Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем та програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Безпека системи «Розумний дім»*

Виконав(ла): студент(ка) IV курсу, групи СБс-41
спеціальності *125 «Кібербезпека»*
(шифр і назва спеціальності)

	(підпис)	Сидорчук А.М. (прізвище та ініціали)
Керівник	(підпис)	Александер М.Б. (прізвище та ініціали)
Нормоконтроль	(підпис)	Лобур Т.Б. (прізвище та ініціали)
Завідувач кафедри	(підпис)	Загородна Н.В. (прізвище та ініціали)
Рецензент	(підпис)	(прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно- інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
« » 20___ р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня **бакалавр**
(назва освітнього ступеня)

за спеціальністю 125 «Кібербезпека»
(шифр і назва спеціальності)

студенту Сидорчук Анастасії Миколаївній
(прізвище, ім'я, по батькові)

1. Тема роботи **Безпека системи «Розумний дім»**

Керівник роботи Александер Марек Богуслав, д.т.н., професор
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*03*» *04* 20*23* року № *4/7-349*

2. Термін подання студентом завершеної роботи 17.06.2023

3. Вихідні дані до роботи Вимоги програмного забезпечення системи безпеки

4. Зміст роботи (перелік питань, які потрібно розробити)
Розділ 1 Система «Розумний дім». Основні поняття та функції. 1.1 Концепція «Розумного дому». 1.2Аналіз технологій обміну даними між розумними модулями. 1.3Постановка задачі. Розділ 2 Аналіз вразливостей та механізмів безпеки розумних будинків.2.1 Вразливість розумних будинків та поширені атаки на розумні домашні пристрої. 2.2Механізми захисту пристроїв розумного дому. 2.3 аналіз існуючої підтримки безпеки в протоколах IoT. Розділ 3 забезпечення захисту в системі «розумний дім» . 3.1 Система безпеки. 3.1.1 Мікроконтролерні платформи для системи безпеки. 3.1.2 Вибір мікроконтролера для проекту. 3.1.3Опис системи безпеки «Розумного дому». 3.3 реалізація пристрою. 3.4 Дослідження продуктивності системи. Розділ 4. Безпека життєдіяльності та охорона праці. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Актуальність. Постановка задачі. Розроблені наступні задачі. Загальні методи атаки включають. Основні засоби захисту. Основні компоненти розробки. Схема безпеки «Розумний дім». Встановлення значення та кількість клавіш мембранної клавіатури. Налаштування входу. Налаштування параметрів екрана та аналогових входів.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, охорона праці	Гурик О. Я., к.т.н., доцент кафедри МТ		

7. Дата видачі завдання 16.01.2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення із завданням до кваліфікаційної роботи	16.01-19.01	*Виконано*
2.	Підбір джерел про принципи побудови та методи забезпечення безпеки в децентралізованих системах	20.01-05.02	*Виконано*
3.	Опрацювання джерел в галузі дослідження	06.02-22.02	*Виконано*
4.	Розроблення програмного коду	23.02-20.03	*Виконано*
5.	Тестування роботи програми та верифікація результатів	21.03-05.04	*Виконано*
6.	Оформлення розділу « Система «Розумний дім». Основні поняття та функції»	06.04-17.04	*Виконано*
7.	Оформлення розділу «Аналіз вразливостей та механізмів безпеки»	18.04-29.04	*Виконано*
8.	Оформлення розділу «Забезпечення захисту в системі «Розумний Дім»»	30.04-13.05	*Виконано*
9.	Оформлення підрозділу «Безпека життєдіяльності, охорона праці»	14.05-21.05	*Виокнано*
10.	Оформлення кваліфікаційної роботи	22.05-05.06	*Виконано*
11.	Нормоконтроль	06.06-11.06	*Виконано*
12.	Перевірка на плагіат	12.06-15.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.06-19.06	*Виконано*
14.	Захист кваліфікаційної роботи	23.06.2023	

Студент _____ Сидорчук А.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Александер М.Б.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Безпека системи «Розумний дім» // Кваліфікаційна робота ОР «Бакалавр» // Сидорчук Анастасія Миколаївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. 64, рис. – 20 , табл. – 3, дод. - 1.

Ключові слова: РОЗУМНИЙ ДІМ, СИСТЕМА БЕЗПЕКИ, МІКРОКОНТРОЛЕРНА СИСТЕМА, ARDUINO UNO, МОДЕЛЮВАННЯ, TINKERCAD.

Кваліфікаційна робота присвячена розробці системи безпеки для розумної домівки на основі мікроконтролера Arduino Uno, магнітно-контактному датчику та датчику руху з відповідним функціоналом для керування системою.

В результаті представлено детальний розгляд атак, уразливостей та існуючих систем безпеки «Розумного дому».

На основі мікроконтролера Arduino розроблено та запрограмовано систему безпеки «Розумного дому», для цього розроблено структуру системи безпеки, підібрані компоненти із відповідними технічними характеристиками, проведене моделювання системи за допомогою онлайн – сервісу Tinkercad.

ANNOTATION

Security of the «Smart Home» system // Qualification work of the OR «Bachelor» // Sydorchuk Anastasija Mykolaivna // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and software engineering, Department of Cybersecurity, СБс-41 group // Ternopil , 2023 // P. 64, figures - 20, tables - 3 , appendices - 1.

Keywords: SMART HOME, SECURITY SYSTEM, MICROCONTROLLER SYSTEM, ARDUINO UNO, MODELING, TINKERCAD.

The qualification work is devoted to the development of a security system for a smart home based on an Arduino Uno microcontroller, a magnetic contact sensor and a motion sensor with the appropriate functionality for controlling the system.

As a result, a detailed review of attacks, vulnerabilities and existing security systems of the "Smart Home" is presented.

Based on the Arduino microcontroller, the Smart Home security system was developed and programmed, for this purpose the structure of the security system was developed, components with appropriate technical characteristics were selected, and the system was modeled using the Tinkercad online service.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

GND – точка нульового потенціалу мікросхеми;

Sketch – програма-прошивка мікроконтролера;

URL (Uniform Resource Locator) – схема створення унікальних адрес електронних ресурсів;

SPI (Serial Peripheral Interface) – послідовний синхронний повнодуплексний стандарт передачі даних;

ВС – вбудована система;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

MST (Micro System Technology) – мікросистемні технології;

SoC (System-on-a-Chip) – система на кристалі;

ЗМІСТ

ВСТУП

Традиційно будинки, квартири, комерційні будівлі та споруди різного призначення складаються з електричного обладнання та систем, кожна з яких потребує індивідуального обслуговування та працює незалежно одна від одної.

Зазвичай у нашому домі ми не можемо використовувати пульт від телевізора, щоб відкрити двері, або використовувати настінний вимикач, щоб змінити станцію. Це пояснюється тим, що кожна система працює незалежно і може взагалі не накладатися на інші системи.

«Розумний дім» – це фактично житло, в якому організована система домашньої автоматизації, яка поєднує в собі управління освітленням, опаленням, кондиціонуванням повітря, вентиляцією, охоронною сигналізацією, аудіо- та відеосистемами, пристроями виклику, пристроями контролю енергії, автоматичними системами (дверями). , вікна, віконниці, ворота), технічна сигналізація (наприклад, у разі випадкового витоку води).

Сьогодні більшість виробників систем розумного дому пропонують можливість дистанційного керування інтерфейсом, який зазвичай складається з веб-сторінки, на якій можна увійти (за допомогою свого імені користувача та пароля) і переглянути стан кожного пристрою та кожної підсистеми.

Тому розумний дім створюється шляхом з’єднання різних частин побутової техніки в одну загальну систему. Ця форма автоматизації зменшує потребу у взаємодії з людьми, підвищує комфорт і забезпечує додаткові переваги та покращену енергоефективність.

Однак ми повинні знати, що ні електричні системи, ні самі будинки не є розумними, оскільки вони не програмуються самі по собі, не вчаться на своїх помилках і не виправляють їх (якщо тільки вони не оснащені штучним інтелектом - Розумна «система»).

