумного будинку [17]. Під час дослідження було опитано 6265 респондентів з США, Іспанії, Австрії, Франції, Німеччини та Великобританії. Було з’ясовано, що приблизно дві третини відповіли, що знають, що «розумний будинок» має можливість автоматично, коли мешканці виходять, вимикати світло, але лише 22% респондентів знали, що деякі розумні кухонні прилади, такі як духова чи мікрохвильова піч можуть давати рекомендації, щодо найкращого рецепту в тому чи іншому випадку. Окрім цього, тільки 50% респондентів знали, що сьогодні системи «розумних будинків» вільно взаємодіють один з одним, не звертаючи уваги на різних виробників. За рейтингом важливості опитувані розташували аспекти можливостей систем в наступному порядку: на першому місці близько 73% респондентів відмітили економію енергії, а друге місце за важливістю зайняла безпека використання та захист даних , як вважають 59% опитаних.

Таким чином можна дослідити наступні тенденції щодо впровадження цифрових технологій в житлові будинки:

1. Інтерес споживачів до технології розумний будинок постійно зростає, а отже, у найближчий час все більше людей будуть готові впроваджувати цю систему у свої домівки;

2. Серед всіх факторів економії ресурсів споживачі віддають перевагу найменш енергозатратним системам;

3. Іншими вагомими факторами, що впливають на вибір конкретної технології smart home, є безпека, стабільність роботи та захист від витоку персональної інформації;

4. Споживачів не дуже цікавить облаштування кухні розумними побутовими приладами, вони віддають перевагу розумним вимикачам світла, бойлерам та ін.

1.4. Поняття безпеки та її значення в системах розумного будинку

Система «Розумний будинок» – це цілий комплекс, завдяки якому можна зробити проживання в будинку або квартирі максимально комфортним, а головне – безпечним. Комплекс дозволить зберегти в цілісності майно власника, а окремі компоненти зможуть зберегти життя і здоров'я мешканцям будинку або квартири.

Заплатинський В.М. доцент кафедри безпеки життєдіяльності Інституту екологічної безпеки Національного Авіаційного Університету, докторант, президент Академії безпеки та основ здоров’я, автор публікації «Логіко-детермінантні підходи до розуміння поняття «Безпека»», висунув пропозицію щодо визначення поняття безпеки, яке описано нижче.

Безпека — це конкретні умови, в яких постійно має перебувати складна система, якщо дія внутрішніх чинників та зовнішніх факторів не призводить до процесів, що можна вважати негативними у відношенні до конкретної для цього в складної системи у відповідності до потреб, уявлень та знать, що наявні на даному етапі [18].

Досліджуючи поняття ми можемо зробити висновок, про необхідні та базові функції, що повинні бути у системи «розумний будинок».

Система «розумний будинок» повинна мати автоматизовану систему, головною функцією в якій обов'язково повинно являтися забезпечення протидії негативним по відношенню до даної складної системи зовнішніх факторів і внутрішніх чинників.

До них можна віднести: фізичну доступність системи, загрози доступу, загрози інфобезпеки, доступність мережевих систем, тощо.

Інформаційна безпека – це один з найважливіших факторів забезпечення безпеки кожного, оскільки саме інформація є найбільш поширеною ціллю серед зловмисників. Для того, щоб дати повне та вірне визначення поняття «інформаційна безпека» слід звернутися до законодавства України.

Інформаційна безпека – це показник рівня захищеності найбільш важливих інтересів конкретної людини, суспільства і навіть держави, завдяки якій можна запобігти завданню шкоди через недостовірність, несвоєчасність і неповноту переданої інформації, порушенню доступу до інформації та забезпеченню її цілісності, незаконному обігу інформації з дуже лімітним доступом, а також через спланований негативний психологічний та інформаційний вплив, або будь-яке навмисне спричинення негативних проблем використання інформаційних технологій [19].

Коваленко Ю. О., який є автором публікації «Забезпечення інформаційної безпеки на підприємстві» пропонує інше визначення поняття «інформаційна безпека», що наведено нижче.

Безпека даних – це стан і рівень захисту даних, які обробляються та зберігаються, що являє собою забезпечення конфіденційності, доступності та цілісності інформації, використання та розвитку в суспільних громадських інтересах або комплекс заходів щодо захисту інформації окремих осіб або навіть держави від незаконного використання, порушення конфіденційності, знищення, модифікації, контролю, ідентифікації даних або пошкодженню її (у цьому значенні зазвичай використовується термін «захист інформації») [20].

Під інформаційною безпекою користувачі систем розумних будинків частіше за все розуміють захист конфіденційної інформації. З ростом кількості пристроїв, що потребують збору інформації, користувачі все частіше задаються питанням, як захистити свої персональні дані.

Розмови про цифрову безпеку викликають занепокоєння, адже конфіденційна інформація користувача системи може бути неправомірно використана або розкрита, щоб заподіяти їм шкоду.

Саме тому, підіймаючи тему інформаційної безпеки систем розумного будинку, буде неправильним оминути поняття – «загрози конфіденційності».

Загрози конфіденційності – це загрози, які призводять до небажаного розкриття конфіденційної інформації.

Під загрозами конфіденційній інформації прийнято розуміти потенційні можливі дії у відношенні до інформаційних ресурсів, які у майбутньому можуть призвести до неправомірного заволодіння даними, що зберігаються в конфіденційності [21].

Наприклад, досліджуючи системи «розумний будинок», можна зрозуміти, що порушення конфіденційності інформації в системі домашнього моніторингу може призвести до випадкового розкриття конфіденційних даних, іноді, навіть таких, як температура внутрішнього середовища будинку.

Це може стати причиною того, що ця інформація буде використовуватися для відстеження находження володаря розумного будинку(вдома, чи ні).

Наступний приклад втрати конфіденційності – це вихід у доступ ключів та паролів, що може призвести до несанкціонованих загроз доступу до системи, а, отже до загрози грабування, проникнення до будівлі, тощо.

Саме тому, безпека систем розумного будинку – є однією з найважливіших галузей, яка потребує уваги та ретельного дослідження [22].

1.5. Кіберзлочинність та Законодавство України відносно кіберзлочинності в системах розумного будинку

Говорячи про безпеку, просто не можливо уникнути її протилежної сторони, а саме – кіберзлочинності, або «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». Саме тому є необхідність визначення поняття «кіберзлочинність». Харитоненко І.О., аспірант Київського університету права НАН України пропонує наступне визначення кіберзлочинності.

Кіберзлочинність – це суспільно небезпечне незаконне діяння у ІТ-просторі (кіберпросторі) з його можливим використанням. За таке неправомірне діяння законом України назначається кримінальна відповідальність, що може бути підтверджена українськими міжнародними договорами.

В Україні, кількість кіберзлочинних атак, за останні п'ять років, виросла майже в три рази. Стрибок кількості кіберзлочинних дій відбувся у 2017 році. Після цього кількість злочинів почала стрімко зростати. У 2017 було зафіксовано 1795 справ, в 2018 — 1023, за останні півроку 2019 році – 1005 справ. Нижче наведено гістограму кількості відкритих справ за статтею 361 – кіберзлочинність (рис. 1.13) [23].

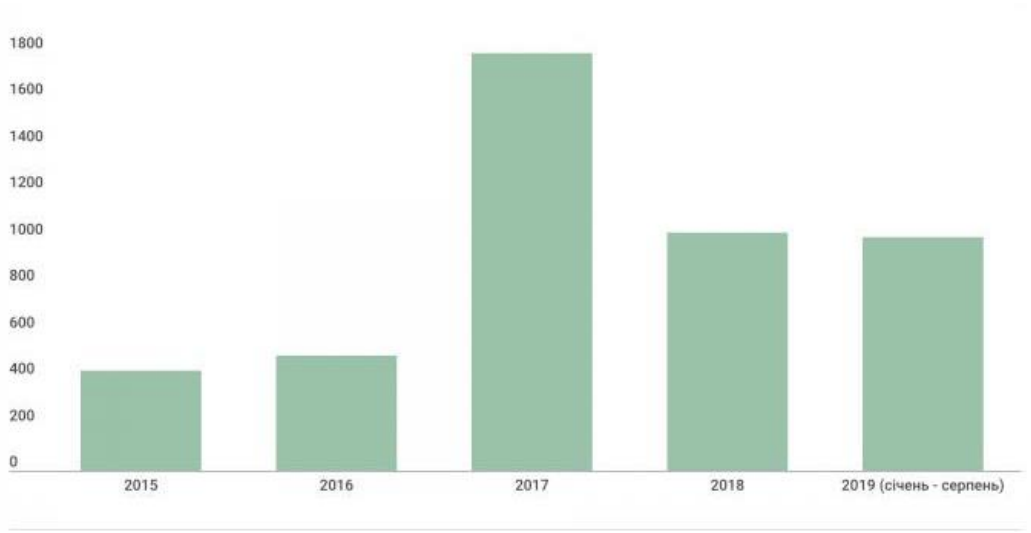

Рисунок 1.13 – Гістограма кількості відкритих справ в Україні в сфері кіберзлочинності

Кіберзлочинці полюють на персональні дані, банківські рахунки, паролі та іншу інформацію, яка існує в електронному вигляді.

Потерпілими можуть стати як фізичні особи, так і бізнес та державний сектор.

На сьогодні найпопулярніша стаття кіберзлочинів – шахрайство, на другому та третьому місцях незаконне втручання в роботу комп'ютерів та розповсюдження інформації для дорослих.

Через велику поширеність кіберзлочинів з'явилося інше поняття – це «кібербезпека».

Кібербезпека – захищеність найбільш важливих інтересів громадянина, суспільства або навіть держави під час використання кіберпростору, завдяки якій забезпечується стабільний розвиток інформаційного середовища та суспільста та цифрового середовища комунікацій, завчасне виявлення, успішне запобігання і повна нейтралізація потенційних та реальних загроз до національної безпеки України у кіберпросторі [24].

Продавці, що надають на ринку України послуги з розробки і реалізації систем розумного будинку, і не тільки, повинні, згідно контракту, який

підписується підчас купівлі системи, надати клієнтам повний захист і конфіденційність отриманих персональних даних.

Але, треба розуміти, що пункт про безпеку і захист даних, який зазначено у контракті між покупцем та продавець, не дає 100% гарантії, ризик витоку інформації, особливо в системах, де є багато взаємопов’язаних приладів, особливо ті системи, де керування відбувається одним контролером, має далеко не одне джерело.

Тобто, вина за поширення конфіденційної інформації володарів систем розумного будинку лежить на компанії, яка несе відповідну відповідальність, то випадки хакерського зловмисного нападу або кібератаки, регулюються національним і міжнародним законодавством.

В законодавстві України є питання стосовно кіберзлочинності, які регулюються нормами. Ось, деякі законодавчі акти регулювання злочинів:

– Закон України від 7 вересня 2005 року "Про ратифікацію Конвенції про кіберзлочинність" [25];

– Закон України від 31 травня 2005 року "Про внесення змін до Закону України"Про захист інформації в автоматизоване системах" [26].

Окрім цього у кримінальному кодексі України існують статті про злочини у сфері ІТ [27].

Розділ XVI – Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж и мереж електрозв'язку (ст.361-363). Ось деякі статті цього розділу:

– Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

– Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку;

– Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;

– Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

– Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється.

Найголовніша стаття законодавства України для володарів систем розумного будинку, на мою думку – це стаття 361-2.

Стаття 361-2 – це несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації [28].

Предметом злочину виступає інформація з обмеженим доступом, яка зберігається в комп’ютерах, або носіях. Інформація буває конфіденційна, тобто та, яка містить відомості, що перебувають у володінні або користуванні людини, або знаходиться в розпорядженні окремих фізичних або юридичних осіб, але найголовніше, її можна поширювати лише за бажанням вищеперерахованих людей.

Карається таке розповсюдження штрафом від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років з конфіскацією програмних або технічних засобів, за допомогою яких було здійснено несанкціоновані збут або розповсюдження інформації з обмеженим доступом, які є власністю винної особи.

Зрозуміло, що чинне законодавство України намагається регулювати

ситуації, які пов’язані з кібератаками або хакерством, але все одно, регулювання злочинів в «мережі» – це величезний обсяг роботи, який потребує вдосконалення та детального опрацювання спеціалістів.

Кіберзлочинність – це звичайно ж не лише проблема України. Це глобальна проблема усього світу, адже загроза поширюється і за кордонами однієї держави. Глобальні комп’ютерні мережі охоплюють переважну кількість країн світу, а це, у свою чергу, позитивно впливає на розвиток кіберзлочинців. Вони стають все більш професійними та мобільними.

Стрімкий розвиток кіберзлочинності зумовлений великою популяризацією та впровадженням технологій в усі сфери життя людини. Чим більше гаджетів використовує людина – тим більше вірогідність витоку інформації через несанкціонований доступ.

В контексті розумних будинків в країнах ЄС, є оновлені правила обробки персональних даних, встановлені загальним регламентом щодо захисту даних – «Регламент ЄС 2016/679 від 27 квітня 2016 року або GDPR – General Data Protection Regulation».

Уявіть, під якою загрозою знаходяться володарі розумного будинку, адже маже всі кутки розумного будинку мають певні гаджети.

Це означає, що хакери можуть отримати доступ до контролю системи майже через будь яку маленьку вразливість, навіть звичайну аудіосистему, камеру, чи навіть розумний замок.

Декілька років тому, на хакерській конференції «DEF CON 24» дослідники – Ентоні Роуз та Бен Ремсі з Merculite Security розповіли про те, як у рамках свого експерименту проводили атаки на шістнадцять моделей «смарт-замків». Результат виявився досить невтішним – лише чотири змогли встояти перед зломом хакерів.

Смарт замки одних вендорів передавали коди доступу в незашифрованому вигляді. Тож зловмисники могли легко їх перехопити, використовуючи Bluetooth-сніфер. Декілька з замків-піддопитних не встояли проти метода повторного відтворення. Тобто, дверима можна було

маніпулювати за допомогою заздалегідь записаних сигналів відповідних команд.

Якщо користувач вважає, що голосові команди перехилять ваги у бік більшої захищеності, то вони, нажаль, помиляються. Декілька років тому з'ясувалося, що якщо господарський гаджет лежить досить близько до зачинених дверей, то досить голосно промовивши через двері кодову команду для відчинення дверей, наприклад – «Привіт, Сирі, відчини двері», то вас можуть впустити.

2. ДОСЛІДЖЕННЯ ШЛЯХІВ ЗАПОБІГАННЯ ЗАГРОЗАМ БЕЗПЕКИ СИСТЕМ РОЗУМНИЙ БУДИНОК

2.1. Вразливості систем розумного будинку

Можливість об'єднання девайсів (приладів), збору всієї комплексної інформації про свій будинок, себе, а також своїх близьких у власному комп'ютері, побудова аналітики і знаходження найбільш ефективних методів для вирішення побутових потреб – від економії електроенергії до прогнозування поведінки і підтримки здоров'я, свого і своїх близьких, все це – блискучі перспективи розвитку систем розумного будинку, які, разом з тим, можуть мати й слабкі місця, що стосуються безпосередньо впровадження технології в повсякденне життя. Ці слабкі місця також називають – вразливостями систем розумного будинку [29].

Вразливість – нездатність конкретної системи або систем протидіяти конкретній загрозі або сукупності загроз [30].

Також, можна сказати, що це певні «недоліки» системи, завдяки яким можна навмисно, або навіть не навмисно, порушити цілісність, або викликати неправильну роботу системи.

На рисунку 2.1 представлені потенційні загрози безпеки систем розумного будинку.

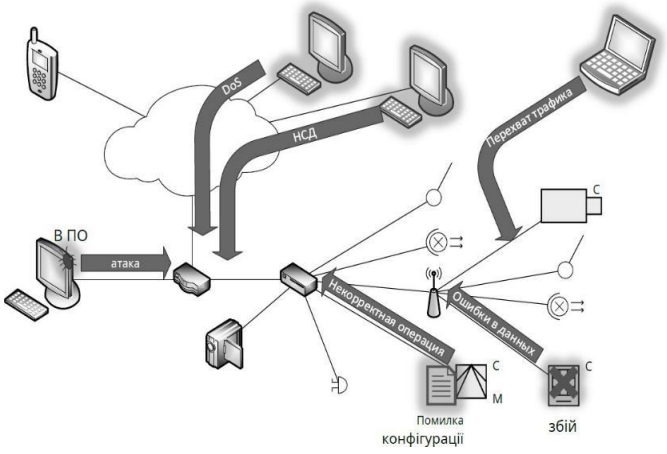

Рисунок 2.1 – Потенційні загрози безпеки систем розумного будинку

Перелік вразливостей систем розумного будинку:

– шкідливий код;
– підключення зараженого пристрою;
– зараження пристроїв в мережі;
– збій пристрою;
– невірні дані датчиків;
– помилкові команди;
– помилка конфігурації;
– неправильна поведінка системи;
– збої в режимах роботи.

Вразливість може виникати в результаті помилок допущених при програмуванні системи, певних недоліків при проектуванні системи, також, це можуть бути ненадійні паролі, або шкідливі віруси та програми, які навмисно було вироблено для нанесення шкоди системам, тощо.

Зрозуміло, що не має систем, які були б ідеальними, без жодних вразливостей, завжди існує загроза порушення безпеки. Кожна загроза тягне за собою певний збиток – моральний чи матеріальний. Захист та протидія загрозі покликане знизити його величину або повністю, або значно, або хоча б частково. Але і це вдається далеко не завжди.

Для кращого розуміння проблеми слід дати визначення поняттю «загроза».

Загроза – це потенційні або реальні дії, що призводять до морального або матеріального збитку [31].

Найбільшою загрозою для систем розумного будинку є саме загрози доступу. Несанкціонований доступ до системного контролеру, особливо на рівні адміністратора, робить всю систему вразливою, та значно спрощує для шахраїв усі можливості для отримання інформації або нанесення шкоди.

Існує багато причин отримання доступу до систем розумного будинку, але нажаль, інколи саме користувачі систем через незнання або, через

нерозуміння важливості безпеки, стають причинами «відкритого» доступу до систем розумного будинку.

Це може бути пов'язано з неправильним керуванням паролями та/або ключами, або з неавторизованими пристроями, що підключаються до мережі.