Тому безпеці в «системах розумного дому» слід приділяти особливу увагу, оскільки втручання в звичайні системи автоматизації може призвести до небезпечних наслідків несанкціонованих дій зловмисників.

Немає сумніву, що безпека близьких для кожного важливіша за гроші та матеріальні речі. Сьогодні захист сім'ї є абсолютною необхідністю. Однак потрібно зробити все можливе, щоб нещасних випадків не сталося. У режимі реального часу обробляються різноманітні події, що фіксуються датчиками розумного будинку, а також дані про опалення, температуру в приміщенні, освітлення, вентиляцію тощо.

Це означає, що система повідомить користувача, щойно відбудеться подія, а не пізніше. У той же час усі ці події можуть автоматично зберігатися в базі даних подій для можливих потреб аналізу. Повернувшись додому, ви можете дивитися ці події чи ні, і ви можете отримати найважливіший вміст на свій смартфон, навіть коли нікого немає вдома.

РОЗДІЛ 1 . СИСТЕМА “РОЗУМНИЙ ДІМ”. ОСНОВНІ ПОНЯТТЯ ТА ФУНКЦІЇ

1.1 Концепція «Розумного дому»

«Розумний дім» — це інтелектуальна система, яка об’єднує електроприлади з лініями керування. Це дає можливість керувати декількома пристроями одночасно, використовуючи лише один елемент управління (дисплей). Складний датчик постійно контролює роботу всього обладнання і завдяки взаємодії всіх систем знижує витрати на технічне обслуговування та підвищує безпеку, надійність і комфорт [2].

Поняття «розумний будинок» означає, що будівлі повинні бути спроектовані щоб усі служби могли інтегруватися один з одним мінімальною вартістю (з точки зору фінансів, часу та сил), а їхні послуги організовані оптимально.

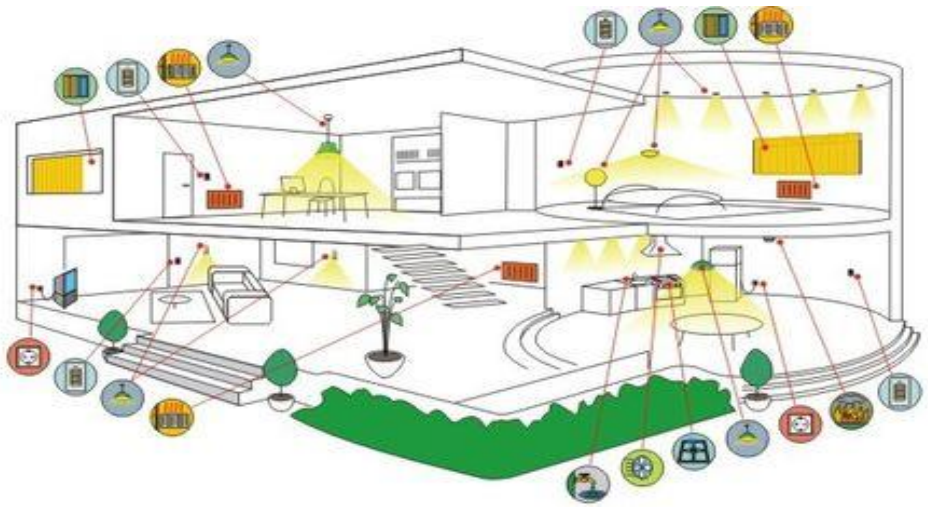

Рисунок 1.1 - Приклад розумного дому [1]

Тим не менш, коли йдеться про домашню автоматизацію або системи розумного дому, ми розуміємо, що мова йде про використання набору пристроїв, які дозволяють вам автоматично (і іноді дистанційно) керувати основними функціями вашого будинку. Людина більшу частину часу

проводить у приміщенні будівлі, де використовує обладнання, яке потребує контролю, особливо протягом дня, десятки, сотні чи навіть тисячі разів, тому особливу увагу слід приділяти контролю доступу, енергозбереженню, і безпеці.

Табл. 1.1 - Основні положення концепції розумних будівель

Послідовність основних положень	**Опис системи**
Створення інтегрованої системи управління будівлею	Системи, яка забезпечує комплексну роботу всіх інженерних систем будівлі: контролю доступу, кондиціонування, водопостачання, вентиляції освітлення, опалення тощо.
Обслуговуючий персонал	Саме в цих підсистемах вбудований «інтелект» будівлі – це алгоритм дій у відповідь на зміну параметрів датчиків системи та інші події, наприклад, надзвичайні події.
Механізм миттєвого впровадження	Впровадити механізми миттєвого відключення та передачі, за необхідності, одна людина, яка керує будь – якою підсистемою розумної будівлі. При цьому всіма підсистемами та частинами «розумного дому» необхідно зручно та однаково керувати і відображати.
Вихід з ладу загальної системи	При виході з ладу загальної системи управління або інших частин системи слід переконатись в належній роботі кожної підсистеми.
Технічне обслуговування та модернізація	Витрати на технічне обладнання та модернізацію системи побудови зведені до мінімуму, що має бути забезпечено шляхом застосування єдиних стандартів у створенні підсистеми, автоматично налаштувати та виявити, коли додаються нові пристрої та модулі до системи.
Підключення обладнання та модулів системи	Потрібно побудувати наявність прокладених засобів зв'язку для підключення обладнання та модулів системи. При цьому як засоби зв'язку в системах управління можуть використовуватися також різні види фізичних каналів: слабкострумові лінії, лінії електропередач, радіоканали.

Розглянемо систему автоматичного управління докладніше:

1. Освітлення є найважливішим і найчастіше використовуваним електричним елементом в будинку. У деяких кімнатах будинку доцільно використовувати освітлення, яке можна приглушувати або рівномірно змінювати температуру світла, змінюючи колір світла.

Розумні будинки також часто мають зовнішнє освітлення. За допомогою різних ламп можна створити різні сцени та атмосферу перед будинком. За допомогою системи розумного дому ви можете керувати різними лампами в режимі ввімкнення/вимкнення або затемнення, вибираючи найкращий інтерфейс (проста кнопка або віддалений інтерфейс, наприклад, за допомогою смартфона або пульта дистанційного керування).

2. Опалення – одна з завжди присутніх підсистем в оселі. Деякі користувачі можуть проживати в будинках з центральним опаленням за допомогою радіаторів. У цьому випадку ви можете встановити термостатичні вентилі, підключені до вашої системи розумного дому, і контролювати їх по кімнатах, встановлюючи різні температури. Інші можуть жити в приватному будинку, і в цьому випадку у вас можуть бути теплі підлоги з гідравлічними колекторами та більше зонних клапанів з приводами, підключеними до вашої системи розумного будинку.

За допомогою цих пристроїв ви навіть можете контролювати опалення у своєму домі за допомогою смартфона. Додана цінність полягає в тому, що він навіть може заощадити рахунки за опалення, нагріваючи виключно лише тоді і там, де потрібно.

3. Протиугінна система. Більшість виробників систем розумного дому продають пристрої, які забезпечують функціональність проти крадіжок, від найнижчого рівня (датчики присутності та сирени) до найвищого рівня (зв’язок із поліцією чи службами безпеки у випадку протиугінних систем). Якщо грабіжник проникає, система «розумний дім» також може змусити всі ліхтарі в квартирі швидко блимати, щоб якомога більше заплутати грабіжника.

4. *Симуляція існування*. Навіть найкраща у світі протиугінна система не зупинить рішучого грабіжника. Але системи «розумного будинку» пропонують екзистенціальне моделювання: ви можете записати те, що сталося за день, тиждень або навіть місяць, просто щоб відтворення запису виглядало якомога реалістичніше.

Описана операція є великою перевагою з точки зору безпеки порівняно з часом простою. Таймер для вмикання та вимикання світла щодня в один і той же час. Потенційний грабіжник може оглянути будинок перед пограбуванням і побачити віконниці, що відкриваються та закриваються, а світло вмикається та вимикається в абсолютно різний час дня чи тижня.

5. Будильник і кімнатний контроль. Система «розумний дім» може не тільки встановити більше будильників, але й підключитися до дитячої кімнати (наприклад, за допомогою планшета або смартфона) і миттєво включити світло в кімнаті на максимум і підняти жалюзі. Звичайно, підлітки можуть встати, вимкнути світло та опустити жалюзі. Запобігайте цьому, вимкнувши вимикачі, які керують світлом і жалюзі в дитячій кімнаті, одним натисканням кнопки.

6. Контроль погоди. Системи розумного будинку можуть бути оснащені погодними модулями, які можуть вимірювати такі дані, як інтенсивність опадів, вологість і швидкість вітру. Якщо вдома нікого немає і раптом почнеться дощ, система може закрити вікна, або при сильному вітрі може підняти тент, щоб не пошкодити його.

Розглянемо переваги розумного будинку:

1. Автоматизація. Повернувшись додому, ви можете за допомогою пульта дистанційного керування або смартфона активувати функцію відкривання дверей, перш ніж увійти в будинок і відкрити двері гаража. Використовуючи електродвигуни, керовані смарт-приводами, підключеними до систем розумного будинку, можна автоматизувати майже все: двері, вікна, жалюзі, ворота, ширми, навіть стільці та дивани. Так само ви можете керувати сторонніми пристроями, які можна інтегрувати в інтелектуальні

засоби керування вашою домашньою системою, такими як сходові підйомники, пристрої для людей з обмеженими можливостями тощо.

2. Енергоефективність. Будинки використовують енергію для різних цілей: опалення приміщень і води, охолодження приміщень, приготування їжі, освітлення, побутова техніка та інші кінцеві потреби. У більшості випадків користувач не знає, скільки енергії споживається, і в цьому випадку його можна контролювати, щоб зменшити споживання енергії.

Система розумного дому може вимірювати та відображати енергоспоживання всіх пристроїв підключений до електричної системи, можна встановити поріг потужності, який не можна перевищувати щоб запобігти спрацюванню загального вимикача, можна активувати прилад, коли тариф на енергію є зручнішим, можна вимкнути світло і опалення, коли в кімнаті нікого немає.

Окрім цього, це може бути інтерфейс з усіма видами систем виробництва відновлюваної енергії. Системи розумного дому з розумними термостатами, датчиками присутності та моніторингом енергії, пристрої прокладають шлях до яскравішого, екологічного майбутнього – і заощаджують кошти.

3. Домашній пульт використовується для керування всіма доступними пристроями та функціями в домі (перемикачі, кнопки, сенсорні екрани та навіть інтерфейси голосового керування). Однак, якщо ви поспішаєте вийти з дому, щоб пізніше в дорозі чи на роботі згадати, що ви не натиснули кнопку «Вимкнути все світло», ви можете просто увійти в систему розумного дому за допомогою виконувати команди на смартфоні, планшеті чи комп’ютері.

4. Безпека. Немає сумніву, що безпека близьких для кожного важливіша за гроші та матеріальні речі. Сьогодні захист сім'ї є абсолютною необхідністю. Проте потрібно зробити все можливе, щоб таких аварій не траплялося.

У режимі реального часу обробляються різноманітні події, що фіксуються датчиками розумного будинку, а також дані про опалення,

температуру в приміщенні, освітлення, вентиляцію тощо. Це означає, що система повідомить користувача, щойно відбудеться подія, а не пізніше. У той же час усі ці події можуть автоматично зберігатися в базі даних подій для можливих потреб аналізу. Повернувшись додому, ви можете переглядати збережені дані та записувати всі події на свій смартфон, навіть якщо вдома нікого немає.

Системи розумного будинку забезпечують зв'язок між різними важливими функціями безпеки. До електроустановок можна підключити сигналізацію, а також датчики руху, диму, переливу води, відкривання дверей та вікон та споживання енергії. З їх допомогою можна захистити свій будинок від пошкоджень. Розумний будинок може забезпечити додатковий комфорт і безпеку, а також покращити екологічність. Наприклад, розумна система кондиціонування повітря може використовувати різноманітні домашні датчики та веб-джерела даних для прийняття розумних операційних рішень, а не прості схеми керування вручну чи за фіксованим графіком.

Розумні системи кондиціонування повітря можуть передбачити очікувану кількість людей у домі, відстежуючи дані про місцезнаходження, щоб переконатися, що кондиціонер досягає бажаного рівня комфорту, коли в домі немає людей, і економити енергію, коли в домі немає людей.

Окрім підвищення комфорту, «розумні будинки» також можуть допомогти людям похилого віку жити самостійно. Розумний дім може допомогти виконувати повсякденні завдання, такі як прибирання, приготування їжі, покупки та прання. Система розумного дому, яка забезпечує своєчасне нагадування про прийом ліків, може підтримувати низькі рівні когнітивного зниження. Моніторинг стану здоров’я вдома може сповістити опікунів про те, щоб вони зреагували до того, як знадобиться дорога та важка госпіталізація.

Система дистанційного замикання гарантує, що вам ніколи не доведеться дублювати ключі або залишати запасні ключі під килимком. Це не тільки допоможе вам керувати доступом для членів сім’ї, але й для

надійних служб, як-от прибиральниці чи няні. Перевірити, чи двері та вікна зачинені, легше, коли фізичні перевірки більше не потрібні, ви можете просто запитати свій пристрій моніторингу. Ви можете посилити безпеку, дистанційно вмикаючи та вимикаючи світло, коли вас немає. Це створить у незнайомця враження, що ви вдома, навіть якщо вас немає у вихідні або ви працюєте допізна.

Віддалений доступ до камер відеоспостереження може дозволити вам помітити потенційні проблеми, наприклад, пакунки, залишені на виду на порозі або відчинені двері. Незважаючи на те, що більшість пристроїв розроблено, щоб полегшити ваше життя та надати можливість зберегти ваш розумний дім у безпеці, у розумних будинках все ще є деякі проблеми безпеки.

Але жодна з цих переваг неможлива, якщо ваша система розумного дому не є безпечною та надійною, а це означає, що ви отримаєте їх, лише якщо ви захистили свою мережу розумного дому та переконалися, що її не можна зламати.

1.2 Аналіз технологій обміну даними між розумними модулями

Системи «Розумний дім» (або системи домашньої автоматизації) і системи автоматизації будівель «побратими»: вони мають однакову технологію і однакові можливості управління, лише незначні відмінності в реалізованих функціях і кількості керованих пристроїв.

Спочатку розглянемо термін «протокол» і його значення. З точки зору мережі, протокол — це набір попередньо визначених правил і стандартів між пристроями. Пристрій може використовувати кілька протоколів, але для певних операцій можуть знадобитися певні протоколи. Протокол домашньої автоматизації— це те, як ця інформація передається на інші дротові та бездротові пристрої. Сьогодні на ринку представлено безліч різноманітних систем розумного будинку. Кожна система базується на певній технології

обміну даними між усіма розумними модулями домашньої системи. Ці різні технології відрізняються продуктивністю, ємністю, швидкістю передачі даних тощо.

Коли новий дім оснащений інтелектуальною електронікою, можна забезпечити професійне проектування, установку та налаштування системи. Однак у більшості випадків технологію розумного дому IoT можна поступово модернізувати в існуючі будинки за потреби. Часто немає постійної професійної підтримки на етапі проектування або етапі експлуатації розгортання розумного будинку IoT.