Навіть, якщо цілісне контролювання не можна отримати, несанкціоноване під’єднання до мережі має можливість «заблокувати» пропускну здатність мережі, або, навіть, стати причиною відмови в підпорядкуванні законному користувачу.

Оскільки велика кількість гаджетів розумного будинку зазвичай мають живлення від батареї і працюють через бездротові мережі з низьким робочим циклом переповнення запитами з цієї самої мережі, наприклад: датчики присутності, руху, тощо, - це може призвести до кіберзлочинів з ослабленням енергії, тобто можливе виникнення відмови в виконанні обслуговування запиту. А це у свою чергу, має можливість викликати збій усієї системи певних функцій.

Також, однією з суттєвих вразливостей систем «розумного будинку» – є доступність мережевої операційної системи.

Мережеві операційні системи – це операційні системи для мережевих пристроїв, таких як маршрутизатор, комутатор з можливостями для роботи в комп'ютерних мережах. До таких можливостей відносять:

- підтримку мережевого обладнання;
- підтримку мережевих протоколів, наприклад протоколів маршрутизації;
- підтримку фільтрації зв'язку;
- підтримку доступу до віддалених ресурсів, таких як принтери, диски і т.п. по мережі;
- підтримку мережевих протоколів авторизації;
- наявність в системі мережних служб, які дозволяють віддаленим користувачам використовувати ресурси комп'ютера [32].

Так як сучасні системи розумного будинку зазвичай підключаються до Інтернету, атаки загрожують відбутися або дистанційно, або за допомогою прямого доступу до мережевих інтерфейсів управління, або за допомогою шляхів завантажування програм на пристрої, які наносять шкоду системі, такі програми також називають віруси.

Комп'ютерний вірус – комп'ютерна програма, що має способність до прихованого самопоширення. В той же час зі створенням власної копії вірус може завдавати шкоди: викрадати дані, пошкоджувати, знищувати, знижувати або й зовсім робить неможливим подальшу працездатність операційних систем комп'ютера. Приклади вірусів: Archiveus, Staog, Neshta [33].

Розрізняють макровіруси, завантажувальні, файлові також комбінації цих типів. Нині відомо близько десяти тисяч комп'ютерних вірусів, що поширюються завдяки мережі Інтернет по всьому світу.

З кожним роком комп'ютерні віруси наносять все більше шкоди, на суму близько декілька мільярдів доларів. Працюють вони наступним чином: викликають критичні системні помилки, через це зупиняються великі сайти та вебдодатки, знищують або модифікують файли, підвищуючи час відклику [34].

За створення та поширення шкідливих програм та вірусів у великій кількості країн передбачено кримінальну відповідальність. В Україні, наприклад, поширення комп'ютерних вірусів переслідується і карається згідно до Кримінального кодексу – статті 361, 362, 363.

Ще однією проблемою системи розумного будинку є її фізична доступність. Як для бездротових так і для фізичних мереж, отримати доступ можна і ззовні, навіть коли сам будинок надійно заблокований.

Наступна вразливість – це обмеженість системних ресурсів. Контролери пристроїв зазвичай раніше представляли собою невеликі мікроконтролери (8-розрядні) з дуже обмеженими ресурсами для обчислювання і ресурсами збереження, що й досі обмежує здатність реалізувати складні алгоритми

безпеки. Завдяки розвитку технологій, ця вразливість найближчим часом планується бути виправлена.

Ще однією вразливістю системи «розумний будинок» є системна неоднорідність. Обладнання виробляється багатьма компаніями-виробниками з різними мережевими стандартами і відмінними один від одного можливостями до оновлення програмного устаткування.

Часто документація стосовно внутрішнього програмного забезпечення та операційні системи, що надається з обладнанням, або не повна, або взагалі відсутня. Тобто інформації для встановлення механізмів безпеки дуже недостатньо.

Фіксована прошивка – це наступна проблема, яка на сьогодні досить поширена в системах «розумний будинок». Існує дуже невелика кількість розумних побутових приладів, до яких надаються будь-які регулярні послуги з оновлення програмного забезпечення для виправлення вразливостей, що періодично виникають під час встановлення даних систем у житлове приміщення.

Також, до вразливостей систем «розумний будинок» можна віднести – повільне впровадження стандартів. Коли деякі пропрієтарні системи, наприклад як підсистема моніторингу працездатності, можуть мати добре розроблену безпеку, яка відповідає стандартам, то більшість сучасних пристроїв розумного будинку реалізують кілька підходів до безпеки, якщо взагалі використовують.

Наприклад, володар може припустити, що веб-камера його розумного будинку доступна тільки користувачам, яким дано ім'я хоста і номер порту, однак за допомогою пристроїв пошуку, які сканують інтернет-пристрої, таких як Censys та Shodan, які законно шукають доступні датчики, багато пристроїв раптово стають відомі і видимі. Що може стати загрозою витоку конфіденційної інформації.

Ще однією вразливістю є – вразливості протоколів передачі даних. На сьогодні у світі існує велика кількість протоколів, що використовуються у

галузі автоматизації управління будівлями. Нажаль, на даний момент не було визначено загальноприйнятих стандартів для організації взаємодії усіх пристроїв в мережі, що складають систему розумного будинку [35, 36].

Застосування з цією метою технологій побудови локальних мереж обчислювання є малоперспективним в зв'язку з їх надмірністю.

Технології, що застосовуються в системах розумного будинку, повинні відповідати таким критеріям:

– низька вартість;
– висока надійність і безпека передачі даних;
– простота фізичного розміщення.
– низьке енергоспоживання;

Окремо можемо зазначити відсутність необхідності в високих швидкостях передачі даних у багатьох «сценаріях» використання систем.

При порівнянні дротових і бездротових мереж вирішальним фактором є – простота фізичного розміщення мережевих пристроїв.

Існує сімейство конкурентоспроможних технологій провідних мереж, які називаються Power Line Communication (PLC). Дані технології покладаються на той факт, що приміщення, в яких розгортається мережа, як правило електрифіковані.

Таким чином, можлива побудова як дротових, так і бездротових мереж із застосуванням ряду технологій таких, як X10, INSTEON, HomePlug, Lonworks для забезпечення зв'язку по дротах електричної мережі, і Bluetooth, Z-Wave і ZigBee для забезпечення бездротового зв'язку.

Z-Wave – запатентований стек протоколів, що розробляється і підтримуваний Z-Wave Alliance. На даний момент, це один з найбільш перспективних протоколів для застосування в сфері побудови систем «Розумного будинку».

Для Z-Wave визначені такі рівні, відповідні моделі OSI:

– Фізичний рівень.

– Канальний рівень. На даному рівні реалізується контроль цілісності і адресація пристроїв в зоні прямої видимості. Можлива багатоадресна і широкомовна розсилки.

– Мережевий рівень. Специфікації протоколу Z-Wave визначають алгоритм маршрутизації одноадресних пакетів, службовець для передачі даних між пристроями, що знаходяться поза прямою досяжності. Всі постійно працюють вузли мережі беруть участь у пересиланні пакетів між іншими учасниками мережі.

Маршрут прямування пакета визначається перед його відправкою вузлом – джерелом. При неможливості знайти потрібний вузол по відомим відправнику маршрутами, існує механізм пошуку вузла по всій мережі шляхом посилки спеціального пакета Explorer Frame всіх вузлів мережі.

– Транспортний рівень. На даному рівні Z-Wave забезпечує підтвердження доставки і повторну відправку в разі втрати пакета під час передачі. Для цього кожен вузол, який бере участь в пересилання, підтверджує факт отримання повідомлення. При використанні такого механізму підтвердження відправляється тільки після досягнення пакетом кінцевого вузла призначення.

– Сеансовий рівень. Використовується тільки при включеному шифруванні для встановлення сеансового ключа.

– Прикладний рівень. Специфікація Z-Wave визначає алгоритм інтерпретації одержуваних на прикладному рівні команд. Даний рівень описаний набором класів команд. Для деяких класів існує кілька варіантів інтерпретації команд, які залежать від класу пристрою.

Критичні компоненти системи автоматизації, такі, як замки, на даний момент використовують шифрування AES-128. Однак, шифрування є розширенням стандарту, і ранні пристрої не підтримують його.

Більш того, ряд пристроїв можуть мати уразливості в реалізації протоколу обміну ключами, що дозволяє отримувати до них доступ з використанням ключа за замовчуванням – 00000000000000000000000000h [37].

Існує ряд рішень для полегшення керування систем розумного будинку на основі протоколу Z-Wave. Основним інструментом для взаємодії з системою є веб-інтерфейс і він використовує API. При цьому не потребується надання механізми аутентифікації і шифрування даних. В такому випадку можна виконувати довільні дії з системою розумного будинку після компрометації локальної мережі.

Також, окрім Z-Wave я би хотіла розглянути мережі ZigBee. Мережі ZigBee використовуються в системі РТЛС як бездротових мереж передачі даних – альтернативи LAN для управління і конфігурації базових станцій і міток, управління процесами позиціонування, а також для передачі результатів вимірювань від міток на сервер для подальшого використання.

ZigBee – це відкритий стандарт бездротового зв'язку для різних систем автоматизації: «Розумний будинок», «Інтелектуальний будинок», системи управління технологічними та бізнес процесами, системи безпеки і т.і [38].

Технологія ZigBee дозволяє створювати самоорганізуються і самовідтворюваними бездротові мережі з автоматичною ретрансляцією повідомлень. Мережі ZigBee при відносно невеликих швидкостях передачі даних забезпечують гарантовану доставку пакетів і захист інформації, що передається.

Стандарт ZigBee використовує частотні канали діапазону 868 МГц, 915 МГц і 2,4 ГГц. Надшвидкісні передачі даних і надзвичайно висока стійкість, може досягатися в діапазоні 2,4 ГГц. Саме тому, велика кількість виробництв, які роблять мікросхеми, випускають приймачі в цьому діапазоні. В цьому діапазоні, також передбається 16 частотних каналів з величиною кроку – 5 МГц.

Швидкість передачі даних враховуючи службову ефірну інформацію може становити 250 кбіт / с. Але, середня пропускна спроможність вузла корисних даних, але це залежить і від мережевої завантаженості та кількості ретрансляцій, може межуватися від 5 до 40 кбіт / с.

Міжвузлова відстань мережі становлить десятки метрів, але коли робота відбувається в середині приміщень. Та сотні метрів, якщо робота відбувається на відкритому повітрі. Покриття мережі може значно збільшуватися за рахунок ретрансляції.

Рівень додатків визначає об'єкт пристрою ZigBee, рівень підтримки додатків і рівень інтерфейсу розробки додатків.

Інтерфейс розробки додатків містить опис визначає стандартні типи даних, дескриптори виявлення служб, формати пакетів. Все це дозволяє швидко розробляти прості профілі на основі атрибутів.

Об'єкти додатків – програмні модулі, що керують пристроями ZigBee в кінцевих точках. Підрівень підтримки додатків відповідає за надання даних додатків і профілів пристрою ZigBee.

Підрівень також керує приєднанням пристроївв мережі ZigBee і зберігає дані про них.

Мережевий рівень виконує функції управління мережевими адресами і маршрутизації. У його завдання також входять:

– запуск мережі;
– привласнення мережевих адрес;
– додавання і видалення мережевих пристроїв;
– маршрутизація повідомлень;
– застосування політики безпеки;
– здійснення пошуку маршрутів.

Постачальник послуг безпеки забезпечує механізми безпеки для мережевого рівня і рівня додатків при використанні шифрування.

Мережі ZigBee можуть функціонувати в режимах, що передбачають роботу без шифрування. Стандартний рівень безпеки не забезпечує безпеку поширення ключа мережі.

Існує механізм призначений для запобігання атак повторно. Однак, реалізація механізму може викликати проблеми в роботі мережі, що призводить до необхідності скидання лічильників власноруч. Без включення

даної опції атака повторюється [39].

Атаки повтору і отримання ключа з перехопленого трафіку реалізовані на практиці в фреймворку KillerBee, призначеному для аналізу мереж ZigBee.

Аналізуючи дані можна зробити таблицю основних вразливостей бездротових протоколів передачі даних. Нижче наведено таблицю 2.1 [40].

Таблиця 2.1 – Перелік вразливостей протоколів передачі даних

№	Назва протоколу	Основні проблеми/вразливості/фактори, які є загрозами інформаційній безпеці
1	Bluetooth	• Bluejacking (атака bluetooth-спамом); Bluebugging (несанкціонована передача даних хакерами); • Bluesnarfing (доступ до хакерів файлів за допомогою Bluetooth приєднання).
2	ZigBee	• Фізичні атаки; • Атаки на зв'язаних ключах; • Атаки повторного підтворення; • Ін'єкційні атаки (Injection attacks).
3	Z-Wave	• Спурфінг атаки; • Виявлення зовнішньої топології; • Довільна модифікація SR кешу; • Атаки відбрасування пакетів.
4	WiFi	• WEP та Wi-Fi захищений доступ (WPA) можливо взламати за хвилини; • WPA2 також може бути взламаний, але якщо користувач налаштує його належним чином, це займе більше часу у злочинця;
5	Celluar	• Відстеження місцезнаходження; • Викрадення смуги пропускання; • Проблеми безпеки через відкриту архітектуру; • DoS атаки.
8	LoRaWAN (Long Range wide Area Network)	• Неоптимальні методи шифрування; • Проблеми, пов'язані з ключами шифрування; • Проблеми з довірою при обробці даних на передавальних пристроях; • Проблема з взломуванням шлюзу; • Компоненти зламаного доступу в Інтернет є частою метою для хакерів.

Опираючись на отримані вище дані можливих загроз та вразливостей систем розумного будинку можна зробити висновок про можливі наслідки, які виникнуть підчас реалізації загроз (табл. 2.2).

Таблиця 2.2 – Перелік загроз, вразливостей та можливих наслідків в системах розумного будинку

Загроза	Вразливість	Можливі наслідки
Хакерські атаки на головний сервер системи розумного будинку	– Підключення мережі розумного будинку до Інтернету, а саме: відсутність або неефективність механізмів захисту мережі	– Порушення роботи або вихід з ладу головного серверу та всієї системи загалом; – Порушення конфіденційності, цілісності та доступності інформації.
Перехоплення інформації, яка передається через дротові та бездротові канали зв’язку системи розумного будинку	– Можливість доступу зловмисника до дротових каналів або до зони перехвату радіосигналів мережі; – Відсутність або неефективність механізмів захисту трафіку.	– Порушення конфіденційності інформації, яка передається по каналу – Можливий доступ до керування системою
Доступ зловмисника з правами адміністратора до центрального або головного серверу системи розумного будинку	– Відсутність або неефективність механізмів аутентифікації та ідентифікації	– Порушення конфіденційності, цілісності та доступності інформації, яка знаходиться всередині мережі

Зрозуміло, що існує велика кількість загроз та вразливостей систем розумного будинку, які потребують швидкого та якісного рішення, але завдяки вияву так званих «слабких місць» та взагалі дослідженню безпеки систем розумного будинку, ймовірність передбачення та застереження користувачів від шахрайських дій з кожним роком лише зростає.

3. ПРОПОЗИЦІЇ ЩОДО ШЛЯХІВ ЗАПОБІГАННЯ ЗАГРОЗАМ БЕЗПЕКИ СИСТЕМ РОЗУМНОГО БУДИНКУ

3.1. Методи для самостійного безкоштовного запобігання загрозам систем розумного будинку

Сучасний темп впровадження систем розумного будинку в житлові приміщення все більше набирає обертів, а отже і збільшується кількість переживань споживачів щодо забезпечення конфіденційності своїх персональних даних, та взагалі, цілісної безперебійної роботи системи без зовнішнього втручання сторонніх осіб. Саме тому, з’явилась потреба у запропонуванні методів для самостійного безкоштовного запобігання загрозам систем розумного будинку.

Аналіз ситуації показав, що найбільш вразливим місцем в системах розумного будинку – є програмна частина. Саме тому потрібно більш детально зупинитися на цьому питанні.

Програмна частина або програмне забезпечення в системах розумного будинку – це сукупність програм, які призначені для розв'язання певних завдань в системах розумного будинку [41].

Для самостійного, з точки зору користувачів, та безкоштовного запобігання загрозам систем розумного будинку можна запропонувати наступні методи:

– забезпечення безпеки роутера;

– використання унікального пароля для кожного пристрою системи «розумний будинок»;

– регулярно оновлювати прошивку на всіх пристроях системи «розумний будинок»;

– не керувати системою «розумний будинок» загальнодоступною мережею «wi-fi».

Як вже було описано вище, перший запропонований метод – забезпечення безпеки роутера. Більшості пристроїв системи «Розумний будинок» для коректного і правильного функціонування, потрібно забезпечити безпосередній доступ до інформаційної комп'ютерної мережі «Інтернет», тобто, у багатьох випадках, єдиним і найбільш вразливим потенціалом злому є маршрутизатор.

Тому, користувачу потрібно підвищити рівень безпеки та організації відповідного ступеня захисту маршрутизатора. Найпростіший метод досягнути цього це – змінення пароля адміністратора, багато користувачів не звертають належної уваги на це, та стають потенційно легкою здобиччю для шахраїв.

Більш складний метод це — встановлення зовнішніх спеціалізованих систем безпеки (firewall), але фінансово це вже не відноситься до бюджетного рішення.

Наступний метод запобігання загрозам систем розумного будинку це – використання унікального пароля для кожного пристрою системи «Розумний будинок». Захищайте пристрої і панелі управління довгим унікальним паролем, тоді зловмисники не зможуть підібрати «ключик» до вашого будинку.

Кожен пристрій, для якого користувачі створюють обліковий запис, повинен мати унікальний складний комбінований пароль. Якщо діюча «парольна фраза» буде використовуватися повторно, то в службах і пристроях системи «Розумний будинок», можна отримати загальний єдиний скомпрометований блок, а це призведе до появи додаткових вразливостей в системі керування, яка була призначена для користувача.

Увімкнення двухфакторної аутентифікації для всіх можливих пристроїв також збільшить ступінь захищеності паролів.

Третій метод запобігання загрозам систем розумного будинку користувачами системи «Розумний будинок» – це регулярно оновлювати прошивку на всіх пристроях системи розумного будинку.