Табл. 1.2 - Мережеві стандарти

Назва	**Характеристика**
Interbus	Це шина даних датчика/приводу. RS 485 – інтерфейс на основі якого характеризується кільцева топологія. Важливим недоліком цієї системи є те, що коли один пристрій виходить з ладу, всі інші пристрої отримують поломку також. За допомогою топології кільця пристроям на шині не потрібні адреси, всередині кільця достатньо розташування для ідентифікації.
P-NET	Це шина головний-підлеглий. З інтерфейсом RS485 та RS 232, проте із значно меншою швидкістю передачі даних.
Profibus	Використовується інтерфейс RS485 або оптичний кабель, як середовище передачі даних. Є три можливих варіанти даної технології: Profibus-FMS (специфікація повідомлень польової шини), Profibus-DP (розподілена периферія), Profibus-PA (автоматизація процесів).
CAN (Мережа контролер)	Призначений для мобільних додатків із високою швидкістю передачі даних із використанням CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) під час передачі даних.

LonWorks	Це стандартизована шинна система (ANSI/CEA-709.1-B та EN ISO/IEC 14908), яка дозволяє інтелектуальним пристроям спілкуватися один з одним через локально керовані мережі керування. Мережеве рішення, для створення мереж автоматизації та управління. Він призначений для використання в централізованих контролерах автоматизації будівель, а також у децентралізованих системах управління будівлями.
BACnet (Building Automation and Control Network)	Використовується в багатьох системах автоматизації будівель по всьому світу удосконалений BACnet, як необхідність для стандартизованого протоколу передачі даних, щоб дозволити різним компонентам автоматизації та керування в будівлі спілкуватись один з одним, забезпечуючи взаємодію та незалежність від виробника.
Z-WAVE	Бездротова система нового покоління, що дозволяє всім електронним компонентам обмінюватися бездротовим зв'язком між собою та з користувачем. При цьому використовується радіосигнал з частотою 868,4 МГц і максимальною потужністю випромінювання приблизно 20 - 30 мВт. У той же час він використовує зрозумілі, безпечні радіохвилі не великої потужності, які можуть злегкістю проходити через стіни. Z-Wave застосовує мережеву топологію Mesh, тому може поширюватися далі, ніж радіохвилі. Стурктура не складна і практична в установці та в експлуатації, не потребує безліч знань та часу для установки і налагодження.
ENOCEAN	Технологія, заснована на ефективному застосуванні найменших змін в навколишньому середовищі, щоб уловити потрібну енергію, та згодом перетворити її на електрику, після чого, використовувати електрику як джерело живлення для надсилання радіочастотних сигналів від датчиків до виконавчих механізмів.
MODBUS	Розроблено Gould Modicon, який підтримується більшістю ПЛК. Він не складний, практичний у використанні, тому його застосовують виробники контролерів і засновники будівельного обладнання. Проте обмежується легким обміном даними, відповідно не може використовуватись для важчих потреб.

X10	Це протокол зв'язку між електронними пристроями, що використовуються в домашній автоматизації. В основному використовують дроти для сигналу та управління. За радіосигналом також визначається протокол передачі. Це перша технологія домашньої автоматизації, доступна в усьому світі сьогодні. Зараз він застарів нажаль, так як уповільнений (близько 20 біт/с).
ZIGBEE	Визначає протокол зв'язку високого рівня з використанням малопотужних цифрових радіосигналів на основі стандарту IEEE 802.15.4 для потреб бездротової мережі (медичні пристрої, димова сигналізація, охоронна сигналізація, автоматизація будівель). Однак, структура не складна та дешевша, ніж інші бездротові мережі, такі як Bluetooth. Найпотужніші вузли ZigBee містять лише 10% ПЗ типової Bluetooth або традиційної бездротової мережі, а найпростіші містять лише 2% .
DALI (DALIa, DALIb)	Це цифровий протокол зв'язку, спеціально розроблений для освітлення. DALI ідеально підходить для створення сценаріїв і отримання зворотного зв'язку від індикаторів несправностей, що робить його ідеальним для інтеграції з автоматизацією будівель для віддаленого моніторингу і обслуговування.
DMX 512/1990	Це стандарт передачі цифрових даних для диммерів і контролерів, що працюють в режимі постійного струму. Можна керувати до 512 каналів. Дані передаються пакетами. Усі пакети оновлюють усі вбудовані пристрої. Кожен пакет містить до 513 кадрів, які позначають початок і кінець кожного пакета. Хоча до пристрою неможливо отримати прямий доступ, інформація, що надсилається на пристрій, визначається в певній структурі кожного пакета.
Konnex (KNX)	Це назва технології та є стандартом. Такий спосіб був уніфікований та поширений у всьому світі європейськими стандартами (EN50090), китайськими стандартами (GB/T 20965), американськими стандартами (ANSI/ASHRAE 135) та міжнародними стандартами (ISO/IEC 14543-3).

Хоча існують дуже поширені професійні стандарти «розумного дому», такі як X.10 Powerline Communication, розроблені вони були швидше не маючи ніякого типу безпеки, як ці мережі керування домом було підключено до Інтернету. На даний момент часу існує безліч стандартів мережевих, які найкраще підходять для домашнього використання (Bluetooth, EnOcean, UPB, Zigbee, RS232, KNX, Zwave, Wifi,Thread, Insteon, Ethernet, C-bus, RS485). Кожний із цих стандартів має як слабкі так і сильні сторони, але сподіватися, що неоднорідна мережа з багатьма різними протоколами буде ефективно й безпечно керована неспеціалістами, є серйозною проблемою.

1.3 Постановка задачі

Метою даної роботи виступає детальний аналіз та розробка мікроконтролерної системи безпеки для «розумного дому» на основі широко використовуваної платформи Arduino Uno, датчиків руху для функцій управління системою та магнітоконтактних датчиків.

Об'єкт роботи - механізм взаємодії компонентів мікроконтролерної системи забезпечення «розумного дому».

Предмет роботи є дані датчиків системи.

Отже із мети та цілей випливає наступне формулювання *завдань* для кваліфікаційної роботи*:*

- детальний розгляд атак, уразливостей і системи безпеки розумної домівки;
- розбір платформ мікроконтролерів для убезпечення «розумного дому» ;
- розгляд та відбір мікроконтролера, який входить до складу забезпечення системи безпеки;
- підбір складових компонентів для розробки системи безпеки;
- оцінка проведення тестування розробленої системи захисту розумної домівки.

РОЗДІЛ 2. АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА МЕХАНІЗМІВ БЕЗПЕКИ РОЗУМНИХ ДОМІВОК

2.1 Вразливість розумних домівок та поширені атаки на розумні домашні пристрої

Дослідницький проект 2021 року виявив, що типовий розумний дім вразливий до атак чималою кількістю даних. Були повідомлення про атаки, спрямовані на розумні будинки, зокрема хакери дистанційно керували розумними світильниками та смарт-телевізорами, відмикали двері з підтримкою IoT, віддалено вмикали та транслювали відео зі смарт-камер.

Дві основні недоліки розумних будинків роблять їх уразливими до цих атак: уразливі локальні мережі та вразливі пристрої IoT.

Вразлива локальна мережа. Один пристрій може бути небезпечним. Деякі домашні пристрої IoT поспішно виходять на ринок, і їхня безпека, можливо, не була належним чином розглянута. У деяких випадках посібники користувача не стосувалися питань конфіденційності та не надавали достатньо інформації для забезпечення безпеки пристрою. Наприклад, радіоняні та камери безпеки були зламані, що дозволило злочинцям бачити, що відбувається вдома.

Фактично, багато експертів вважають, що коли IoT-пристрої зламують, це питання не «якщо», а «коли», тому що багато з цих пристроїв легко зламати.

Wi-Fi може бути вразливим через стандартні або слабкі SSID або паролі та вразливі протоколи шифрування. Облікові дані за замовчуванням дозволяють зловмисникам отримати доступ до маршрутизаторів без особливих проблем. Надійні паролі Wi-Fi змушують хакерів знаходити складніші шлюзи для проникнення в мережі.

Перехоплення та шифрування є найпоширенішими методами злому. Під час прослуховування хакер перехоплює будь-які пакети, що проходять

між пристроєм і маршрутизатором, передає їх на свій пристрій і використовує грубу силу. Зазвичай це займає лише кілька хвилин. Більшість маршрутизаторів Wi-Fi використовують протоколи безпеки: WPA (Wi-Fi Protected Access), WPA2, WEP (Wired Equivalent Privacy).

WEP — це потоковий шифр RC4. Одним із недоліків WEP є малий розмір вектора ініціалізації (24-бітний IV), через що його повторно використовують. Це повторення робить його вразливим.

Більш безпечними варіантами є WPA і WPA2. Але дослідники виявили серйозну вразливість KRACK, скорочення від Key Reinstallation Attack in WPA. Атаки типу Man-in-the-middle можуть використати це для викрадення конфіденційних даних, які надсилаються через з'єднання Wi-Fi із шифруванням WPA. Зловмисники можуть підслуховувати трафік і отримувати паролі, банківські облікові дані та інформацію про кредитні картки.

Вразливі пристрої IoT. Дослідники протестували загалом 16 звичайних розумних домашніх пристроїв від різних брендів і виявили 54 уразливості, які піддали користувачів хакерам. Можливість атаки варіюється від вимкнення систем безпеки до викрадення особистих даних. Близько 80% пристроїв IoT вразливі до різних атак.

Розумні домашні пристрої вразливі, тому що вони спеціально створені. Постачальники IoT не можуть надати необхідні спеціалізовані рішення безпеки. Крім того, розумні домашні пристрої часто працюють під керуванням невеликих операційних систем, таких як INTEGRITY, Contiki, FreeRTOS і VxWorks, і їхні рішення безпеки не такі надійні, як рішення систем на базі Windows або Linux.

Після розгортання більшість доступного обладнання не можна оновити, щоб не відставати від можливостей кіберзахисту, що розвиваються. Залежно від пристрою та протоколу зв'язку пристрої розумного дому можна атакувати різними методами.

Табл. 2.1 Основні види загроз

Вид загрози	**Опис**
Конфіденційність	Це ті, які призводять до безумисного розкриття конфіденційної інформації. Наприклад, недотримання приватності в системі домашнього моніторингу може призвести до ненавмисного розкриття приватних медичних даних. Навіть, як здається на перший погляд не шкідливе таке як температура в будинку та знання про роботу системи кондиціонування повітря, можуть бути використані, щоб визначити, чи є в будинку люди як передвісник крадіжки зі зломом. Втрата конфіденційності таких речей, як ключі та паролі, створює небезпеку нелегального доступу до системи.
Автентифікація	Дані загрози можуть призвести до фальсифікації або контролю інформації. Наприклад, неавтентифіковані сповіщення про статус системи можуть змусити операторів будівлі подумати про надзвичайну ситуацію та відкрити двері та вікна, щоб дозволити аварійні виходи, хоча насправді вони дозволяють незаконний вхід. Питання, яке буде порушено пізніше, стосується автоматизованих оновлень програмного забезпечення. Якщо вони не автентифіковані належним чином, можуть виникнути проблеми.
Доступ	Несанкціонований доступ до системного контролера, особливо на рівні адміністратора, може зробити всю систему незахищеною. Це може бути викликано неправильним керуванням паролем і ключем або підключенням до мережі неавторизованих пристроїв. Навіть без контролю неавторизовані підключення до мережі можуть викрасти пропускну здатність мережі або спричинити відмову в обслуговуванні для законних користувачів. Оскільки багато пристроїв розумного дому можуть працювати від акумуляторів і бездротових мереж із низькими робочими циклами, заповнення мережі запитами може призвести до атаки із виснаженням енергії, форми відмови в обслуговуванні.

Загальні методи атаки включають:

- Порушення даних і викрадення особистих даних. Незахищені пристрої IoT генерують дані та дають кіберзлочинцям широкі можливості для атаки на особисту інформацію. Це може призвести такі наслідки, як крадіжку особистих даних і шахрайських операцій.

- Крадіжка та втручання в пристрій. Інтелектуальні пристрої можуть бути захоплені, передаючи контроль зловмиснику. Зловмисник маніпулює пристроєм, втручається в зв'язок між двома сторонами та може отримати контроль над іншими пристроями або навіть усією мережею.

- Розподілена відмова в обслуговуванні (DDoS) - недоступність пристрою або мережевого ресурсу для призначених користувачів через тимчасове або невизначене переривання обслуговування.

- Миготіння - ця атака може пошкодити пристрій настільки, що його потрібно буде замінити.

Домашня мережа може бути незахищеною, і зловмисники можуть отримати доступ до будь-яких даних, що зберігаються в ній. Злочинці можуть відстежувати моделі використання різних пристроїв, наприклад, коли ви перебуваєте поза домом. Якщо ваша домашня мережа контролюється основним обліковим записом в Інтернеті, під загрозою можуть опинитися не лише дані з ваших пристроїв IoT. Будь-яке порушення може поставити під загрозу вашу особисту інформацію, зокрема електронні листи, облікові записи в соціальних мережах і навіть банківські рахунки.

Багато користувачів використовують свої смартфони для керування своїми підключеними будинками, що робить їх дуже цінною базою даних для тих, хто хоче зламати ваше життя. Це піддає вас високому ризику, якщо ваш телефон зламано, викрадено або якщо комусь вдасться підслухати ваше з'єднання.

Безпека має вирішальне значення для успіху розумного будинку. Відчувати себе в безпеці у власному домі є основною потребою людини. Наші домівки наповнені пристроями Інтернету речей, багато з яких уразливі

до цифрових загроз. Ми всі знаємо, що комп'ютери та смартфони становлять загрозу кібербезпеці: однак сьогодні навіть розумні холодильники та радіоняні мають підключення до Інтернету, яке може бути вразливим до атак і хакерів.

Близько 80% пристроїв IoT вразливі до різних атак. Зрозуміло, що підключення традиційно «автономних» розумних пристроїв, таких як освітлення, побутова техніка та замки, створює безліч ризиків для кібербезпеки. Навіть підключені до Інтернету радіоняні вразливі для цифрових зловмисників, і багато наляканих батьків лише пізніше дізнаються, що хакери спілкувалися з їхніми дітьми через заражені пристрої.

На закінчення можна відзначити, що доступність мережевої системи є основною вразливістю. Оскільки сучасні системи розумного дому підключені до Інтернету, атаки можна здійснювати віддалено, або через прямий доступ до веб-інтерфейсу керування, або шляхом завантаження шкідливого програмного забезпечення на пристрій.

Матеріальний доступ системи є проблемою. Можна отримати матеріальний доступ до мереж і бездротових технологій поза домом, навіть якщо будинок повністю замкнено.

Втілювання складних алгоритмів безпеки – перебувало в певних обмеженнях, так як контролери пристроїв є невеликими (8-розрядними мікроконтролерами), які володіють нечисленними пам'яттю та обчислювальними ресурсами.

Безліч продуцентів висувають прилади з відмінними можливостями оновлення програмного забезпечення та мережевими стандартами. Інколи ці прилади володіють малою документацією ато і взагалі вона відсутня, щодо внутрішнього програмного забезпечення, операційної системи та встановлених механізмів безпеки.

Виправлення прошивки — це також проблематична ситуація. Небагато розумних домашніх пристроїв пропонують регулярні поновлення ПЗ (програмного забезпечення), задля усунення вразливостей безпеки. Деякі

підозрюють, що зараз немає стимулів продовжувати корегувати програмне забезпечення або попереджувати прогалини в безпеці багато доларових пристроїв.

Повільне впровадження стандартів є слабкою ланкою. У той час як деякі пропрієтарні системи, такі як підсистеми моніторингу працездатності, можуть мати добре спроектовану безпеку, яка відповідає стандартам, більшість сучасних пристроїв розумного дому мають невеликий рівень безпеки.

Але найбільшою слабкістю є відсутність відданих спеціалістів із безпеки, які можуть керувати складністю мереж розумного дому. Небагато сімей можуть дозволити собі професійну постійну допомогу в управлінні домашньою мережею. Натомість власники будинків повинні мати змогу просто, безпечно та надійно керувати власними системами. Встановлення розумного дому з різними контрзаходами — це спосіб утримати небажаних зловмисників мережі.