Виробники регулярно знаходять окремі баги (помилки в написанні коду), неполадки, помилки або конфлікти сумісності в пристроях, та виправляють їх, тим самим збільшуючи можливості пристроїв, а отже і їх безпеку, за рахунок впровадження нових або поліпшення старих функцій. Також, користувачам потрібно завантажувати програми з офіційних джерел і не надавати їм занадто багато дозволів, особливо, якщо програма потребує доступ до занадто конфіденційної інформації.

Ще один метод, який зможе хоча б трохи підвищити вірогідність збереження безпеки систем розумного будинку – це купувати систему розумний будинок лише у перевірених та знайомих фірм. Тобто, перед купівлею користувачу потрібно звернути увагу не дешевизну системи, а на компанію, яка її продає, та якомога більше ознайомитися з нею.

Маже всі пристрої, якими користувачі комплектують системи розумного будинку, взаємодіють із серверами у віддаленому хмарному сховищі. Найголовніша небезпека у цьому питанні – кому належать ці сервери. Якщо порівняти нещодавно випущений продукт невідомого виробника, з тим, який вже багато років є на ринку, то неможливо точно визначити, з якими ресурсами новоспечений виробник взаємодіє. Зрозуміло, що після того, як хтось його перевірить, то це питання буде знято, але ризи чи малий.

Якщо користувач не належить до дослідників безпеки систем розумного будинку, які цілеспрямовано тестують і перевіряють доступні нові пристрої, то, звичайно, краще буде відмовитися від придбання нового, незнайомого продукту. У такому випадку краще віддати перевагу більш перевіреним і відомим виробникам систем розумного будинку, якщо пріоритет безпеки розумного будинку стоїть на першому місці.

Крім того, найбільша проблема, яка виникає в системах розумного будинку – впровадження в єдину систему пристроїв. Зрозуміло, що з часом експлуатації, деякі пристрої можуть вийти з ладу та перестати працювати. Ось тут користувач і може зіштовхнутися з проблемою маловідомої компанії.

Виробник системи може просто збанкрутувати, або навіть зникнути, або ухвалити рішення перейти на новий продукт і припинити підтримку, раніше випущених пристроїв, наприклад, з метою зниження фінансового навантаження. Тобто, користувач системи після придбання може просто залишитися без післяпродажної підтримки від виробника.

Зрозуміло, що використання продукції від відомого виробника також не гарантує, що надалі нічого подібного з цією системою не відбудеться, проте, користувачі зможуть ознайомитися, переглянути історію випуску продуктів, подивитися кількість придбаних систем розумного будинку, проаналізувати життєздатність системи та вивчити граничні часові рамки гарантованої підтримки компанією своїх продуктів.

На мою думку, цієї аргументації більше ніж достатньо для того, щоб бути більш схильним на придбання систем розумного будинку від відомих та знайомих користувачам фірм, які вже доволі багато існують на ринку.

Останній з запропонованих методів, який не потребує значних фінансових вкладень – це запропонування користувачам системи «Розумний будинок» – не керувати системою загальнодоступною мережею «Wi-Fi», навіть якщо є впевненість, що мережа гарантовано безпечна. Все одно існує значний ризик відкрити доступ до пристроїв в своїй системі стороннім користувачам, а це може призвести до шкідливих дій.

Якщо користувачам необхідний віддалений доступ, то треба використовувати пристрій з підтримкою «LTE» або розглянути можливість настройки персональної віртуальної приватної мережі «VPN» для безпечного підключення.

Усі описані вище результати дослідження – це методи для самостійного безкоштовного покращення роботи пристроїв та підвищення рівня захисту системи «Розумний будинок».

Більш професійні методи запобігання атакам на систему «Розумний будинок» потребують залучення спеціалізованих компаній, а отже, потребують більшого фінансового вкладу.

3.2. Методи для запобігання загрозам систем розумного будинку з точки зору інженера електронника

3.2.1. Використання менеджерів паролів для забезпечення більшої надійності систем розумного будинку

Ознайомившись більш детально з літературою стосовно забезпечення безпеки систем розумного будинку, та провівши певне дослідження з цього питання, можна зробити висновок, що близько 90% джерел рекомендують для користувачів системи розумний будинок звернути особливу увагу саме на використання унікальних, неповторних паролів. Особливо, наголошується пункт про забезпечення системи різноманітними паролями для кожного, за можливості, приладу системи розумного будинку.

Звідси виникає ряд питань:

1. Чи є можливість генерування паролів?
2. Де зберігати інформацію про всі паролі?
3. Що робити, якщо один з користувачів системи загубив або зламав керуючий прилад? Наприклад – мобільний телефон, планшет, тощо.
4. Як регулювати кількість користувачів та надавати доступ до системи новим користувачам?
5. Чи можна керувати паролями систем розумного будинка не підходячи до головного базового блоку керування системи розумного будинку? Наприклад, якщо базовий блок знаходиться в важкодоступному місці, або якщо вводити зміни щодо користувачів системи або щодо зміни паролів потрібно дуже часто.

Усі ці питання – є дуже затребуваними та відомими, саме тому, вони потребують швидкого та якісного рішення, адже, якщо у користувачів виникають певні потреби, то розробникам систем розумного будинку потрібно знаходити компромісне рішення, адже це стане вагомим «за» при виборі

користувачами системи розумного будинку, у бік компаній, які подбали про ці питання.

Для деяких користувачів систем розумного будинку, керування розумним будинком – є важким та обтяжливим питанням. А завдання в присвоєнні кожному пристрою системи унікального пароля — взагалі неможливо складним завданням, зокрема якщо до мережі під'єднана велика кількість пристроїв.

В результаті, один й той самий пароль найчастіше використовується повторно та присвоюється кожному компоненту в мережі, адресам електронної пошти та навіть банківським рахункам.

Нижче наведено перелік помилок у використанні паролів, які найчастіше здійснюють користувачі:

– використання простих паролів. до них відносяться – короткі паролі, паролі з словами зі словників, легко вгадуємі паролі з різних причин, паролі без спільного використання символів різних типів, тобто без цифр, розділових знаків, літер у верхньому та нижньому регістрах, тощо;

– використання паролів, які легко можуть бути знайдені іншими – на наліпках на моніторах, у блокноті біля комп'ютера, у документі на комп'ютері, на смартфоні, у вигляді відкритого тексту, тощо;

– використання однакових паролів для багатьох сайтів, відсутність зміни паролів, тощо;

– спільне використання паролів, тобто, володарі паролів розповідають іншим свої паролі, надсилають незашифровану електронну пошту з паролями, тощо;

– входи до сайтів або інших систем за допомогою адміністративного доступу, там де повинні використовуватись обмежені або користувацькі облікові записи.

Наявність зазначених розповсюджених і типових помилок робить злом до системи дуже легким завданням. Збиток від такої халатної поведінки, навіть якщо скомпрометовано тільки один пристрій, вважається катастрофічним,

адже хакер може впевнено маневрувати в середині мережі та отримувати доступ до будь якої частини системи, використовуючи один і той же пароль.

Звичайно, рішення вже давно запропоноване, вигадане та відоме. Це – менеджер паролів. Для кращого розуміння слід зробити визначення цього терміну.

Менеджер паролів – локально встановлене програмне забезпечення, або веб-сайт, який допомагає користувачам генерувати, зберігати та вводити складні паролі із зашифрованої захищеної бази даних та вести облік користувачів, які мають, або будуть мати доступ до паролів.

Менеджер паролів може бути виготовлено і як окремий пристрій, наприклад у вигляді токенів. Токени — локально доступні пристрої, які аутентифікують користувачів замість або на додачу до традиційних текстових паролів. Дані, які зберігаються у токені, зазвичай надійно зашифровані від неавторизованого читання сторонніх осіб.

Деякі системи, виконані на токенах, потребують додаткового програмного забезпечення, наприклад, драйверів, для того, щоб правильно прочитати або декодувати дані.

Токенами можуть буди смарт картки, захищенні flash-носії зазвичай з інтерфейсом USB, тощо.

Головними завданнями менеджерів паролів – є створення або генерування надійного, персонального, унікального та неповторного, в системі розумного будинку, паролю; зберігання, адміністрування та шифрування комбінацій паролю для кожного пристрою системи.

Данна програма вирішує одразу низку питань, вона вирішує проблему користувачів системи розумного будинку від вигадування, запам’ятовування великої кількості паролів, також вона допомагає вести адміністрування користувачами набагато зручніше, швидше та простіше, адже є можливість автоматично заповнити облікові данні користувачів [42].

Існує три типи менеджерів паролів:

– хмарні додатки;

– локальні сховища;

– менеджери, які вже включені в рішення.

Переважна більшість менеджерів паролів працюють, як хмарний додаток. Хмарний додаток – це додаток, який працює в повністю віртуалізованих сервісах, який базується на великому парку комп'ютерних архітектур, тобто з можливістю повністю абстрагуватися від фізичних коренів можливостей. Це додаток, доступ до якого можна отримати через будь який браузер.

Однією з найбільших переваг даного типу менеджера паролів – є можливість швидкого відновлення усіх даних в разі зміни браузера або при заміні керуючого пристрою. Також, у випадку, якщо користувачу потрібно буде зареєструватися на нових сервісах, користувач може скористатися власними «ключовими фразами», або вбудованим генератором створення випадкових та, головне, безпечних комбінацій.

Недолік у менеджера паролів хмарного типу також є, і це те, що незалежно від обраного додатку, все одно користувачу облікового акаунту доведеться створити одну, надійну комбінацію пароля для захисту усіх його конфіденційних облікових даних, які використовуються для доступу до різних служб. Для хмарного менеджера паролів – це неминуча процедура створення облікового запису.

Наступний тип менеджера паролів це – локальні сховища. Тобто, це такий тип менеджерів, який зберігає усі облікові дані користувача на певному, обраному користувачем пристрої.

Користувач може обрати один з декількох варіантів з відкритим вихідним кодом, які надають безліч функціональних можливостей, проте, часто мають скромний дизайн на відміну від менеджерів паролів хмарного типу.

Останній тип менеджерів паролів – є менеджери, які вже включені в рішення, наприклад в рішення з безпеки комп'ютерів або ноутбуків, тощо. Для

того, щоб допомогти користувачу керувати обліковими даними, як наприклад, для входу в систему, забезпечуючи також повний захист цієї системи.

Прикладом є модуль ESET Password Manager, який є частиною рішення ESET Smart Security Premium, та доступний на всіх головних платформах. Таки як – Windows, Android та iOS.

Одними з найпопулярніших, та найрекомендованіших користувачами менеджерів паролів є – Зв'язка ключів iCloud, паролі Chrome, LastPass, Dashlane, 1Password.

Захист від перелічених раніше загроз системи розумний будинок, зручність у використанні, зґрупованість даних, можливість керування одразу великою кількістю пристроїв системи розумного будинку, безпечність, генерування та зберігання ключів, робить менеджери паролів дуже важливою, корисною та зручною частиною забезпечення безпеки систем розумного будинку.

3.2.2. Криптографічне шифрування для забезпечення більшої надійності систем розумного будинку

Ще один спосіб забезпечення безпеки систем розумного будинку – шифрування даних. Для кращого розуміння необхідності шифрування потрібно більш детально розібрати схему передачі даних системи розумного будинку, та виявити певні потенційні небезпеки, які можуть при цьому виникнути.

На рисунку 3.1 наведено схему передачі даних системи розумного будинку.

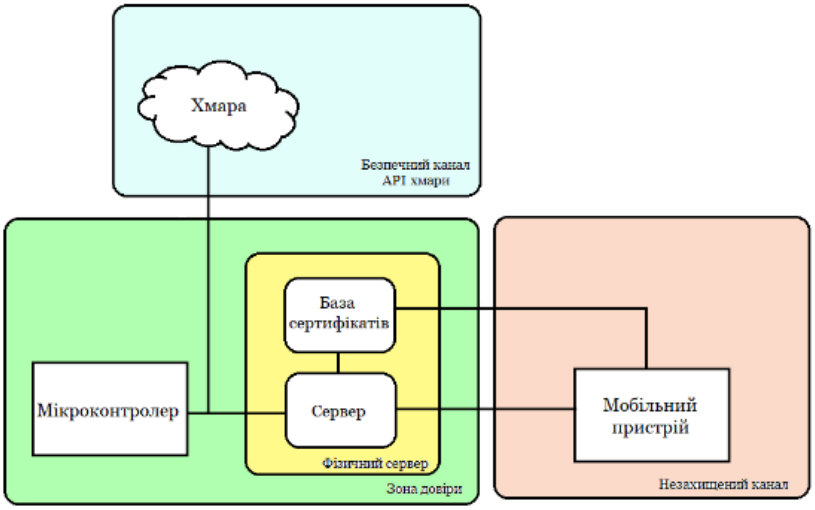

Рисунок 3.1 – Схема передачі даних в системах розумного будинку

Хмара або хмарне сховище (англ. *cloud storage*) – модель online середовища, данні у якому зберігаються на багаточисельних розподілених у мережі серверах, які даються користувачам для використання. На відміну від моделі зберігання даних на власних серверах, в «хмарі» кількість серверів, або будь яка внутрішня структура не може бути побачена користувачами.

Хмарним сховищем є такі інтернет сервіси як – Dropbox, OneDrive, Google Drive, iCloud, Яндекс.Диск, Mega, BOX, TeraBox, тощо. З рисунку 3.1 можна чітко побачити, що хмара знаходиться в певному безпечному каналі API хмари. API (*Application Programming Interface*) – це прикладний програмний інтерфес, або набір визначених методів або підпрограм для взаємодії різних компонентів [43].

Мікроконтролер – це спеціалізований комп'ютер, у вигляді мікросхеми, який має в своїй структурі мікропроцесор, оперативну та постійну пам'ять, яка потрібна для збереження коду, який буде виконуватися, програм і даних, також, в свої будові мікроконтролер має порти вводу та виводу і блоки зі спеціальними функціями. В системах розумного будинку, мікроконтролер відіграє функцію керування системою.

Як видно з рисунка 3.1, в тілі фізичного сервера знаходяться база сертифікатів та сам сервер. Сервер в системах розумного будинку потрібен для

забезпечення безперебійного та автономного реагування на зовнішні події відповідно до встановленого програмного забезпечення.

База сертифікатів в системах розумного будинку потрібна для зберігання всіх цифрових підписів. Доступ до цих підписів має логічний сервер, користувач має лише частковий доступ, наприклад зі свого мобільного пристрою.

Зрозуміло, що в рамках локальної мережі, або так званої мережі сервера, усі дані вважаються захищеними. Тоді, зрозуміло, виникає питання необхідності шифрування даних.

Велику низку небезпек становить саме канал користувача. Наприклад, як описано в одному з класичних сценаріїв – «людина по середині», або «man-in-the-middle». Цей сценарій означає, що існує можливість підключення інших осіб до каналу між сервером та користувачем.

Тобто, ця «людина по середині» може видавати себе за когось з ключових осіб, беручи на себе роль «невидимого посередника», а це, у свою чергу, може призвести до витоку інформації, псуванню інформації, порушенню цілісності інформації, що може призвести до поганого функціонування систем розумного будинку. Для того, щоб забезпечити безпеку від витоку даних і потрібне шифрування даних.

Серед схем шифрування даних в сучасних інформаційних технологіях захисту даних можна виділити дві основні – симетричні та асиметричні криптосистеми.

Криптографічна система (криптосистема) – це алгоритм здійснення перетворень вихідного тексту в зашифрований, та зворотно.

Різниця в симетричних та асиметричних криптосистемах полягає лише в використанні ключів. В симетричних криптосистемах для шифрування та дешифрування використовується один й той самий криптографічний ключ, а в асиметричних криптосистемах, для шифрування та розшифрування даних використовуються різні криптографічні ключі.

Тобто, знаючи ключ шифрування й зашифрований текст, в симетричних криптосистемах можна дешифрувати повідомлення. На відміну від симетричних криптосистем, в асиметричній криптосистемі для шифрування використовується відкритий ключ, а для дешифрування – закритий. Тобто, відновити вихідне повідомлення знаючи ключ шифрування й зашифрований текст майже неможливо.

Зрозуміло, що для більш надійнішого шифрування даних в системах розумного будинку краще використовувати асиметричні криптографічні алгоритми, але, вони потребують більших обчислювальних потужностей, проте, найчастіше, для економії, для керування системами розумний будинок встановлюють мікроконтролери з невисокими обчислювальними потужностями. Звичайно, що застосування більш дорогої елементної бази призведе до підвищенню цін на системи розумного будинку, а це у свою чергу негативно відобразиться на популярність «розумних будинків» на ринку.

3.2.3. Забезпечення механізму аутентифікації користувача

Для забезпечення більшої надійності до доступу системи розумного будинку, рекомендовано ввести механізму аутентифікації санкціонованого користувача. Головною метою цього механізму є те, що керування будь якими компонентами системи розумного будинку повинно відбуватися лише після аутентифікації користувача в системі загалом, та після його подальшої авторизації.

Це дуже потрібна процедура адже найчастіше, користувачі системи розумний будинок дуже часто керують системою зі свого смартфону або планшету, або іншого портативного девайсу (приладу) з’єднуючись з розумним будинком використовуючи безпровідну мережу, ось на цьому етапі і випливає найбільша загроза, а саме – загроза перехвату ідентифікаційних або аутентифікаційних даних сторонніми.

Реалізація цього перехвату може бути через впровадження в пристрої системи розумного будинку шкідливого програмного забезпечення, або користуючись вже існуючими вразливостями програмного забезпечення пристроїв системи. Також, перехват даних може відбутися через прослуховування каналу зв'язку керуючого пристрою, наприклад планшету або смартфону користувача системи, з пристроями системи розумного будинку, тощо.

Відсутність механізму аутентифікації санкціонованого користувача у більшості приладів, які є частиною системи розумного будинку, одразу робить їх вразливими «маячками» для програмних засобів за допомогою яких можна отримати несанкціонований доступ до таких приладів. Яскравими представниками таких програмних засобів є – «Shodan» та «Censys».