2.2 Механізми захисту пристроїв розумного дому

Низка контрзаходів безпеки може захистити пристрої IoT і інсталяції розумного дому, не порушуючи роботу Інтернету. Керування життєвим циклом безпеки гарантує, що розумні пристрої, які більше не використовуються, виводяться з експлуатації, щоб запобігти їх використанню та становленню загрози безпеці для служб. Деякі пристрої мають вбудовані функції безпеки, і для того щоб пристрої розумного дому могли захиститись від атак, їхні мають дотримуватись засобів захисту (табл.2.2).

Управління життєвим циклом безпеки. Управління життєвим циклом безпеки дозволяє постачальникам мережевих послуг і ПК контролювати безпеку пристроїв IoT і керувати ними під час їх підключення та роботи. У разі кібератаки використовуйте ключі пристроїв Rapid Over The Air (ROTA), щоб мінімізувати перебої в роботі.

Табл. 2.2 – Основні засоби захисту

Засоби захисту	**Рекомендації до їх застосування**
Технологія безпечного завантаження	Технологія безпечного завантаження запобігає використанню хакерами зашифрованих кодів для встановлення шкідливих програм. Це гарантує, що підключені пристрої використовують код, згенерований OEM пристрою або іншими авторизованими та надійними третіми сторонами, запобігаючи зловмисним атакам.
Надійні паролі	Переконайтеся, що ваш маршрутизатор і всі пристрої мають надійні паролі. Паролі, збережені за умовчанням, є звичайною точкою входу для хакерів.
Гостьові мережі	Якщо можливо, налаштуйте пристрої розумного будинку за допомогою гостьової мережі. Це допомагає відокремити пристрої від цінної інформації, що зберігається на ноутбуках або телефонах. Навіть якщо кіберзлочинці скомпрометують один із пристроїв IoT, вони не зможуть проникнути в основну мережу та скомпрометувати підключені до неї комп'ютери та смартфони.
Двофакторна автентифікація	Інсталяції «розумного дому» мають бути підключені до домашньої мережі, щоб працювати належним чином, і перед тим, як це зробити, необхідно пройти автентифікацію перед надсиланням і отриманням цінних даних. Коли пристрій потребує додаткової перевірки за допомогою мобільного пристрою або програми автентифікації, увімкнення двофакторної перевірки дійсності набагато зменшує можливість хакерів підробити пристрій. Двостороння автентифікація гарантує, що всі дані надходять із безпечних і відомих пристроїв, а не з заражених і шкідливих джерел. Двостороння автентифікація використовує алгоритми шифрування з симетричними та асиметричними ключами, щоб гарантувати оптимальний захист і уникнути шахрайства.
Оновлення мікропрограми	Багато пристроїв хочуть отримати автоматичне оновлення, ручну перевірку та оновлення мікропрограм вашого маршрутизатора або пристрою IoT гарантує, що найновіші протоколи безпеки активні.
Уникайте хмари	Використовуйте локальне сховище: вам слід використовувати зберігання локально, а не в хмарі, щоб мінімізувати ризик атаки під час отримання даних у хмарі.
Шифрування найвищого рівня	Використовуйте на маршрутизаторі шифрування найвищого рівня (WPA3), щоб забезпечити безпечний зв'язок. Шифрування забезпечує безпечний зв'язок, дозволяючи лише тим, хто має захищені описові ключі, отримувати доступ до даних, отриманих і переданих між установками розумного дому та мережевими службами.

Брандмауер	Використання брандмауера є популярним способом захисту пристроїв розумного дому. Брандмауери дозволяють користувачам переглядати потенційні атаки та керувати рівнем безпеки окремих підключених пристроїв. колись знайдено аномалії в мережі або пристрої, брандмауер надсилає сповіщення хосту.
Моніторинг і аналіз безпеки	Процес моніторингу та аналізу безпеки використовує критично важливі дані, такі як дані термінального пристрою та трафік мережевого з'єднання, і перевіряє їх для виявлення загроз безпеці та вразливостей системи. У разі виявлення будь-яких підозрілих загроз або зломів буде вжито найбільш відповідних контрзаходів, зокрема розміщення пристрою на карантині, доки він більше не представлятиме загрозу. Процес моніторингу, аналізу та дій відбувається в режимі реального часу, щоб забезпечити захист інтелектуальних приладів і пристроїв від маніпуляцій, які можуть призвести до неточного моніторингу та аналізу.

2.3 Аналіз існуючої підтримки безпеки в протоколах IoT

Здебільшого чисельна кількість пристроїв IoT застосовують мікроконтролери які мають лімітовану пам'ять і самі нижчого класу, відповідно потребують низького енергоспоживання. Цей тип контролера ідеально підходить для автономного контролера, наприклад, пральної машини або кондиціонера.

Дані критерії дають ускладнення переходу до мережевих контролерів IoT, оскільки для цих вбудованих пристроїв часто не розроблені існуючі Інтернет-протоколи. Для вирішення таких ускладнених питань було створено декілька інженерних робочих груп Інтернету (IETF).

Робота IETF зі стандартизації IoT зіграла важливу щоденну роль у запровадженні важливих полегшених протоколів зв'язку із обмежених середовищ через існуючі IP-мережі. До них належать IPv6 через бездротові персональні мережі з низьким енергоспоживанням (6LoWPAN: RFC 6282),

для мереж із низьким енергоспоживанням і мережами протокол обмежених додатків (CoAP: RFC 7252) та з втратами (RPL: RFC 6550).

На рисунку 2.1 показано порівняння стеків протоколів IETF IoT і TCP/IP. Загроза безпеки, яка виикаю в інтернеті, також загрожує безпеці та конфіденційності IoT, коли пристрої підключені до Інтернету.

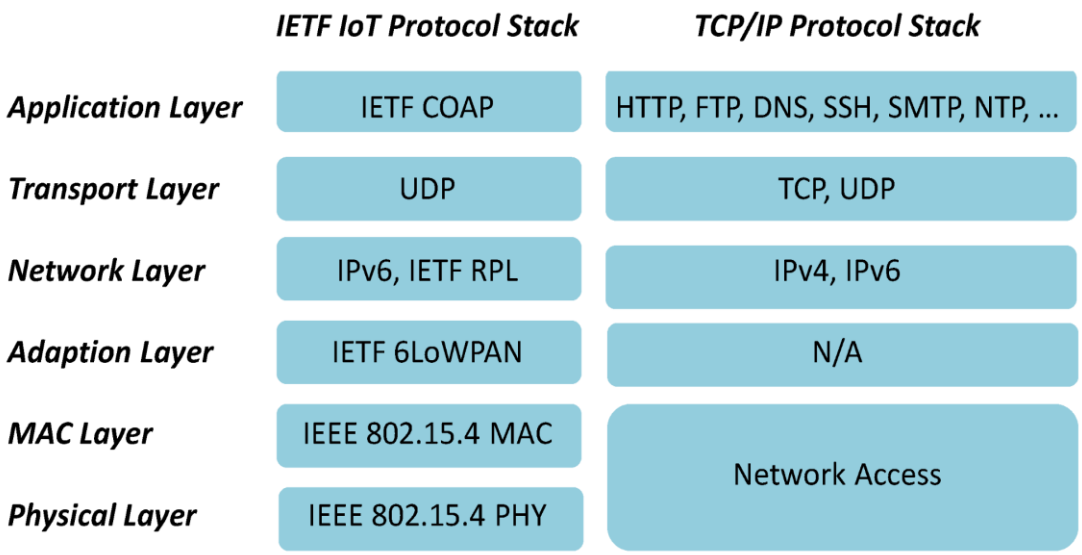

Рисунок 2.1 - Порівняння стеків протоколів IETF IoT і TCPIP

2.3.1. 6LoWPAN і безпека

Стандарт IEEE 802.15.4 для бездротових персональних мереж був визначений інститутом інженерів з електротехніки та електроніки.