«Shodan» та «Censys» – це пошукові системи, які дозволють користувачам шукати різні типи серверів, наприклад, Web-камери, маршрутизатори і таке інше, які під'єднані до глобальної павутини «Інтернет». Такі програми можуть надати користувачам різні методані з цих серверів, наприклад – яке серверне програмне забезпечення використовує та чи інша веб-камера, скільки цих веб-камер, хто відповідає за них, я вони називаються, чи мають вони мережевий інтерфейс, яким можна скористатися, тощо.

Ці програми не створюють ризик, якщо ваші прилади захищені паролями та різними додатковими аутентифікаціями, серйозну загрозу ці програми несуть тим маршрутизаторам або веб-камерам, наприклад, які недбало віднеслися до своєї безпеки. Наприклад, якщо користувачі не змінили дані, такі як, паролі та логіни, а залишили їх за замовченням.

Тоді, за допомогою «Shodan» або «Censys», зловмисник може знайти інтерфейс вашої, наприклад, веб-камери, дізнатися логін та пароль, а це буде не важко, адже інформацію про стандартні логіни та паролі для того, чи іншого приладу, якій підключається до інтернету, можна знайти у вільному доступі на сайтах виробників, та отримати доступ до зображення цієї веб-камери, або отримати повний доступ до її керування [44].

4. МЕТОДИЧНІ ПІДХОДИ ТА КРИТЕРІЇ ВИБОРУ ПАРАМЕТРІВ БЕЗПЕКИ СИСТЕМ РОЗУМНОГО БУДИНКУ

4.1. Способи вибору систем розумного будинку

При вирішенні практичних завдань завжди існує декілька варіантів вибору. Вибір – відання переваги в бік одного варіанту в умовах безлічі альтернатив [45].

Вибір відбувається, через велику кількість пропозицій в певному сегменті і через пошук найоптимальнішого варіанту серед усіх представлених.

Існує три способи, за допомогою яких можна зробити вибір:

– випадковим чином;

– вольовим чином;

– критеріальним чином.

Вибір випадковим чином – це спосіб вибору, який не залежить від поставлених завдань. Цей метод є одним з найпростіших методів, проте, залишається вірогідність незадоволеності отриманих результатів.

Вибір вольовим чином – це спосіб, який визначається рисами характеру особи, яка робить вибір. Такий спосіб є доволі складним, адже відповідальність та наслідки за зроблений вибір буде нести особа, яка робить вибір. Цей метод, також, не гарантує отримання повної задоволеності отриманих результатів.

Останній з представлених методів вибору є – критеріальний метод. Він набагато складніший з усіх представлених, адже потребує певних аналітичних методів дослідження та обґрунтування. Проте, цей спосіб вибору має найбільшу вірогідність отримання задоволеності отриманих результатів особою, яка робить вибір.

Саме тому, для дослідження безпеки систем розумного будинку було обрано критеріальний метод вибору. Один з методів для вирішення багатокритеріальних задач використовують метод аналізу ієрархій.

4.2. Метод аналізу ієрархій

Метод аналізу ієрархій (МАІ) – це структурований психо-математичний метод аналізу багатокритеріальних задач.

Цей метод був розроблений професором Пенсильванського та Піттсбурзького університетів Томасом Сааті в 1980 році [46].

В основі цього методу лежить декомпозиція бажаного результату (БР). Тобто розбиття БР на декілька більш легких складових, як певну ієрархію, для того, щоб мати змогу обрати найважливішу, серед розбитих, складову, яка потім буде порівнюватися з іншими складовими за допомогою методу попарного порівняння.

Принцип декомпозиції передбачає структурування проблеми вибору як ієрархії рівнів з вершини (мета вибору) через проміжні рівні (показники якості системи) до найнижчого рівня (альтернативні варіанти побудови системи). Просту ієрархію МАІ можна представити наступним чином – рис.4.1 [47].

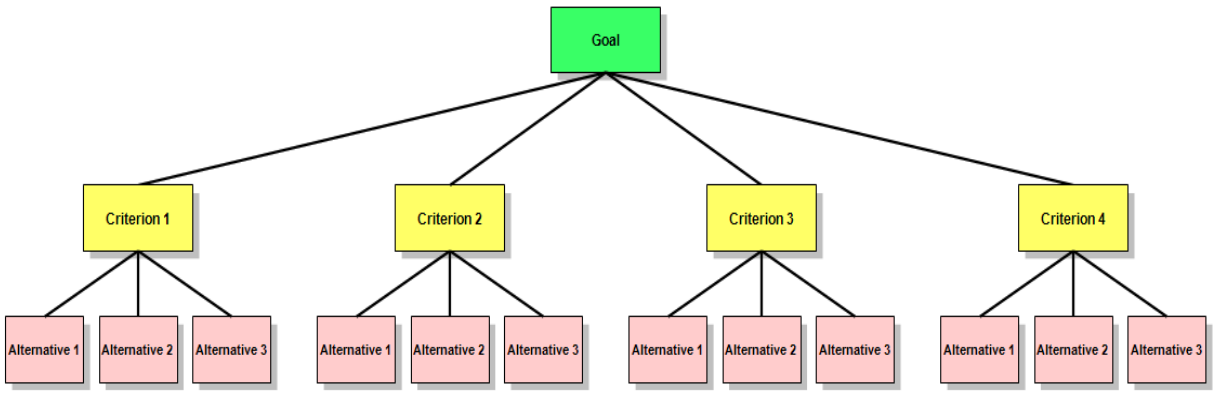

Рисунок 4.1 – Схематичне зображення декомпозиції цілі

Порівняння та оцінення складових базується або на судженнях експертів, або на судженнях конкретної особи, яка робить вибір (ОРВ).

Далі, в результаті обробки отриманих чисельних даних думок експертів або ОРВ формується матриця парних порівнянь (формула 4.1).

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1j} \\ a_{21} & a_{22} & \dots & a_{2j} \\ \dots & & & \\ a_{i1} & a_{i2} & \dots & a_{ij} \end{pmatrix}, \qquad (4.1)$$

де $a_{ij} = \frac{w_v}{w_j}$ – це оцінки певних парних порівнянь елементів вибору.

Діагональ матриці заповнюється значенням «1», а елементи матриці, що лежать нижче діагоналі, заповнюються відповідними зворотними значеннями – $1/a_{ij}$, так як матриця парних порівнянь є обернено-симетричною.

Для цієї матриці обчислюється головний власний вектор і згідно з певною математичною процедурою одержують компоненти глобального вектору пріоритетів, компоненти якого характеризують пріоритетність вибору варіантів проектованої системи. Єдиному переважному варіанту системи із заданої множини варіантів відповідає максимальне значення компонент пріоритетів глобального вектору.

Чисельні дані думок експертів або ОРВ визначаються за шкалою відносної важливості елементів, яка представлена в табл. 4.1 [48].

Таблиця 4.1 – Шкала відносної важливості елементів

Відносна важливість	Визначення
1	Рівна важливість елементів порівняння
3	Не значна перевага одного елемента над іншим
5	Істотна перевага одного елемента над іншим
7	Значна перевага одного елемента над іншим
9	Дуже сильна перевага одного елемента над іншим
2,4,6,8	Проміжні рішення між двома судженнями

Після сформування матриці за шкалою відносної важливості елементів, далі виконується певна обробка даних, яка з математичної точки зору зводиться до обчислення головного власного вектору, що відповідає максимальному власному значенню матриці.

Компоненти головного власного вектору матриці парних порівнянь показників якості обчислюються як середнє геометричне значення в рядку матриці парних порівнянь.

$$V_j = \sqrt[n]{\prod_{i=1}^{n} a_{ij}} \quad , j = \overline{1,n} \qquad (4.2)$$

де n – це кількість показників якості.

За допомогою компонентів головного власного вектору обчислюються відповідні компоненти вектору пріоритетів, які мають вигляд нормованих значень.

$$P_j = \frac{V_j}{S}, j = \overline{1,n} \qquad (4.3)$$

де $$S = \sum_{j=1}^{n} V_j \qquad (4.4)$$

Таким самим чином, продовжується знаходження оцінки матриць попарних порівнянь варіантів на наступному рівні ієрархії, окремо по відношенню до кожного показника якості системи. Тобто, спочатку такі розрахунки відбуваються на рівні 2, потім продовжуються на рівні 3.

На основі цих матриць обчислюються компоненти відповідних головних власних векторів та векторів пріоритетів систем – $\overrightarrow{Q_J}$ по відношенню до окремих показників якості систем.

Користуючись отриманими даними розраховується значення компонентів вектору глобальних пріоритетів – $\vec{C}$ відповідно до формули 4.5.

$$C_i = \sum_{j=1}^{n} P_j Q_{ij} \ , \quad i = \overline{1, N} \ , \qquad (4.5)$$

де N – число порівнюємих варіантів систем.

Бажаний варіант обирається відповідно до найбільшого значення компоненту вектору глобальних пріоритетів, тобто відповідно до формули 4.5.

4.3. Критерії вибору безпеки систем розумного будинку

Для аналізу та виявлення найбільш безпечної системи розумного будинку за допомогою MAI, потрібно визначити основні критерії безпеки систем розумного будинку.

Провівши аналіз літератури та даних стосовно безпеки систем розумного будинку було обрано наступні чотири критерії безпеки:

1. Безпечність монтажу;
2. Стійкість до збурюючих параметрів;
3. Загроза «man-in-the-middle»;
4. Післяпродажне обслуговування.

Під критерієм вибору «безпечність монтажу» систем розумного будинку можна розуміти складність встановлення системи, недоступність системи з точки зору випадкового нанесення шкоди користувачами, або навмисної – шахраями.

Система повинна встановлюватись у прихованому місці. Видим повинен залишитися тільки сенсорний екран або взагалі весь інтерфейс повинен знаходитися на телефоні, та бути схованим від сторонніх.

З точки зору початкового налаштування, певний візуальний огляд встановленої системи розумного будинку повинен бути, проте згодом, ця система повинна бути повністю прихована, або взагалі вимкнена до активації користувачем.

Для того, щоб краще розуміти критерій «Стійкість до збурюючих парметрів» слід дати роз’яснення поняттю «зубурюючі параметри».

Якщо розглядати систему розумного будинку як об’єкт управління, тобто як систему, головний вплив на яку відбувається за допомогою системи керування для досягнення необхідного результату, на який впливають різні параметри, тоді систему розумного будинку можна представити наступним схематичним чином, як зображено на рис. 4.2.

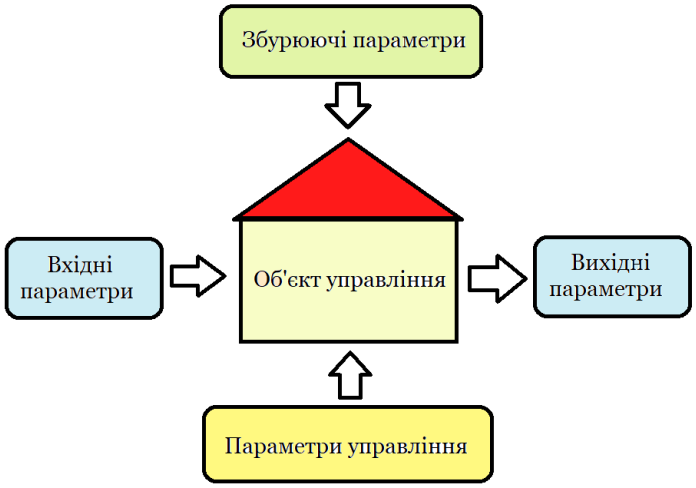

Рисунок 4.2 – Схематичне представлення системи розумний будинок як об’єкта управління

Як видно з рисунку 4.2, на систему розумного будинку впливають одразу чотири параметри:

– вхідні;
– вихідні;
– параметри управління;
– збурюючі.

Вхідні параметри об'єкта управління – це стан об’єкту чи процесу в момент часу, що приймається за початковий. У більшості моделей це нуль - початок всього.

Для системи розумного будинку вхідними параметрами є:

– джерело живлення;

– розмір будинку;

– товщина стін та матеріал з яких зроблено стіни;

– кількість вікон та матеріал з яких зроблено вікна;

– кількість радіаторів опалення та матеріал з якого зроблено радіатори;

– кількість та типи встановлених датчиків та/або сенсорів, тощо.

Вихідні параметри ОУ – фізичні параметри, які цілеспрямовано змінюються або зберігаються незмінним у процесі керування.

Вихідними параметрами для системи розумного будинку є:

– час, витрачений на передачу та отримання керуючого сигналу;

– час, витрачений на виконання команди від керуючого приладу;

– освітленість будинку;

– час, за який прогрівається будинок;

– температура будинку;

– вологість будинку;

– витрати на обслуговування будинку, тощо.

Параметри управління – це параметри об'єкта регулювання, які можливо змінювати для зміни фізичних параметрів об'єкта регулювання.

До параметрів управління системи розумного будинку можна віднести:

– заміну приладів, що вийшли з ладу;

– способи передачі керуючого сигналу (через wi-fi, zigbee, bluetooth, тощо);

– вибір датчиків та/або сенсорів (виробник, модель, параметри живлення, гарантійний термін служби);

– регулювання потужності (за допомогою димера можна плавно або східчасто регулювати потужність, напругу або струм, що подається на пристрій, зменшуючи або збільшуючи яскравість лампи, температуру нагрівання електричного обігрівача, тощо);

– вибір лампочок освітлення (наприклад, енергозберігаючі лампочки яскравіші та економніші, на відміну від звичайних);

– кількість та час відкриття вікон (цей параметр впливає на освітленність та температуру кімнати).

Збурюючі параметри – це фізичні параметри, якими неможливо керувати для зміни об'єкта регулювання.

До збурюючих параметрів системи розумного будинку можна віднести:

– пору року;

– час доби;

– температуру зовнішнього середовища;

– погодні умови;

– рівень вологості;

– вимкнення електропостачання мережі живлення;

– перепади напруги;

– збої в інтернет з’єднаннях (наприклад, якщо система керується за допомогою wi-fi, то система може взагалі перестати функціонувати).

Звичайно, від збурюючих параметрів не можливо стовідсотково застерегтися, проте, існують способи, попередження збурюючих параметрів:

– встановлення незалежного генератору живлення (він може бути екологічним, та живитися від сонячної енергії, енергії вітру, тощо);

– резервування генератору електроживлення. резервування – метод підвищення надійності об'єкту введенням надлишковості. тобто, це спосіб забезпечення надійності об'єкта за рахунок використання додаткових засобів та (або) можливостей, а саме надлишкових, відносно мінімально необхідних

для виконання потрібних функцій. тобто, замість одного генератору живлення, можна встановити один-два резервних, на випадок виходу з ладу одного з них;

– використання реле-переривника, який розмикає електричний ланцюг при підвищенні чи зниженні напруги електромережі до певних значень. коли реле перервало подачу струму, воно починає раз на кілька секунд перевіряти параметри напруги, і якщо воно в межах норми та стабільне, подача електроенергії відновиться;

– встановлення стабілізатору напруги. у разі виходу показників напруги за межі норми, стабілізатор нормалізує напругу рівно до 220 в. а, якщо, напруга підвищиться критично (наприклад до 250 в і вище в однофазному ланцюзі), стабілізатор відключить подачу електроживлення. після того, як напруга мережі стабілізується, пристрій відновить подачу струму. стабілізатор напруги встановлюється на одну розетку для одного приладу, на окремий пункт роздачі електроенергії;

– від поганих погодних умов можна застерегтися використанням розумних розеток. наприклад, якщо на вулиці ураган, гроза або інші катаклізми, саме в цей час велика ймовірність, що обірвуться дроти і стрибатиме напруга, або блискавка вдарить у ваш дім. тоді, можна підстрахуватися та вимкнути техніку підключену до розумної розетки: холодильник, телевізор, бойлер, посудомийну чи пральну машину – все, що могло працювати за вашої відсутності з будь-якої точки світу;

– від температури зовнішнього середовища можна захиститись встановленням або додаткового обігріву приладів, або навпаки, додаткового охолодження приладів (найвідоміші з них – радіатори охолодження комп’ютеру);

– від збоїв wi-fi з’єднання можна спробувати захиститися шляхом підключення додаткового інтернет з’єднання. наприклад, мобільного інтернету з функцією роздачі wi-fi.

Захищеність та стійкість системи – є одним з найголовніших критеріїв в виборі безпечної системи розумного будинку, адже під терміном «безпека», користувачі розумію не лише захищеність їх конфіденційної інформації, а й безперебійне, коректне та постійне забезпечення функціонування системи розумного будинку.

Наступним критерієм було визначено загрозу «man-in-the-middle». Як вже було описано вище, сценарій «man-in-the-middle» означає, що існує можливість підключення інших осіб до каналу між сервером та користувачем.

Тобто, ця «людина по середині» може видавати себе за когось з ключових осіб, беручи на себе роль «невидимого посередника», а це, у свою чергу, може призвести до витоку інформації, псуванню інформації, порушенню цілісності інформації, що може призвести до поганого функціонування систем розумного будинку. Саме тому, для забезпечення безпеки систем розумного будинку потрібно враховувати цей критерій.

Ще один критерій, який є необхідним для правильного функціонування системи розумний будинок – це підсяпродажне обслуговування.

Післяпродажне обслуговування – це сукупність послуг, які надаються компанією користувачам після придбання товару або послуг [49].

До післяпродажного обслуговування можна віднести:

– ремонт;
– постачання запчастин;
– консультації користувачів;
– монтаж;
– налагодження;
– підтримка та оновлення програмного забезпечення.

Під критерієм вибору «Післяпродажне обслуговування» в системах розумного будинку можна розуміти складність підтримки роботи системи, оновлення прошивок, монтаж системи, забезпечення спеціалістами та деталями у випадку поломки.

4.4. Визначення альтернатив та побудова ієрархії бажаного варіанту безпеки систем розумного будинку

Сформувавши критерії вибору з точки зору безпеки систем розумного будинку потрібно визначити системи, які будуть порівнюватися та аналізуватися за допомогою MAI.

З точки зору основних типів управління системами розумного будинку можна визначити три головні типи:

- провідна система;
- безпровідна система;
- мішана система.

Провідна система – це передача керуючого сигналу від центрального процесора до всіх датчиків і виконавчих механізмів відбувається за допомогою проводів [50]. Переважно використовується вита пара, проте існують рішення з використанням силових кабелів.

Головною перевагою провідної системи є надійність та стабільність з точки зору передачі та отримання керуючого сигналу, адже вони надходять за допомогою спеціальних прокладених кабелів, що водночас слугує й джерелом живлення.

Недоліки такої системи полягають в складності монтажу та великій кількості дротів, адже кожен датчик повинен мати свій персональний дріт. Такі системи рекомендується встановлювати на початку ремонту та по спеціальному проекту підібраному конкретно під потреби користувача.

Безпровідна система – це система, яка надсилає керуючі сигнали до датчиків та виконавчих механізмів за допомогою радіохвиль. Цими радіохвилями можуть бути Wi-Fi, Bluetooth, ZigBee, Z-Wave, тощо.

Перевагою таких систем є менша кількість проводів, простіші методи монтажу, можливість оновлень, перестановок та змін дизайну.

Недоліками такої системи є те, що керуючі сигнали або інформаційні сигнали надходять довше, є обмеження в радіусі дій та живленні пристроїв, адже акумулятори потребують постійного контролю живлення та підзарядки.

Через складність інсталяції провідних систем та обмежений радіус дій почали з’являтися пропозиції щодо встановлення так званої мішаної системи розумного будинку, де керування відбувається частково через дроти та радіосигнали.

Визначивши варіанти альтернатив можна скласти таблицю показників альтернатив відносно обраних критеріїв (табл. 4.2)

Таблиця 4.2 – Таблиця показників альтернатив відносно критеріїв

Альтернативи	Безпечність монтажу	Стійкість до збурюючих параметрів	Загроза «man-in-the-middle»	Післяпродажне обслуговування
Провідна система (N1)	середня	висока	невисока	висока
Безпровідна система (N2)	висока	невисока	висока	висока
Мішана система (N3)	середня	середня	середня	середня

Обравши альтернативи та критерії вибору, тобто декомпозитувавши проблему бажаного результату, можна побудувати схему ієрархії безпеки систем розумного будинку (рис. 4.3).

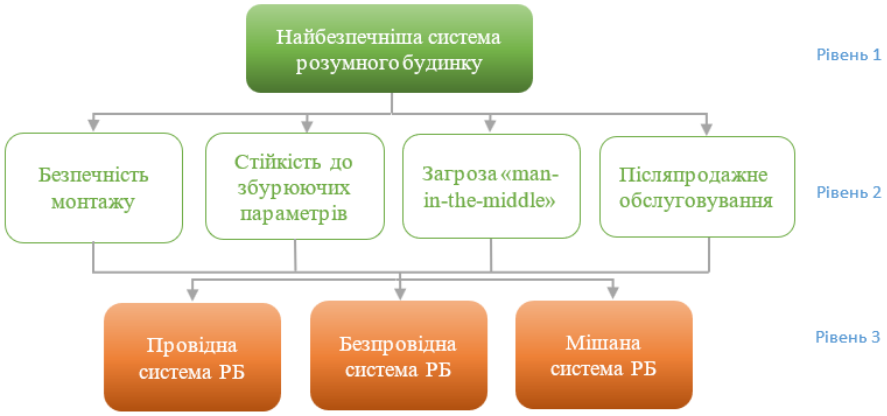

Рисунок 4.3. – Схема ієрархії безпеки систем розумного будинку

Обґрунтувавши вибір, визначивши альтернативи та критерії вибору безпеки систем розумного будинку, можна перейти до розрахунку отримання БР за допомогою MAI. Також, слід зауважити, що розрахунок буде відбуватися відповідно до даних думок ОРВ.

4.5. Розрахунок бажаного варіанту безпеки систем розумного будинку методом аналізу ієрархій

Перший етап розрахунку – це визначення пріоритетності обраних критеріїв відповідно даних думок ОРВ та таблиці 4.1 шляхом використання методу «Середньо геометричного значення рядка». Для цього потрібно знайти добуток n елементів кожного рядка – П, та витягти корінь n-го ступеню з отриманого П. Результати розрахунків наведено нижче у таблиці 4.3.

Пояснення значень, використаних у таблиці 4.3.

C1 – Безпечність монтажу;

C2 – Загроза «man-in-the-middle»;

C3 – Стійкість до збурюючих параметрів;

C4 – Післяпродажне обслуговування;

V_j – Компоненти головного власного вектору;

P_j – Компоненти вектору пріоритетів.

Таблиця 4.3 – Таблиця пріоритетності критеріїв

	C1	C2	C3	C4	П	Vj	Pj
C1	1	7	2	5	70	2,893	0,523
C2	1/7	1	1/5	1/3	0,010	0,312	0,057
C3	1/2	5	1	3	7,5	1,655	0,299
C4	1/5	3	1/3	1	0,2	0,669	0,121
					Сума V =	5,529	

За даною таблицею можна зробити висновок, що для ОРВ найголовнішим критерієм вибору системи розумного будинку є – безпечність монтажу, а незначним серед представлених є – стійкість до загрози «man-in-the-middle». Тобто, для ОРВ більш важливо зберегти функціонування системи розумного будинку, а ніж стійкість до перехвату даних.

Зрозумівши потреби ОРВ можна продовжити подальші розрахунки для підбору найоптимальнішого варіанту системи розумний будинок.

Наступний розрахунок визначить систему, у якої, на експертну думку ОРВ, найбільша безпечність монтажу. Результати представлено у таблиці 4.4.

Таблиця 4.4 – Визначення системи відповідно безпечності монтажу

Безпечність монтажу	N1	N2	N3	П	Vj	Pj
N1	1	1/4	1/3	0,083	0,437	0,117
N2	4	1	3	12	2,289	0,614
N3	3	1/3	1	1	1	0,268
				Сума V =	3,726	

Серед обраних систем розумного будинку, найбільш безпечний монтаж з точки зору експертної думки ОРВ має бездротова система розумного будинку.

Наступний розрахунок – це визначення системи з найбільшою стійкістю до збурюючих параметрів, базуючись на експертній думці ОРВ – таблиця 4.5.

Таблиця 4.5 – Визначення системи стійкої до збурюючих параметрів

Стійкість до збурюючих параметрів	N1	N2	N3	П	Vj	Pj
N1	1	9	6	54	3,78	0,749
N2	1/9	1	1/6	0,019	0,265	0,071
N3	1/6	6	1	1	1	0,268
				Сума V =	5,044	

Найбільш стійкою системою, з точки зору ОРВ є – провідна система розумного будинку.

Наступним за важливістю критерієм відповідно до експертної думки є – післяпродажне обслуговування. Розрахунки критерію відповідно до систем розумного будинку наведено у таблиці 4.6.

Таблиця 4.6 – Визначення системи розумного будинку відповідно до післяпродажного обслуговування

Післяпродажне обслуговування	N1	N2	N3	П	Vj	Pj
N1	1	2	5	10	2,154	0,582
N2	1/2	1	3	1,5	1,145	0,307
N3	1/5	1/3	1	0,067	0,405	0,109
				Сума V =	3,70463	

Провідна система розумного будинку, відповідно до думки ОРВ, має найбільш краще післяпродажне обслуговування, а мішані системи РБ – найгірше.

Останнім критерій за яким будуть порівнюватися системи розумного будинку з точки зору безпеки – стійкість до загрози «man-in-the-middle». У таблиці 4.7.

Таблиця 4.7 – Порівняння стійкості систем розумного будинку щодо загрози «man-in-the-middle»

Загроза «man-in-the-middle»	N1	N2	N3	П	Vj	Pj
N1	1	8	6	48	3,634	0,761
N2	1/8	1	1/3	0,042	0,347	0,093
N3	1/6	3	1	0,5	0,794	0,213
				Сума V =	4,775	

Найбільш стійкою системою до загрози «man-in-the-middle» є – провідна система розумного будинку, а найменш стійкою є – безпровідна система.

Отримавши порівняння альтернатив відносно усіх критеріїв безпеки систем розумного будинку, можна визначити найбільш безпечну систему розумного будинку відповідно до експертної думки ОРВ. Таблицю розрахунку наведено нижче.

Таблиця 4.8 – Визначення найбільш безпечної системи розумного будинку

Альтернативи	Безпечність монтажу	Стійкість до збурюючих параметрів	Загроза «man-in-the-middle»	Післяпродажне обслуговування	Оцінка
Pj	0,523	0,057	0,299	0,121	
Провідна система	0,117	0,749	0,761	0,582	0,402
Безпровідна система	0,614	0,071	0,093	0,307	0,390
Мішана система	0,268	0,268	0,213	0,109	0,232

Відповідно до експертної думки ОРВ та визначеної пріоритетності критеріїв вибору систем розумного будинку методом MAI було визначено найбільш безпечну систему розумного будинку – провідна система РБ.

Безпровідна система отримала оцінку лише на 0,1 бал нижче, що свідчить про те, що ця система є цілком безпечною, та може рекомендуватися ОРВ.

Найнижчий бал отримала мішана система РБ, проте, це не означає, що система є небезпечною у використанні, та не може рекомендуватися. Отримані результати свідчать лише про те, що ця система не рекомендується відповідно до такого розташування пріоритетності критеріїв та експертної думки ОРВ.

5. ЕКОНОМІЧНЕ ДОСЛІДЖЕННЯ

5.1. Розрахунок створення моделі безпеки системи розумного будинку

Кожний прилад, кожна система проходить етап розробки. Це потрібно для того, щоб в процесі створення прорахувати та проаналізувати найбільш кращий варіант реалізації, визначити усі можливі труднощі, які можуть виникнути, зробити чіткий план дій задля досягнення бажаного результату з відсутнім або мінімальними відхиленнями від проекту [51].

Процес створення моделі безпеки системи розумного будинку можна умовно поділити на чотири етапи:

1. Підготовка;
2. Проектування;
3. Створення;
4. Фінальне узгодження.

В перший етап входить збір та упорядкування необхідних вимог, попереднє планування етапів та умов робіт, строків виконання, визначення приблизних ресурсів та вартості, вибір типу системи методом МАІ, ознайомлення з місцем, де в подальшому буде встановлено безпеку системи розумного будинку, тощо.

До етапу проектування можна віднести – отримання та узгодження з замовником технічного завдання, розробка специфікацій, кошторисів, ознайомлення та аналіз існуючих проектних рішень, тощо.

Етап створення, у свою чергу, можна поділити на три стадії:

1. Дизайн;
2. Тестування;
3. Документування.

До дизайну можна віднести отримання графічних моделей, створення персонального стилю, розробка інтерфейсу, розробка схеми безпечного монтажу моделі безпеки системи розумного будинку.

Документування – це розробка технічної документації стосовно створеної моделі безпеки системи розумного будинку.

Останній етап створення моделі безпеки системи розумного будинку – це фінальне узгодження. До цього етапу можна віднести умов реалізації створеної моделі безпеки системи розумного будинку. Також, до цього етапу відноситься супровід – це виправлення помилок, узгодження з замовником, тощо.

Система розумного будинку має доволі складний процес реалізації, адже це багатоскладова система, що потребує багатогалузевих знань та навиків. Це означає, що для створення моделі безпеки системи розумного будинку потрібне залучення фахівців з різних галузей знань. Строки розробки, кількість фахівців необхідних для створення проекту системи розумного будинку наведено у таблиці 5.1.

Таблиця 5.1 – Дані для створення проекту системи розумного будинку

Назва етапу	Кількість робочих днів	Кількість спеціалістів
Підготовка	2	3
Проектування	5	4
Створення	5	4
Підтримка	10	3

Для того щоб визначити та візуалізувати терміни створення моделі системи розумного будинку на рисунку 5.1 наведено лінійний графік залежності стадій розробки від терміну виконання.

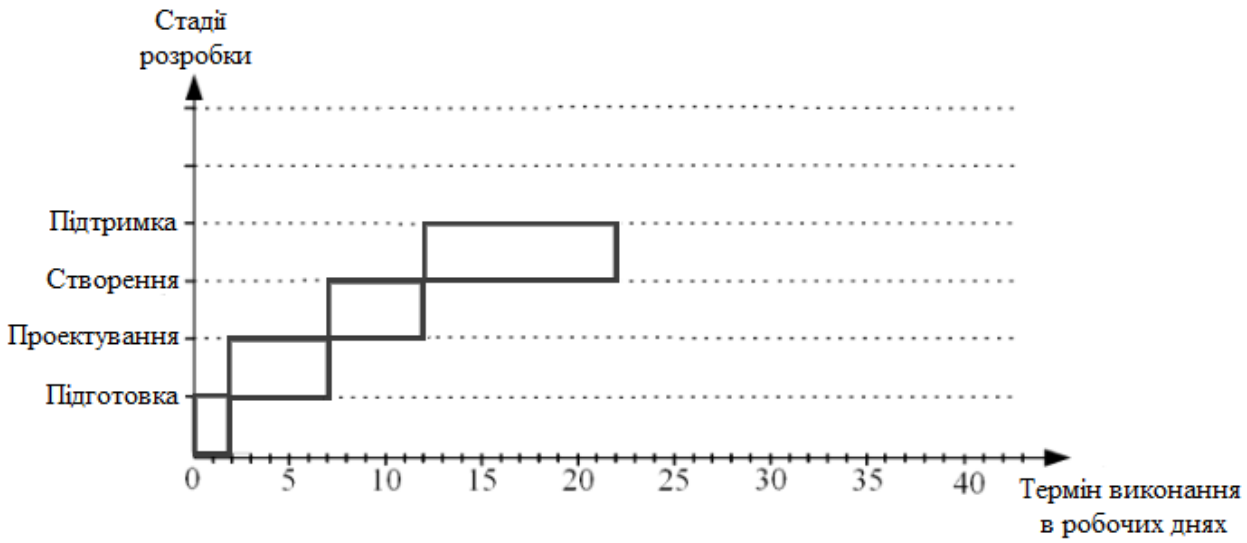

Рисунок 5.1 –Графік терміну створення проекту системи розумного будинку

На виконання проекту системи розумного будинку витрачено 22 робочих дня.

У таблиці 5.2 наведено необхідний перелік працівників та кількість робочих годин для реалізації моделі безпеки системи розумного будинку.

Таблиця 5.2 – Перелік співробітників проекту та кількість робочих годин

Посада робітника	Кількість робочих годин
Директор проекту	176
Інженер з монтажу та розробки	160
Дизайнер	176
Кошторисник	96

Визначивши кількість робочих годин кожного з робітників, необхідних для створення однієї моделі безпеки системи розумного будинку, можна визначити заробітну плату працівників. Заробітна плата розраховується за формулою 5.1. Результати наведено у таблиці 5.3.

$$ЗП = N_{роб} \cdot T_{сер} \cdot В \qquad (5.1)$$

де, $N_{роб}$ – кількість учасників проекту;

$T_{сер}$ – заробітна ставка кожного співробітника (грн./год.);

В – кількість годин витрачених на проект.

Таблиця 5.3 – Розрахунок заробітної плати робітників за проект

Працівник	$N_{роб}$	$T_{сер}$	В	ЗП
Директор проекту	1	130	176	22 880
Інженер з монтажу та розробки	1	113	160	18 080
Дизайнер	1	97	176	17 072
Кошторисник	1	108	96	10 368
Загальна сума				68 400

Наступний розрахунок, необхідний для створення моделі безпеки системи розумного будинку – кошторис витрат. Він складається з таких показників:

– основні технічні засоби (комп'ютер з програмним забезпеченням);

– заробітна плата;

– відрахування до єдиного фонду – 37%;

– накладні витрати (60…150% від фонду заробітної плати), які включають різні господарські та адміністративні витрати.

У таблиці 5.4 наведено розрахунок вартості технічного забезпечення з розрахунку на три роки роботи компанії. Оскільки приблизний термін виконання одного проекту – 1 місяць, як наслідок за рік компанія виконає 12 проектів, а за три роки – 36.

Таблиця 5.4 – Вартість технічного забезпечення за один проект

Найменування технічного забезпечення	Кількість	Загальна вартість одиниці	Ціна одиниці, грн.	Вартість, грн.
Ноутбук	4	14 000	388,89	1 555,56
Програма для дизайну інтер'єру	1	1 390	115,83	115,83
Програма 1С для кошторисника	1	2 240	186,66	186,66
Інженерне устаткування	1	5 000	416,67	416,67
Загальна сума				2 274,72

Розрахунок амортизації основних засобів:

$$S_{аморт} = \sum \frac{a_{ам}}{100} \cdot вартість \cdot \frac{T_{вик}}{T_{можвик}} \qquad (5.2)$$

$$S_{аморт} = 0,15 \cdot 2\,274,72 \cdot (32 \cdot 8/2100) = 41,59 \text{ грн.}$$

Електроенергія, що витрачається при роботі над проектом:

$$S_e = \text{тариф} \cdot \text{потужність} \cdot N \cdot T_{вик} \qquad (5.3)$$

де N – кількість комп'ютерів.

$$S_e = 1,68 \times 0,5 \times 4 \times 256 = 860,16 \text{ грн.}$$

У таблиці 5.5 наведено загальний кошторис витрат на створення моделі безпеки системи розумного будинку.

Таблиця 5.5 – Загальний кошторис витрат

Найменування витрат	Вартість, грн
Технічне забезпечення	2 274,72
Амортизація основних засобів	41,59
Витрати на електроенергію	860,16
Заробітна плата робітникам	68 400,00
Загальна сума	71 576,47

Провівши розрахунки можна зробити висновок, що забезпечення безпеки систем розумного будинку підвищує вартість системи, але не значно. Тому, застосування та покращення безпеки систем розумного будинку є раціональним та рекомендованим користувачам систем.

6. ОХОРОНА ПРАЦІ ТА ТЕХНІКА БЕЗПЕКИ НА ВИРОБНИЦТВІ

6.1. Загальні положення з охорони праці та техніки безпеки на виробництві

Підчас виробництва працівники повинні чітко дотримуватися правил техніки безпеки, незалежно від посади та обов'язків. Якщо кількість людей, які працюють в компанії перевищує 50, тоді підприємство зобов'язано мати відділ з охорони праці відповідно статті 15 Законодавства України «Про Охорону праці» [51]. Цей департамент буде підпорядковуватися роботодавцю.