Специфіка стандарту визначати як мають працювати фізичні рівні та рівні керування доступом до носіїв у типових середовищах для цих мереж із низькою пропускною здатністю, низькою вартістю та низькою швидкістю. Легкий протокол, який дозволяє передавати пакети IPv6 через бездротові мережі IEEE 802.15.4 —6LoWPAN.

Internet Protocol Security Suite (IPsec) визначає Authentication Header (AH) і Secure Payload Encapsulation (ESP) задля убезпечення неподільності даних, конфіденційності, автентифікації джерела та захисту від поновленого відтворення пакетів.

Для мереж схема ключів та автентифікації більш розширена 6LoWPAN (EAKES6Lo) розділена на два кроки задля удосконалення охоронної системи безпеки мереж 6LoWPAN: конфігурація системи, автентифікація та ключ.

На кроці 1: у мережі для шифрування передачі даних застосовується симетричне шифрування Advanced Encryption Standard (AES). Використовуються хеш-функції алгоритму дайджесту повідомлень 5 (MD5) або алгоритму безпечного хешування (SHA) задля перевірки цілісності даних.

Крок 2: обміняйтеся 6 повідомленнями, завершіть автентифікацію та обробку ключів і встановіть взаємну автентифікацію. Таким чином, надається шаблон для убезпечення бездротового зв'язку навіть для пристроїв з обмеженими ресурсами 6lowPAN.

2.3.2 RPL і безпека

Кардинальною частиною традиційних мереж є протоколи маршрутизації, це вважається вірним та справедливим для мереж 6LoWPAN. Протокол спеціально розроблений для мереж з мінімальними втратами і низьким енергопостачанням (LLN), оптимізований протокол маршрутизації IPv6 — RPL. Топологія відображення протоколу базується на структурі DODAG (Destination-Oriented Directed Acyclic Graph), це протокол дистанційної векторної маршрутизації.

У дереві DODAG всі вузли, крім кореня, повинні мати батьківський елемент, тому дуже важливо, щоб вузли правильно вибирали своїх батьків. Рівні RPL використовують для опису положення вузлів у топології дерева. Тому існуючі рішення можна надійно створити безпечні переліки маршрутизації в межах розумного будинку.

2.3.3 CoAP і безпека

CoAP — це HTTP-подібний протокол прикладного рівня, розроблений для обмеженої мережі, і оскільки, пристрій має певні особливі вимоги, як-от групове спілкування в мережі Інтернету речей, CoAP забезпечує підтримку багатоадресної передачі, яка немає у HTTP.

CoAP використовує протокол дейтаграм користувача (UDP) для кращого пристосування до з'єднань із низьким показником кількості одиниць інформації і середовищ із низьким обсягом комп'ютерів. У порівнянні з протоколом керування передачею (TCP), з меншою затримкою без підключення простішим протоколом транспортного рівня є UDP.

CoAP — це протокол без збереження стану, заснований на архітектурній моделі клієнт/сервер. Операція запит/відповідь використовується задля обміну інформацією між сервером та клієнтом. Як і HTTP, CoAP базується на моделі Representational State Transfer (REST).

Найпоширенішим протоколом шифрування для HTTP на даний момент часу є безпека транспортного рівня (TLS: RFC 5246), проте втілення TLS з обмеженими ресурсами надто ускладнене для пристроїв IoT. CoAP застосовує Datagram Transport Layer Security (DTLS: RFC 6347) протокол безпеки для забезпечення зв'язку безпеки. TLS і DTLS надають одинакові служби безпеки.

Головна відмінність між DTLS і TLS зводиться до того, що TLS заснований на TCP, тоді як DTLS заснований на UDP. В специфіці CoAP відзначаються різні чотири рівні безпеки. Пристрої можуть перебувати в одному з чотирьох режимів безпеки: PreSharedKey , RawPublicKey , NoSec, і Certificate. Подібним чином стандарти IETF забезпечують механізми безпеки для безпечного веб-зв'язку через обмежені мережі.

РОЗДІЛ 3. ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ В СИСТЕМІ «РОЗУМНИЙ ДІМ»

3.1 Система безпеки «Розумний дім»

Система безпеки «розумний дім» - це автоматизована система, яка встановлює захист за допомогою системи взаємодіючих компонентів і пристроїв. Одним словом, ви можете контролювати безпеку свого будинку одним натисканням кнопки. Основне призначення системи безпеки будинку - захистити безпеку людей і майна в будинку.

3.1.1 Мікроконтролерні платформи для систем безпеки «розумного дому»

Всі можливості систем безпеки можна реалізувати за допомогою мікроконтролерних систем, які сьогодні стрімко прискорюють темпи розвитку. Це пов’язано зі стрімким зростанням ролі електронних пристроїв у житті та повсякденному житті людей, а також із дедалі складнішою природою цих пристроїв. Не менш важливим фактором є принципова спрямованість сучасних розробок на мініатюризацію та максимальну компактність систем електронного обладнання без втрати їх ефективності та продуктивності.

Мікроконтролер - це в свою чергу однокристальний мікрокомп'ютер, виконаний у вигляді мікросхеми, який є дуже компактним і в той же час функціональним пристроєм. Мікроконтролер, здатний забезпечити працездатність та ефективну взаємодію кількох пристроїв в одній системі, є невід’ємним компонентом якісної системи убезпечення охоронної системи розумної домівки та може бути глибоко інтегрований в інші підсистеми комплексу «Розумний дім».

Мікроконтролерні системи для «розумного будинку» - системи пристроїв, об'єднаних в єдиний комплекс для максимального комфорту і особистої безпеки - сильно залежать від ефективності і функціональності мікроконтролерів. [3].

Для забезпечення повноцінної роботи таких систем, забезпечення їх ефективності, доступна велика кількість мікроконтролерів. До таких мікроконтролерів належать, наприклад, NodeMCU, Arduino UNO, MSP430, STM32VL-Discovery, які є функціональними мікроконтролерами, що забезпечують роботу таких систем.

Одним із найпоширеніших сімейств мікроконтролерів сьогодні є сімейство мікроконтролерів Arduino. Вони широко використовуються в системах безпеки «розумного будинку».

Набір мікроконтролерів об'єднаний стандартною структурою і програмною оболонкою, що дозволяє легко інтегрувати нові елементи в систему без ускладнення системи шляхом переходу з одного програмного середовища в інше.

У свою чергу, на фізичному рівні реалізації потреба в ускладненні системи через необхідність забезпечення роботи компонентів різних архітектур інакше вимагається бути сумісними, або штучно забезпечити зникнення цієї сумісності, що може призвести до подальшого завершення системи Проблеми в . Мікроконтролери сімейства Arduino відомі простотою програмування, створення систем спеціального призначення та встановлення великої кількості сумісних пристроїв, низьким енергоспоживанням.

Це дозволяє швидко створити єдину систему з великою кількістю елементів і, при необхідності, використовувати кілька підключених мікроконтролерів, кожен зі своєю спеціалізацією, розширюючи можливий діапазон функціональних можливостей системи і її загальне призначення. Теоретично масштабованість таких систем обмежена лише споживанням енергії для розробки системи, фізичної реалізації та програмування.

Також необхідно знати про особливості програмування сімейства мікроконтролерів Arduino. Винятково задля цього сімейства створено спеціальне програмне середовище Arduino IDE. Він написаний на Java на основі проекту Processing, який використовує мову Arduino C на основі мови C++.

Тому мова програмування Arduino вимагає деякого часу, щоб розкрити деякі унікальні особливості мови, проте в результаті стає простіше застосовувати сімейство мікроконтролерів Arduino з часом. Така перспектива ефективно доповнює уніфіковану конструкцію цього сімейства мікроконтролерів і компонентів, які були наумисно розроблені або видозмінені для сумісності з мікроконтролерами Arduino [4].