Також, потрібно враховувати, що незалежно від форми та виду підприємства, якщо є наймані робітники, тоді підприємство повинно розробити та мати усі документи стосовно охорони праці відповідно до чинного законодавства, розкладу робіт та специфіки видів діяльності. До таких документів можна віднести наступні:

– нормативну документацію – це норми, закони, типові положення, правила, знаки, бланки, тощо;

– розпорядчу документацію – розпорядження, накази, інструкції, тощо;

– звітну документацію – форми офіційної статистичної звітності;

– облікову документацію, яка відображає усю діяльність підприємства відповідно до законів про охорону праці – це журнали, протоколи, графіки, схеми, тощо.

Уся документація повинна зберігатися в порядку, зручному для використання та у випадку перевірки, зручному для перевіряючих органів.

Також, кожен з робітників, перед початком робіт на підприємстві повинен пройти інструктаж з охорони праці ЫІ[52]. Ці інструктажі можна поділити на:

– вступний;

– первинний;

– повторний;

– позаплановий;

– цільовий.

Вступний або водний інструктаж проводиться один раз при прийнятті співробітника на роботу перед початком виконання робіт. Також, проводиться незалежно від професії, посади, стажу робіт та строку перебування на підприємстві. Цей інструктаж є обов’язковим для щойно найнятих робітників, для тимчасових робітників, робітників, які знаходяться на вашому підприємстві у відрядженні, для, студентів-практикантів, учнів шкіл, тощо.

Без проходження вступного інструктажу робітник не може допускатися до виконання робіт на підприємстві.

Цей інструктаж проводиться інженером з охорони праці, або лицем, який має повноваження відповідно до наказу роботодавця, по чіткому, узгодженому роботодавцем плану та програми.

Після проходження вступного інструктажу відбувається перевірка знань методом опитування. Після опитування у журналі проходження вступного інструктажу з охорони праці робиться запис з обов’язковим підписом особи, яка проходила інструктаж та особи, яка проводила інструктаж.

Первинний інструктаж повинен проводитися перед початком робіт керівником підрозділу, майстром, якому буде підпорядковуватися робітник. Цей інструктаж проводиться безпосередньо на робочу місці. Цей інструктаж проводиться з:

– робітниками підрозділу, які були щойно прийняті на роботу, а також працівниками, які виконують роботу на умовах трудового договору, укладеного до двох місяців або на період виконання сезонних робіт, у вільний від основної роботи час, а також вдома з використанням матеріалів, інструментів і механізмів, що виділяються роботодавцем або придбаних за власні кошти;

– працівниками організацій, які були переведені в установленому порядку з іншого структурного підрозділу, та/або працівниками, яким було

доручено виконання нової роботи з якою дані робітники не зіштовхувалися раніше;

– працівниками сторонніх організацій, які знаходяться у відрядженні на вашому підприємстві, особи, які навчаються в освітніх установах відповідних рівнів, які проходять виробничу практику на вашому підприємстві, та іншими особами, які беруть участь у виробничій діяльності підприємства.

Первинний інструктаж повинен проводитися за чітко розробленою та затвердженою роботодавцем програмою інструктажу на робочому місці з метою отримання конкретних, відповідних специфіки роботи знань, за для безпечного виконання виробничого завдання на робочому місці.

Програма первинного інструктажу передбачає:

– загальне ознайомлення з технологічним процесом на конкретній ділянці роботи;

– ознайомлення з обладнанням, з небезпечними зонами обладнання та огорожами для захисту від травмування;

– ознайомлення та демонстрація з порядком підготовки приладу або робочої зони до роботи. Наприклад – перевірка справності обладнання, приладу загалом, його пускових приладів, заземлюючих пристроїв, інструментів, тощо;

– порядок застосування запобіжних заходів та пристроїв;

– вимоги до спеціального одягу, спеціального взуття та інших ЗІЗ робітника при роботі на робочому місці, та при роботі з робочим обладнанням;

– випадки виробничого травматизму, їх причини та шляхи уникнення;

– вимоги безпеки до електроустаткування, освітлювальних приладів, приладів під напругою, тощо;

– правила безпеки під час спільного виконання робіт разом з іншим робітником, або робітниками;

– заходи надання першої допомоги за нещасних випадків, особисту гігієну робітника;

– ознайомлення з відповідальністю робітника за порушення правил техніки безпеки.

Первинний інструктаж з охорони праці на робочому місці проводить проводиться з кожним працівником.

Після завершення первинного інструктажу на робочому місці інструктований робітник повинен зареєструватися в журналі та карті особи з підписом інструктора та інструктованого.

Знову прийнятий працівник повинен проходити стажування від 2 до 14 змін під ретельним наглядом керівника підрозділу або майстра, чи досвідченого працівника. Після цього, керівник підрозділу перевіряє роботу новоприйнятого працівника, засвоєння ним вимог норм техніки безпеки та отримує допуск до роботи шляхом ставлення підпису у журналі інструктажів.

Повторний інструктаж проводиться двічі на рік, тобто не рідше ніж раз на 6 місяців. Його проходять усі робітники, які проходили первинний інструктаж з техніки безпеки. Робітники, які обслуговують прилади підвищеної небезпеки проходять повторний інструктаж не рідше ніж раз на три місяці.

Повторний інструктаж здійснює керівник робіт, це може бути керівник підрозділу, майстер, інструктор виробничого навчання, тощо.

Повторний інструктаж відбувається за програмою, яка була розроблена для попереднього інструктажу. Метою повторного інструктажу є – перевірити та підвищити рівень знань інструкцій з охорони праці та ТБ.

Цей інструктаж може бути проведеним як індивідуально з кожним робітником, так і з групою працівників однієї професії.

Після завершення повторного інструктажу на робочому місці інструктований робітник повинен зареєструватися в журналі та карті особи з підписом інструктора та інструктованого.

Позаплановий інструктаж – це інструктаж, який повинен проводитися у випадку:

– введення в експлуатацію нових, або оновлених стандартів, правил, або інструкцій з охорони праці;

– при повному зміненню технологічного процесу, модернізації обладнання та/або інструментів, вихідного продукту, використовуваних матеріалів та інших факторів, які впливають на безпеку робітників підчас праці;

– при порушенні працівником або працівниками вимог, норм, інструкцій з охорони праці, особливо у випадку, якщо ці порушення створили або могли створити загрозу несприятливих та небажаних наслідків робітникам або підприємству. Наприклад – створення аварійної ситуації, небезпечне поводження з приладами, травмування робітників через необережність, тощо;

– на вимогу посадових осіб;

– при перервах у роботі: для робіт із шкідливими та/або небезпечними умовами праці понад 30 днів, а для решти робіт – понад 2 місяці;

– за рішенням роботодавця або уповноваженої роботодавцем особи.

Позаплановий інструктаж здійснюється безпосередньо керівник робіт, це може бути керівник підрозділу, майстер, інструктор з техніки безпеки, тощо.

Після завершення позапланового інструктажу на робочому місці інструктований робітник повинен зареєструватися в журналі та карті особи з підписом інструктора та інструктованого.

Цільовий інструктаж має бути проведеним у випадку виконання разових робіт, які не мають прямого відношення до спеціальних обов'язків, наприклад: навантаження, вивантаження, територіальне прибирання, роботи разові, які будуть проведені поза відділом підприємства, тощо. У випадку ліквідації наслідків аварійних ситуацій, стихійних лих або катастроф. Під час проведення екскурсійних заходів або при організації масових заходів із практикантами, студентами, учнями загально освітніх шкіл, тощо.

Цільовий інструктаж проводиться керівником робіт – майстром, інструктором виробничого навчання, викладачем, або особа, яка була назначена роботодавцем.

Окрім проведення інструктажу, роботодавець повинен придбати робітникам засоби індивідуального захисту (ЗІЗ), а також подбати про наявність повного комплектування, видачу та зберігання в стані дозволеному для використання ЗІЗ відповідно до нормативно-правових актів з охорони праці. Найбільш розповсюдженими ЗІЗ є – засоби захисту голови, очей, органів дихання, спеціальний одяг та взуття зображених на рисунку 6.1.

Рисунок 6.1 – Приклади ЗІЗ

ЗІЗ також можна поділити за групами захисту:

Перша група захисту – це ЗІЗ, які захищають робітників від механічних впливів робочого середовища, виробничих забруднень загального типу, від води, від речовин, які є нетоксичними та або їх розчинів, від пилу, який не є токсичним, від стирання, від порізів, від вібрації, від шуму, від можливості пошкодження різних частини тіла, від падання при роботі на висоті і засоби порятунку з висоти, від пилу, азбесту, дисперсного пилу, тощо.

До другої групи захисту відносять захист від хімічних факторів, наприклад від токсичних речовин, як кислоти, луги або різних органічних

розчинів або розчинників, такі як лак та фарба на їх основі, нафти, нафтопродуктів, олій та жирів.

До неї входять підгрупи захисту від токсичних речовин, які мають твердий агрегатний стан, від різних концентрацій кислот та лугів, від органічних розчинників, ароматичних або не ароматичних речовин, хлорованих вуглеводнів, сирої нафти, продуктів легкої фракції, нафтових олій та продуктів важких фракцій, рослинних та тваринних олій та жирів .

Третя група захисту – від біологічних чинників. До неї входять підгрупи захисту від мікроорганізмів, комах та павукоподібних.

Четверта група захисту – від радіаційних чинників. До неї входять підгрупи захисту від забруднень радіоактивних або іонізуючих випромінювань.

П'ята група захисту – від високих або навпаки низьких температур, від можливих бризків нагрітого або розплавленого матеріалу. Включає підгрупи захисту від температурного випромінювання, полум’я, іскор, бризок і виплесків розплавленого матеріалу, захищає від контакту з поверхнями температура яких понад 45°С, від 40 до 100°С, від 100 до 400°С, від температури повітря яка є нижче від -20°С до -50°С, від контакту з дуже холодними або охолодженими поверхнями;

Шоста група захисту – це захист від електричної дуги, та наслідків ураження електричною дугою, від неіонізуючих випромінювань, уражень струмом, впливу статичної електрики, тощо. До неї відносяться підгрупи захисту від електричного ураження напругою до та понад 1000 В, електромагнітних полів.

Група захисту сім складається з одягу спеціальної сигнальної підвищеної видимості.

Восьма група захисту – це комплексні ЗІЗ.

Дев'ята група захисту включає в себе дерматологічні ЗІЗ. До цієї групи входять підгрупи захисту засобів гідрофільної, гідрофобної, комбінованої дії, від впливу низьких температур, високих температур, вітру, ультрафіолетового

випромінювання діапазонів А, В, С, комах, мікроорганізмів, що очищають, регенерують, відновлюють засоби [53, 54].

6.2. Електробезпечність підчас виконання робіт

Систем розумного будинку – це один з видів електроустаткування. Уся електронна частина потребує живлення, в особливості провідна система розумного будинку, де для забезпечення функціонування системи потрібне постійне електроживлення. Це, у свою чергу, викликає необхідність постійного ознайомлення та вивчення техніки безпеки та електробезпеки в цілому. Як під час виробництва так і підчас користування потрібне невідхильне дотримування правил ТБ та поводження з електроустаткуванням.

В галузі електробезпеки повинне бути чітке ґрунтування на конкретній системі заходів, щодо забезпечення повного та точного виконання «Правил технічної експлуатації електроустановок споживачів» та «Правил техніки безпеки під час експлуатації електроустановок споживачів».

Особлива увага роботодавців та керівників повинна бути приділена невідхильному виконанню вимог зазначених норм стосовно утримування та експлуатації електричних приладів та систем.

Електроустановки у яких напруга до 1000 В і понад 1000 В поділяються на дві групи. Парадоксально, проте відповідно статистиці найбільша кількість електротравм частіше відбувається при роботі з електроустановками напруга яких не перевищує 1000 В.

Найбільшу увагу слід приділити порушенням таким як:

– доторкання до відкритих струмоведучих частин та дротів устаткування;

– доторкання до струмоведучих частин, у яких була пошкоджена або відсутня ізоляція;

– доторкання до металевих частин не заземленого устаткування, яке опинилося під напругою;

– доторкання до струмоведучих частин предметами із низькою ізоляційною здатністю;

– відсутності чи порушення заземлення;

– подання напруги під час ремонтних робіт або оглядів устаткування.

– ураження через дугу електричним струмом та ін.

Для наглядного прикладу впливу електричного струму на організм людини нижче наведено таблицю 6.1, де описано впливу на тіло людини електричного струму в залежності від його струму [55].

Таблиця 6.1 – Вплив електричного струму на тіло людини

Сила струму, мА	Змінний струм 50 — 60 Гц	Постійний струм
0,6 — 1,5	Легке тремтіння пальців рук	Не відчутно
2 — 3	Сильне тремтіння пальців рук	Не відчутно
5 — 7	Судороги в руках	Зуд. Відчуття нагріву
8 — 10	Руки важко, але ще можна відірвати від електродів. Сильні болі в руках, особливо в кистях та пальцях	Більш сильніше відчуття нагрівання
20 — 25	Руки паралізуються негайно, відірвати руки від електродів неможливо. Дуже сильний біль. Важке дихання	Ще більше посилення нагрівання, незначне скорочення м'язів рук
50 — 80	Параліч дихання. Початок тріпотіння шлуночків серця	Сильне відчуття нагрівання. Скорочення м'язів рук. Судоми. Утруднення дихання
90 — 100	Параліч дихання та серця при дії понад 0,1 с.	Параліч дихання

Окрім описаних вище впливів також можуть бути електричні опіки, знаки, або металізація шкіри.

Електричні опіки різного ступеня – результат короткого замикання електроустановок і постійної присутності тіла, зазвичай рук, у сфері світла ультрафіолетових та теплових інфрачервоних впливів електродуги, а також опіки третього та четвертого ступенів з важкими наслідками - при контакті людини прямо або через електродугу зі струмом напругою понад 100 В.

Електричні знаки відмітки струму є специфічними ураженнями, спричиненими механічними, хімічними або їх сполученими впливами. Уражена область шкіри майже безболісна, довкола неї немає запальних процесів. Згодом вона затвердіє, а поверхнева тканина відмирає. Електрознаки, зазвичай, швидко зцілюються.

Металізацією шкіри є - просочення шкіри дрібними паровими або плавними частинами металу під впливом механічних чи хімічних впливів струмів. Уражені ділянки шкіри мають жорстку поверхню і характерне забарвлення. Металізація найчастіше виліковується, не залишивши слідів на шкірі.

У виробничих умовах ураження електричним струмом часто виникає через торкання людей до струмопровідних частин, що знаходяться під небезпечною напругою.

Розрізняють два види небезпечного доторкання людиною струмопровідних частин: небезпечне – це доторкання до однієї струмопровідної частини (рис. 6.2), та більш небезпечне – це доторкання до обох частин (рис. 6.3).

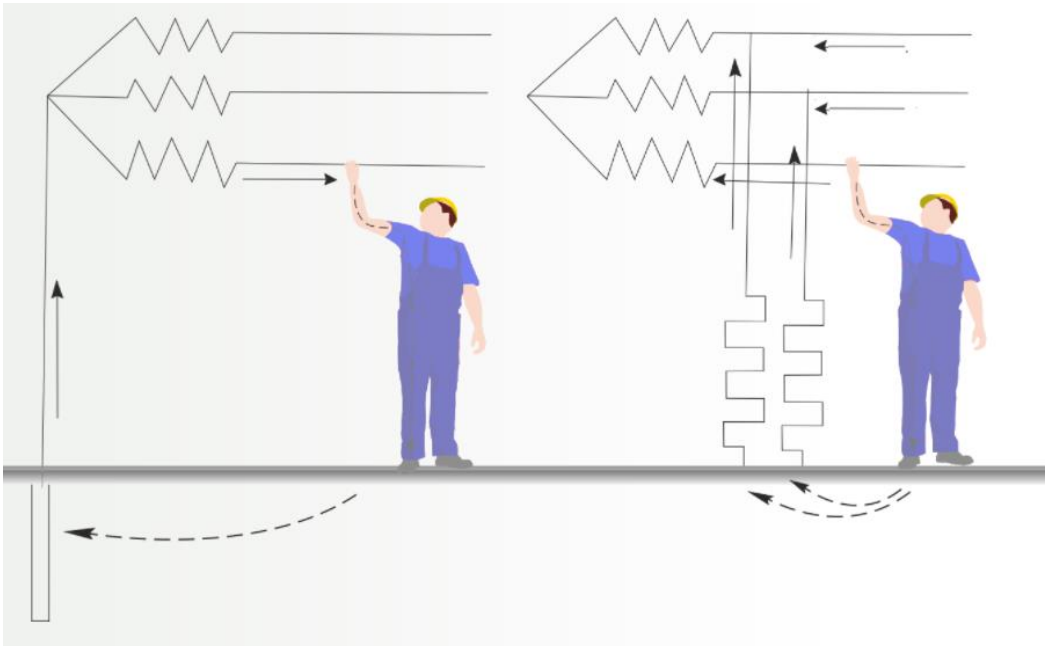

Рисунок 6.2 – Однофазне включення людини у ланцюг: а) з заземленням нейтралі; б) з ізольованою нейтраллю

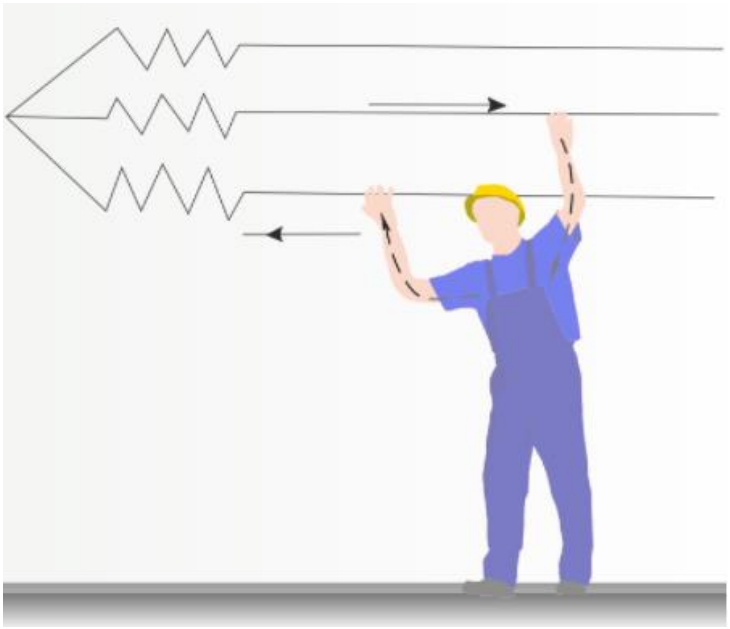

Рисунок 6.3 – Двофазне включення людини у ланцюг

Можливе попередження ураження людей струмом на підприємстві можливе, якщо дотримуватися наступного:

– використовувати технічні рішення, які роблять можливість приєднання людей до ланцюга струму двох фаз або однієї фази і землі мінімальним. таким чином, струмоведуча частина, що нормально перебуває в напрузі, недоступна випадковому дотику;

– забезпечення надійної ізоляції, огорожі, розташування приладів на достатній відстані або під землю, або ін.;

– використання захисних заземлювальних пристроїв або автоматичних вимикачів, що забезпечують при пошкодженнях ізоляції обмежують напругу або вимикають несправну техніку;

– використовування напруги електроустановок, безпечної для працівників, що буде відповідати умовам експлуатації;

– урахування при плануванні електробезпеки вологість, струмопровідний пил, їдкий пар і гази, що призводять до руйнування теплоізоляції, струмову підлогу та кількість достатньо велику саме заземлюючих металевих обладнань, яке може навпаки призвести до підвищення небезпеки ураження.

Пропонуючи рішення щодо забезпечення безпечнішої експлуатації електрообладнання неможливо оминути такий метод, як заземлюючий пристрій. Так називають навмисні електричні з’єднання обладнання та землі заземлювачами. Це виконується задля зменшення напруги до безпечної. Відповідно до правил ТБ, опір захищеного заземлення повинен не перевищувати 4 Ом.

Головними умовами при будівництві заземлювального пристрою, є розмір заземлювального пристрою.

За матеріалами, такими як: куточки, смуги, круглі сталі, мінімальний розмір заземлювача повинен мати параметри не менші ніж:

- смуга 12х4 – 48 мм2;
- куточок 4х4;
- кругла сталь – 10 мм2;
- сталева труба – 3.5 мм.

Розмір арматури, мінімальний, задля для встановлення заземлювального пристрою зображено на рисунку 6.4

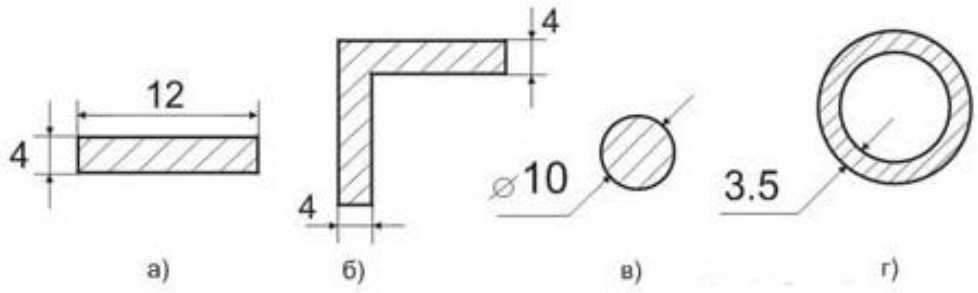

Рисунок 6.4 – Розмір арматури для заземлювального пристрою

Заземлюючий стержень відносно своєї довжини також має певні мінімальні обмеження, а саме – не менше ніж 1,5-2 м (рис. 6.5).

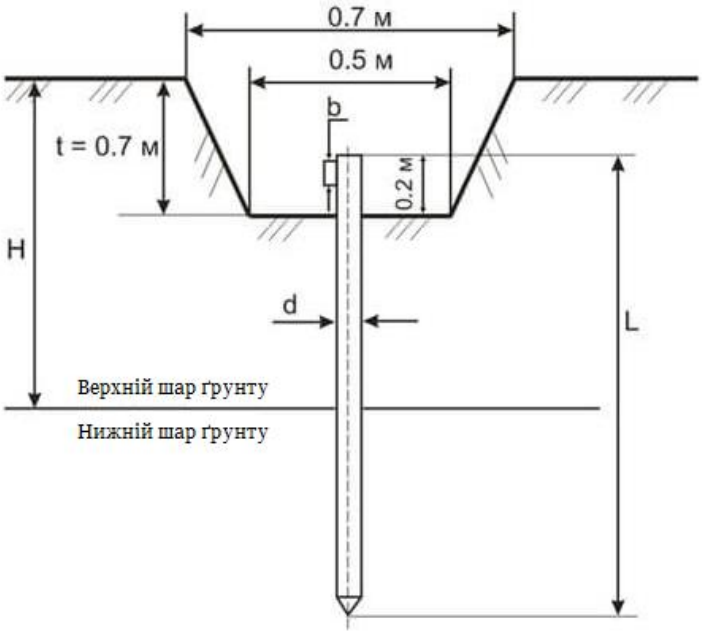

Рисунок 6.5 – Приклад заземлюючого пристрою

Остання складова заземлюючого пристрою, яка також має лімітовані та стандартизовані обмеження довжини – це відстань між стрижнями.

Найчастіше, пропонується співвідношення довжини до стрижня наступне – a = 1xL; a = 2xL; a = 3xL. Проте, розміщення стрижнів може бути як трикутним, так і квадратним, або іншої геометричної фігури, яке буде запропоноване проектувальником. На рисунку 6.6 зображено креслення стрижнів.

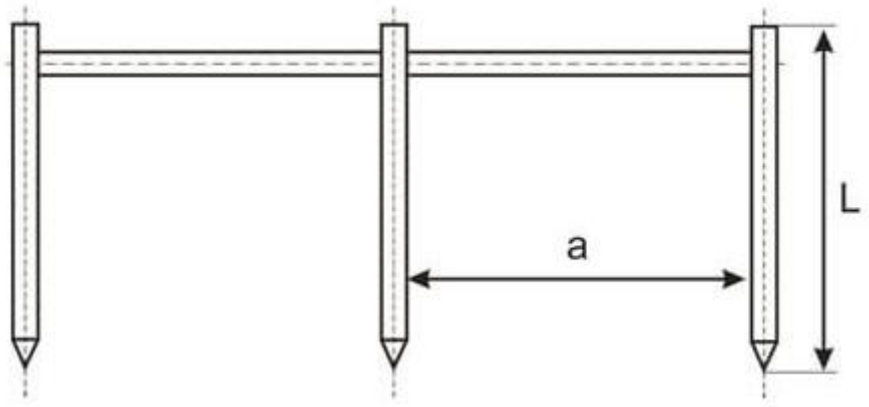

Рисунок 6.6 – Стрижні заземлюючого пристрою

6.3. Розрахунок заземлюючого пристрою

Розрахунок заземлюючого пристрою буде проведено за наступними вхідними даними, які представлено у таблиці 6.2.

Таблиця 6.2 – Вхідні дані для розрахунку заземлюючого пристрою

Позначення	Найменування	Од. вим.	Значення
R	Нормований опір розтікання струму в землю	Ом	4.00
1 □	Питомий опір верхнього слою піску	Ом·м	50
2□	Питомий опір нижнього слою піску	Ом·м	60
d	Діаметр стержня	мм	20.00

Позначення	Найменування	Од. вим.	Значення
L	Довжина вертикального заземлювача	м	3.00
H	Товщина верхнього слою ґрунту	м	1.00
$t_{полоси}$	Глибина закладення горизонтального заземлювача	м	0.50
t	Відстань від поверхні землі до середини заземлювача	м	2.00
1k	Кліматичний коефіцієнт для вертикальних електродів	–	2
2 k	Кліматичний коефіцієнт для горизонтальних електродів	–	6
b	Ширина сталевої полоси	мм	50.00
ã l	Довжина горизонтального заземлювача	м	70.00

Питома розрахунковий коефіцієнт опору двошарового піску визначимо за формулою 6.1:

$$\rho = \frac{(\rho_1 \cdot \rho_2 \cdot L)}{(\rho_1 \cdot (L - H + t_{полоси}) + \rho_2 \cdot (H - t_{полоси}))} \qquad (6.1)$$

$$\rho = \frac{(50 \cdot 60 \cdot 3)}{(50 \cdot (3 - 1 + 0{,}5) + 60 \cdot (1 - 0{,}5))} = 58{,}06 \text{ (Ом·м)}$$

Опір розтікання електрода вертикального положення визначається з використанням формули 6.2:

$$r_{\text{в}} = \frac{0.366 \cdot k_1 \cdot \rho}{L} \cdot \left(lg\left(\frac{2 \cdot L}{0{,}95 \cdot d}\right) + \frac{1}{2} \cdot \lg\left(\frac{4 \cdot t + L}{4 \cdot t - L}\right)\right) \qquad (6.2)$$

$$r_{\text{в}} = \frac{0.366 \cdot 2 \cdot 58{,}06}{3} \cdot \left(lg\left(\frac{2 \cdot 3}{0{,}95 \cdot 20}\right) + \frac{1}{2} \cdot \lg\left(\frac{4 \cdot 2 + 3}{4 \cdot 2 - 3}\right)\right) = 39{,}12 \text{ (Ом)}$$

Загальна кількість заземлювачів вертикального типу, яка потрібна для забезпечення безпеки визначається використовуючи формулу 6.3:

$$n_{\text{їð}} = \frac{r_{\text{â}}}{R_i \cdot \text{ŋ}_{\text{â}}} \qquad (6.3)$$

Де, $\text{ŋ}_{\text{â}}$ – коефіцієнт використання вертикальних заземлювачів (табл.6.3)

Таблиця 6.3 – Параметри вертикальних і горизонтальних заземлювачів

Позначення	Найменування	Од. вим.	Значення
$\text{ŋ}_{\text{â}}$	Коефіцієнт використання вертикальних заземлювачів	-	0,66
$\text{ŋ}_{\text{â}}$	Коефіцієнт використання горизонтальних заземлювачів	-	0,36
h	Відстань між заземлювачами	м	5,83

З цього можна зробити висновок, що відповідно до формули 6.3 було отримано такі розрахунки:

$$n_{\text{їð}} = \frac{39{,}12}{4 \cdot 0{,}66} = 14{,}8 \approx 15 \text{ (шт)}$$

Кількість передбачених вертикальних заземлювачів = 15 шт виходячи з розрахунку.

Наступний розрахунок – опір горизонтального заземлювача , який буде визначено за формулою 6.4:

$$r_{\text{â}} = \frac{0{,}366 \cdot k_2 \cdot \rho}{l_{\text{â}} \cdot \eta_{\text{â}}} \cdot \lg\left(\frac{2l_{\text{â}}^2}{\text{b} \cdot \text{t}_{\text{полоси}}}\right) \qquad (6.4)$$

$$r_{\text{â}} = \frac{0{,}366 \cdot 6 \cdot 58{,}06}{70 \cdot 0{,}66} \cdot \lg\left(\frac{2 \cdot 70^2 \cdot 1000}{50 \cdot 0{,}5}\right) = 15{,}43 \text{ (Ом)}$$

Вертикальних заземлювачів опір визначається за формулою 6.5:

$$R = \frac{R_{\text{í}} \cdot r_{\text{â}}}{r_{\text{â}} - R_{\text{í}}} \qquad (.5)$$

$$R = \frac{4 \cdot 15{,}43}{15{,}43 - 4} = 5{,}39 \text{ (Ом)}$$

Якщо враховувати опір вертикальних заземлювачів повний, тоді уточнена кількість вертикальних заземлювачів з урахуванням сполучної смуги буде визначатися відповідно формулі 6.6:

$$n_{\text{їð}} = \frac{r_{\text{â}}}{R_i \cdot \eta_{\text{â}}} \qquad (6.6)$$

$$n_{\text{їð}} = \frac{39{,}12}{5{,}39 \cdot 0{,}66} = 10{,}99 \approx 11 \text{ (шт)}$$

Приймаються до установки 11 вертикальних заземлювачів, загальна довжина горизонтального заземлювача 70.00 м при середній відстані між вертикальними заземлювачами 5,83 м. Остаточна відстань між вертикальними заземлювачами уздовж сполучної смуги зображується на плані заземлювального пристрою.

Монтажні параметри одиночного заземлювача в двошаровому ґрунті вказані на рисунку 6.7, а конструкція заземлюючого пристрою на рисунку 6.8.

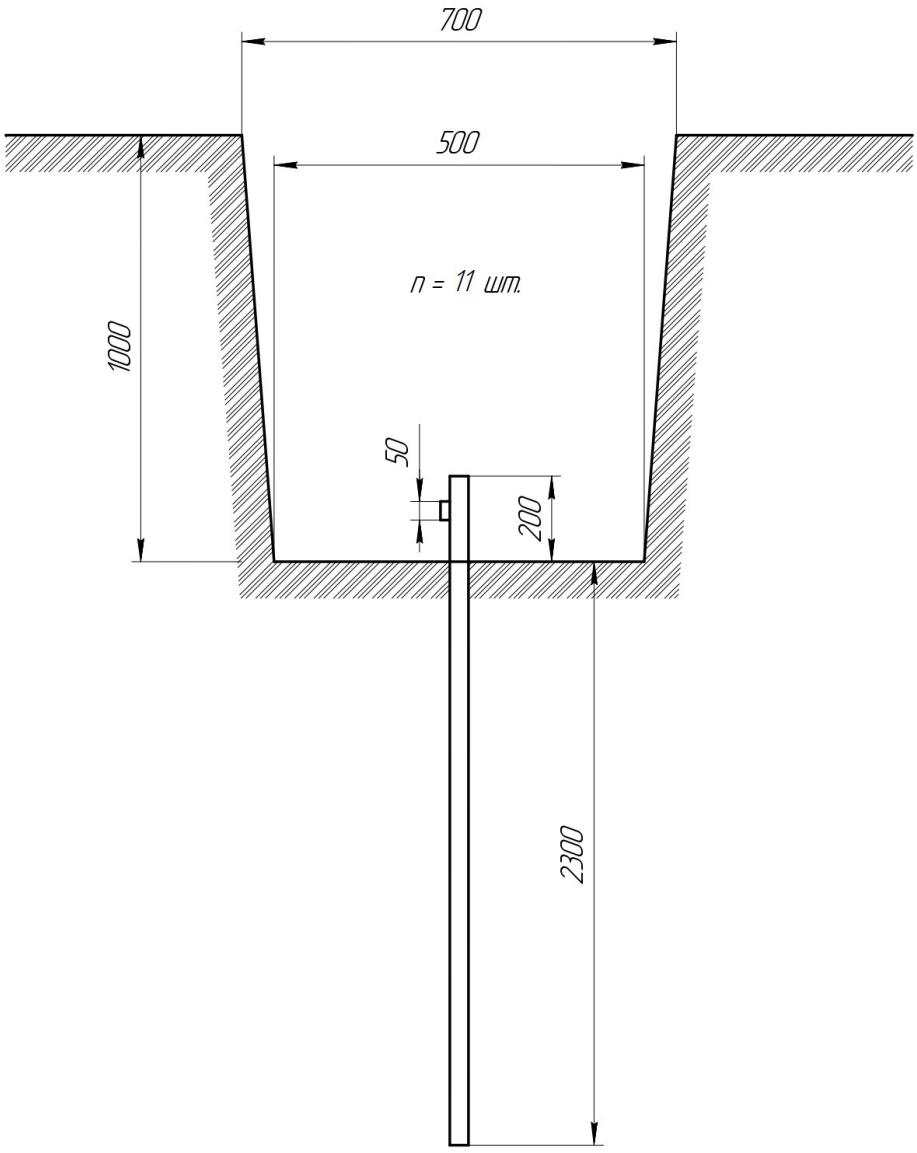

Рисунок 6.7 – Креслення заземлювача відповідно розрахункам

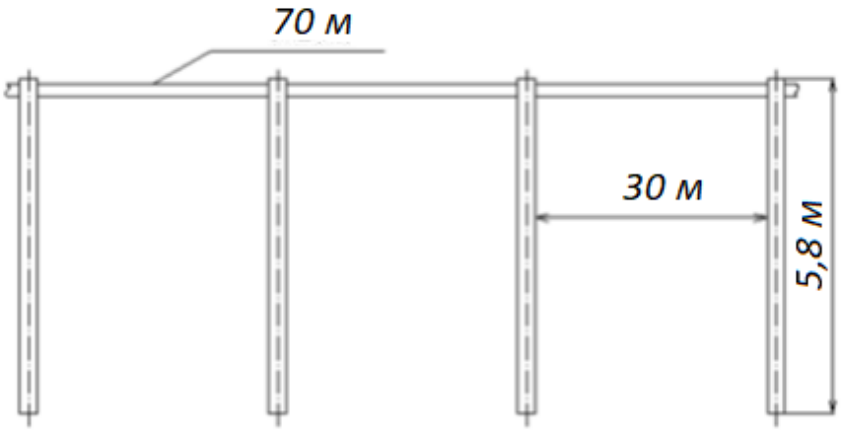

Рисунок 6.8 – Креслення стрижнів заземлювача відповідно розрахункам

Після проведення розрахунків було отримано заземлюючий пристрій, який відповідає вимогам техніки безпеки, електробезпеці та нормам охорони праці в цілому. Для безпечної та коректної роботи з електроустаткування рекомендовано використання даного заземлення.

Також, окрім встановлення заземлення рекомендовано працівникам та всім учасникам процесу дотримуватися правил та інструкцій з охорони праці, ТБ, та особливо електробезпеки, адже за даною специфікою роботи, саме можливе ураження струмом є найбільшою небезпекою при виконанні даних видів робіт. Для збільшення безпечних умов праці з електроустаткуванням рекомендовано використання ЗІЗ та ознайомлення з порядком дій при виникненні аварійної ситуації з ураженням струмом людини та правилами надання першої медичної допомоги постраждалому [56].

ВИСНОВОК

У магістерській кваліфікаційній роботі відповідно до загальної мети і конкретних завдань сформульовані такі висновки:

1. За результатами вивчення теоретичних засад домашньої автоматизації та дослідженню безпеки систем розумного будинку було визначено поняття «розумний будинок», його головні складові – контролери, датчики та/або сенсори актуатори. Що для вмикання, вмикання, вимикання, для зміни параметрів елементів кола і т.п., використовується комутація ланцюга. Головні елементи – блок живлення, перетворювач або трансформатор, регулятор напруги, автоматичний вимикач, реле, тощо. Елементи комутації мають також функцію захисту.

Після проведення дослідження тенденцій впровадження цифрових технологій в житлові приміщення спостерігається наступне: інтерес споживачів до технології smart home постійно зростає, серед всіх факторів економії ресурсів споживачі віддають перевагу найменш енергозатратним системам, вагомими факторами є безпека, стабільність роботи та захист від витоку персональної інформації, споживачів не дуже цікавить облаштування кухні розумними побутовими приладами, вони віддають перевагу розумним вимикачам світла, бойлерам та ін.

Підчас вивчення основних характеристик безпеки систем розумного будинку було визначено поняття «безпека». Головною функцією безпеки є забезпечення протидії негативним по відношенню до даної складної системи зовнішніх факторів і внутрішніх чинників. До них можна віднести: фізичну доступність системи, загрози доступу, загрози інфобезпеки, доступність мережевих систем, тощо.

Говорячи про безпеку, просто не можливо уникнути її протилежної сторони, а саме – кіберзлочинності. Вина за кіберзлочинність, а саме за поширення конфіденційної інформації володарів систем розумного будинку лежить на компанії, яка несе відповідну відповідальність. В законодавстві

України є питання стосовно кіберзлочинності, які регулюються нормами, проте, користувачам рекомендовано використання методів для зменшення загроз безпеки систем розумного будинку.

2. Не існує систем, які були би ідеально захищені, і системи розумного будинку не виключення. Завдяки вразливостям можна навмисно, або навіть не навмисно, порушити цілісність, або викликати неправильну роботу системи. Вразливість може виникати в результаті помилок допущених при програмуванні системи, певних недоліків при проектуванні системи, також, це можуть бути ненадійні паролі, або шкідливі віруси та програми, які навмисно було вироблено для нанесення шкоди системам, тощо. Найбільшою загрозою для систем розумного будинку є саме загрози доступу. Несанкціонований доступ до системного контролеру, робить всю систему вразливою, та значно спрощує для шахраїв усі можливості для отримання інформації або нанесення шкоди. Існує багато причин отримання доступу до систем розумного будинку, але нажаль, інколи саме користувачі систем через незнання або, через нерозуміння важливості безпеки, стають причинами «відкритого» доступу до систем розумного будинку. Проте, завдяки вияву так званих «слабких місць» та взагалі дослідженню безпеки систем розумного будинку, ймовірність передбачення та застереження користувачів від шахрайських дій з кожним роком лише зростає.

3. Запропоновано методи для самостійного безкоштовного запобігання загрозам систем розумного будинку, методи для запобігання загрозам систем розумного будинку з точки зору інженера електронника : використання менеджерів паролів для забезпечення більшої надійності систем розумного будинку криптографічне шифрування для забезпечення більшої надійності систем розумного будинку, забезпечення механізму аутентифікації користувача.

4. Запропоновано методи для самостійного, безкоштовного запобігання загрозам систем розумного будинку та професійні інженерні рішення задля забезпечення безпеки систем розумного будинку. Виявлено

критерії вибору параметрів безпеки систем розумного будинку, запропоновано математично-психологічний метод підбору найоптимальнішого варіанту системи розумного будинку відповідно до пріоритетності критеріїв та особистої експертної оцінки – MAI. Відповідно до експертної думки ОРВ та визначеної пріоритетності критеріїв вибору систем розумного будинку методом MAI було визначено найбільш безпечну систему розумного будинку – провідна система РБ.

5. Було проведено економічне дослідження, після якого можна зробити висновок, що забезпечення безпеки систем розумного будинку підвищує вартість системи, але не значно. Тому, застосування та покращення безпеки систем розумного будинку є раціональним та рекомендованим користувачам систем.

6. Розглянуто охорону праці та здійснено розрахунок пристрою заземлення. Після проведення розрахунків було отримано заземлюючий пристрій, який відповідає вимогам техніки безпеки, електробезпеці та нормам охорони праці в цілому. Для безпечної та коректної роботи з електроустаткування рекомендовано використання даного заземлення. Також, окрім встановлення заземлення рекомендовано працівникам та всім учасникам процесу дотримуватися правил та інструкцій з охорони праці, ТБ, та особливо електробезпеки, адже за даною специфікою роботи, саме можливе ураження струмом є найбільшою небезпекою при виконанні даних видів робіт. Для збільшення безпечних умов праці з електроустаткуванням рекомендовано використання ЗІЗ та ознайомлення з порядком дій при виникненні аварійної ситуації з ураженням струмом людини та правилами надання першої медичної допомоги постраждалому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Дуднік А.С. Застосування датчиків вимірювання механічних величин в комп'ютерній мережі «Розумний дім» Метрологія та прилади. 2017. Вип. № 5. С.106 -110. [Електронний ресурс] — Режим доступу: https://ela.kpi.ua/bitstream/123456789/27396/1/Dudnik_aref.pdf

2. Дужак І.О. Розумний будинок // Автоматизація технол. І бізнес-процесів. – 2013. – № 13-14. – С. 31-33. – [Електронний ресурс] — Режим доступу: http://journals.uran.ua/atbp/article/download/32920/29533

3. Michael S., Ulf L., 7 Smart-Home-Starter-Kits imSicherheits-Test // AV-TESTStudie. 2014. pp. 16-41.

4. Пантелеев М.Ю. Открытая архитектура «Умный дом» [Електронний ресурс] — Режим доступу: https://articlekz.com/article/13576

5. Полякова О. В. Класифікація функціональних складових елементів системи інтелектуального керування середовищем при проектуванні житла // Вісн. Київ. нац. ун-ту технологій та дизайну. Техн. науки. – 2016. – № 4 (100). – С. 133-140.

6. М.Э. Сопер. Практические советы и решения по созданию «Умного дома», Сопер М. Э. - М.: НТ Пресс, 2007. - 432 с.

7. В.Н. Харке «Умный дом. Объединение в сеть бытовой техники и систем коммуникаций в жилищном строительстве» / Харке В.Н. - М.: Техносфера, 2006. - 292с.

8. Федоров Д. Збільшення комфорту життя за допомогою інтелектуальних машин «Безпечний будинок» // Наук. зап. Малої акад. наук України. Серія: Пед. науки. – 2018. – Вип. 12. – С. 179-185. – [Електронний ресурс] — Режим доступу: https://u.to/CPZGGw

9. Фурман І. О. Огляд можливостей «розумного будинку» для покращання побутових умов та зменшення витрат на утримання омогосподарств / І. О. Фурман, Р. М. Старовєров, Д. О. Мельський // Вісн. Харк. нац. техн. ун-ту сіл. госп-ва ім. Петра Василенка. – 2014. – Вип. 154. –

С. 75-76. – URL: https://u.to/tfBLGw ; Енергетика та комп’ют.-інтегр. технології в АПК. – 2014. – № 2. – С. 79-80. – [Електронний ресурс] — Режим доступу: https://u.to/vvBLGw

10. Т. Р. Элсенпитер, Дж. Велт. «Умный Дом строим сами» / Т. Р. Элсенпитер, Дж Велт/ КУДИЦ–ОБРАЗ. 2005. – 384 с.

11. Wiki ТНТУ «Розумний дім» [Електронний ресурс] — Режим доступу: https://wiki.tntu.edu.ua/Розумний_дім

12. Золенко М. Що таке розумний будинок: функції, види, складові та екосистеми [Електронний ресурс] — Режим доступу: https://ek.ua/ua/post/1990/618-chto-takoe-umnyy-dom-funkcii-vidy-sostavlyayuschie-i-ekosistemy/

13. New smurt home «7 основных датчиков для умного дома и их функции» [Електронний ресурс] — Режим доступу: https://newsmarthome.ru/smart-home/datchiki-dlya-umnogo-doma

14. Mastery of building «Елементи системи розумний будинок, їх призначення та принцип роботи» [Електронний ресурс] — Режим доступу: https://mastery-of-building.org/uk/sostavlyayushhie-elementy-sistemy-umnyj-dom-ix-naznachenie-i-princip-raboty/

15. Княгинин В. Н. «Розумні» середовища, «розумні» системи, «розумні» виробництва: Промисловий і технологічний Форсайт РосійськоїФедерації на довгострокову перспективу. - CSR North-West, 2013.

16. Smirnov A. et al. Context-based access control model for smart space// Cyber Conflict (CyCon), 2013 5th International Conference on. - IEEE, 2013. -С. 1-15.

17. Заплатинський В. М. Логіко-детермінантні підходи до розуміння поняття «Безпека». Вісник Кам'янець-Подільського національного університету імені Івана Огієнка. Фізичне виховання, спорт і здоров'я людини. / [редкол.: П. С. Атаманчук (відп. Ред..) та ін.]. — Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2012. — Випуск 5. (−336 с.) С. 90-98.

18. С. О. Гудзинський, В. П. Попович, О. П. Петриченко Висновок до проекту Закону України від 18.02.2019 № 9340 [Електронний ресурс] — Режим доступу: https://ips.ligazakon.net/document/XH77G00A

19. Коваленко, Ю. О. (2010). Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості (3). с. 123–129. Процитовано 2019-11-16.

20. StudFiles «Загрози конфіденційної інформації» [Електронний ресурс] — Режим доступу: https://studfile.net/preview/5178442/page:3/

21. Донченко А.Г. Загрози і вразливості безпеки розумного будинку [Електронний ресурс] — Режим доступу: https://naukam.triada.in.ua/index.php/konferentsiji/70-tridtsyat-dev-yata-vseukrajinska-praktichno-piznavalna-internet-konferentsiya/933-zagrozi-i-vrazlivosti-bezpeki-rozumnogo-budinku

22. Економічна правда «За п'ять років кіберзлочинність в Україні виросла вдвічі» [Електронний ресурс] — Режим доступу: https://www.epravda.com.ua/news/2019/10/21/652782/

23. Харитоненко І. О. Кіберзлочинність: поняття та ознаки [Електронний ресурс] — Режим доступу: http://aphd.ua/publication-781/

24. Про ратифікацію Конвенції про кіберзлочинність Закон №2824-IV от 07.09.2005 [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/2824-15#Text

25. Про внесення змін до Закону України "Про захист інформації в автоматизованих системах". Закон від 31.05.2005 № 2594-IV [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/2594-15#Text

26. Кримінальний кодекс України від 05.04.2001 № 2341-III (Редакція станом на 25.11.2021) [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14

27. Мего-Інфо-Юридичний портал №1 «Злочини у сфері використання електронно-обчислювальних машин комп’ютерів систем» [Електронний ресурс] — Режим доступу: http://mego.info/ матеріал/ розділ-xvi-

злочини-у-сфері-використання-електронно-обчислювальних-машин-компютерів-систем/

28. Мего-Інфо-Юридичний портал №1 «Несанкціонований збут або розповсюдження інформації з обмеженим доступом» [Електронний ресурс] — Режим доступу: http://mego.info/стаття-361-2/ несанкціонований-збут-або-розповсюдження-інформації-з-обмеженим-доступом

29. Хабр «Страхи и проблемы будущего умных домов» [Електронний ресурс] — Режим доступу: https://habr.com/ru/company/iridiummobile/blog/385311/

30. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 1999.

31. StudFiles «Угрозы конфиденциальной информации» [Електронний ресурс] — Режим доступу: https://studfile.net/preview/5178442/page:3/

32. ВікіпедіЯ «Мережева операційна система» [Електронний ресурс] — Режим доступу: https://uk.wikipedia.org/wiki/ Мережева_операційна_система

33. ВікіпедіЯ «Комп'ютерний вірус» [Електронний ресурс] — Режим доступу: https://uk.wikipedia.org/wiki Комп%27ютерний_вірус

34. Broadcom «Laurence. Viruses that can cost you» [Електронний ресурс] — Режим доступу: www.symantec.com

35. Collotta M., Pau G. A Solution Based on Bluetooth Low Energy for Smart Home Energy Management // Energies. - 2015. - Т. 8. - №. 10. - С. 11916-11938.

36. Cheng J., Kunz T. A survey on smart home networking // Carleton University, Systems and Computer Engineering, Technical Report, SCE-09-10. - 2009.

37. Fouladi B., Ghanoun S. Security Evaluation of the Z-Wave Wireless Protocol // Black hat USA. - 2013. - Т. 24

38. RTLS «Мережева інфраструктура системи РТЛС» [Електронний ресурс] — Режим доступу: http://www.rtlsnet.ru/technology/view/3

39. Снегуров А. В., Ткаченко Є. А., Кравченко А. Д. Ризики інформаційної безпеки систем, побудованих за технологією "Розумний будинок" // Східно-Європейський журнал передових технологій. - 2011. - Т. 4. -№. 3 (52).

40. Донченко Андрій «Система моніторингу та оцінки загроз інформаційній безпеці розумного будинку [Електронний ресурс] — Режим доступу: https://ela.kpi.ua/bitstream/123456789/38429/1/Donchenko_magistr.pdf

41. Lib MDPU «Класифікація програмного забезпечення» [Електронний ресурс] — Режим доступу: http://lib.mdpu.org.ua/e-book/vstup/L2.htm

42. Eset «Використання менеджера паролів: навіщо потрібен та як правильно обрати» [Електронний ресурс] — Режим доступу: https://eset.ua/ua/blog/view/79/ispolzovaniye-menedzhera-paroley-zachem-nuzhen-i-kak-pravilno-vybrat

43. ВікіпедіЯ «Прикладний програмний інтерфейс» [Електронний ресурс] — Режим доступу: https://uk.wikipedia.org/wiki/Прикладний_програмний_інтерфейс

44. Webznam «Поисковые системы интернета вещей – чем пугают Shodan и Censys» [Електронний ресурс] — Режим доступу: https://webznam.ru/blog/poiskovye_sistemy_interneta_veshhej/2018-09-19-684

45. ВікіпедіЯ «Выбор» [Електронний ресурс] — Режим доступу: https://ru.wikipedia.org/wiki/Выбор

46. ВікіпедіЯ «Метод аналізу ієрархій» [Електронний ресурс] — Режим доступу: https://uk.wikipedia.org/wiki/Метод_аналізу_ієрархій

47. Smurthome «Розумний дім» [Електронний ресурс] — Режим доступу: http://zenchom.com/smarthome

48. Попова В.Д. Методичні вказівки до виконання економічної й організаційної частини дипломної роботи – Запоріжжя, 2005,-36с.

49. Sendpulse «Что такое послепродажное обслуживание: выясняем» [Електронний ресурс] — Режим доступу: https://sendpulse.ua/ru/support/glossary/after-sales-service

50. Edison «Цикл разработки и его этапы» [Електронний ресурс] — Режим доступу: https://www.edsd.ru/ru/princypy/cikl_razrabotki_po

51. Про охорону праці Закону України від 14.10.1992 № 2694-XII (Редакція станом на 14.08.2021) [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/2694-12#Text

52. Protrud «Охрана труда» [Електронний ресурс] — Режим доступу: https://www.protrud.com/ инструктажи-по-охране-труда/

53. Protrud «Классификация средств индивидуальной защиты» [Електронний ресурс] — Режим доступу: https://www.protrud.com/обучение/учебный-курс/классификация-средств-индивидуальной-защиты/

54. Uteka «Охрана труда на предприятии: что нужно знать?» [Електронний ресурс] — Режим доступу: https://uteka.ua/publication/news-14-ezhednevnyj-buxgalterskij-obzor-39-oxrana-truda-na-predpriyatii-chto-nuzhno-znat

55. Ot.kiev «Служба охраны труда» [Електронний ресурс] — Режим доступу: https://www.ot.kiev.ua/new_page_301.htm

56. Электрик в доме «Расчет защитного заземления» [Електронний ресурс] — Режим доступу: https://electricvdome.ru/zazemlenie/raschet-zazemlenia.html

Формат	Зона	Поз.	Позначення	Найменування	Кіл.	Примітка
				Документація		
А1			ЕС М.403 20.00.00.00.00.Д1	Дослідження безпеки систем розумного будинку. Схематичне зображення системи розумного будинку		
А1			ЕС М.403-20.00.00.00.00.Д2	Дослідження безпеки систем розумного будинку. Перелік загроз, вразливостей та можливих наслідків в системах розумного будинку		
А1			ЕС М.403-20.00.00.00.00.Д3	Дослідження безпеки систем розумного будинку. Схема передачі даних в системах розумного будинку		
А1			ЕС М.403-20.00.00.00.00.Д4	Дослідження безпеки систем розумного будинку. Схема ієрархії безпеки в системах розумного будинку		
А1			ЕС М.403-20.00.00.00.00.Д5	Дослідження безпеки систем розумного будинку. Розрахунок найбезпечнішої системи розумного будинку		

Зм.	Арк.	№ докум.	Підп.	Дата	ЕС М.403-20.00.00.00.00		
Розроб.		Панченко		10.12.21	Дослідження безпеки систем розумного будинку	Літ.	Арк. 1 / Аркушів 2
Перевір.		Шмалій		10.12.21			
Н.контр.		Туришев		10.12.21		ІННІ ім Ю.М. Потебні ЗНУ 8.1710	
Затверд.		Критська		10.12.21			

Перед застосув.

Довід. №

Інв. № дубл.

Взам. інв. №

Інв. № подл.

Формат	Зона	Поз	Позначення	Найменування	Кіл.	Примітка
А1			ЕС М.403-20.00.00.00.00.Д6	Дослідження безпеки систем		
				розумного будинку		
				Розрахунок економічних показників		
А1			ЕС М.403-20.00.00.00.00.Д7	Дослідження безпеки систем		
				розумного будинку		
				Заземлювальний пристрій		
А1			ЕС М.403-20.00.00.00.00.Е1	Дослідження безпеки систем		
				розумного будинку		
				Схема електрична структурна		

Інв. № подл. | Підп. і дата | Взам. інв. № | Інв. № дубл. | Підп. і дата

Зм.	Арк.	№ докум.	Підп.	Дата	ЕС М.403-20.00.00.00.00	Арк. 2

Копіював Формат А4