Тому, незважаючи на відносну простоту сімейства мікроконтролерів Arduino, вони все ще популярні і широко використовуються. Розробка і випуск мікроконтролера Arduino були завершені в 2005 році. Завдяки високій доступності та простоті використання мікроконтролерів така оказія відізвалась значно помітно на розвитку систем «розумного дому», тим самим розширюючи коло користувачів, які можуть встановити систему «розумний дім».

3.1.2 Вибір мікроконтролера для проекту

Плата з сімейства Arduino, застосовувана для втілення та реалізації системи безпеки «розумного будинку». Arduino Uno у видозміні Arduino Uno Rev3 було вибрано, як найлогічніший варіант для структурної будови безпечної системи (рис. 3.1).

Ця плата використовується в багатьох сферах, найпопулярнішими з яких є системи «розумного будинку», робототехніка, системи безпеки, квадрокоптери, невеликі метеостанції тощо.

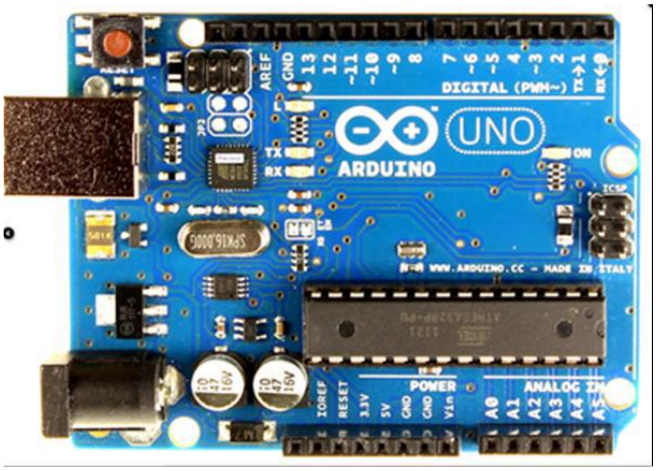

Рисунок 3.1 - Плата Arduino UNO Rev3

Arduino Uno є найзбалансованішим, ніж інші популярні розробки в сімействі Arduino. Arduino Uno володіє більшим об'ємом пам'яті – 32 Кб, ніж Arduino Nano, який має об'єм пам'яті 16 Кб, необхідний для систем безпеки, які часто складаються з великої кількості компонентів, але має більший розмір: 6,9 см у довжину, і 5,3 см в ширину, тоді як Arduino Nano має 4,2 см в довжину і 1,85 см в ширину.

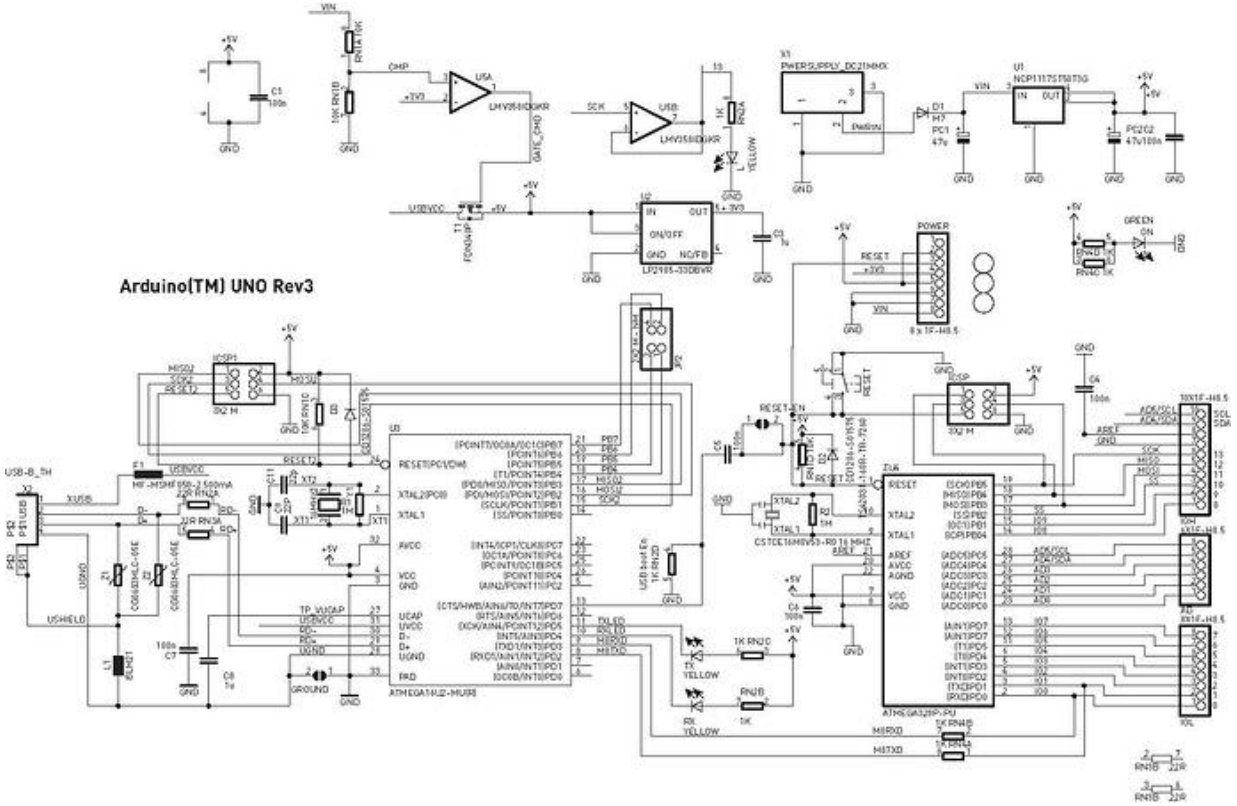

Рисунок 3.2 - Схема плати Arduino Uno Rev3 [9]

У той же час плата Arduino Uno менша, ніж інші популярні плати Arduino Mega, з її новою версією, Arduino Mega 2560, і її USB-сумісною модифікацією, Arduino Mega ADK, розміром 10,2 см в довжину і 5,3 см в ширину, з більшою кількістю входів/виходів.

Зате такий розмір і потужність зазвичай надлишкові і використовуються лише у великих системах з великою кількістю непростих компонентів.

3.1.3 Компоненти розробки

На додаток до Arduino Uno Rev3 мікроконтролера задля системи безпеки розумної будівлі, використовується декілька сенсорних підсистем, а саме датчики руху та магнітоконтактні датчики. Ці компоненти покликані забезпечити одну з двох основних функцій системи безпеки «розумного будинку», яка полягає у виявленні спроб проникнення на об’єкт, що охороняється. Тому, крім мікропроцесора, система буде складатися з компонентів, розглянутих нижче.

Датчик руху HC-SR501 (рис. 3.3). Цей датчик є інфрачервоним датчиком руху для Arduino та інших мікроконтролерів. Він дозволяє виявляти рух людей або домашніх тварин. Датчик оснащений двома входами живлення (+5 В і 0 В) і цифровий вихід, який можна використовувати для збору даних. Якщо перешкоди немає, то високий (3,3 В), якщо перешкода є, то низький (0 В).

Рисунок 3.3 - Датчик руху HC-SR501

Магніто-контактний датчик МС-38 (рис. 3.4). Даний датчик застосовують для подання сигналу при відкритті дверей та вікон, а також застосовується для сигналізації.

Рисунок 3.4 - МС-38Магнітно-контактний датчик

Датчик спроектований на основі двох елементів: в пластиковому корпусі магніта і датчика, які володіють однаковою формою. Посередині датчика розташований геркон з нормально розімкненим контактом. Коли двері закриті, контакти датчика замикаються, коли магніт наближається до датчика, і розмикаються, коли двері відкриваються.

Вивіска або макет. У рамках кваліфікаційної роботи використовують Arduino Shields - спеціальну технологію, деталь, яка дозволяє збільшити кількість входів і виходів, доступних плат, пристроїв або інших елементів системи. Shields — це інструмент, який дозволяє примножити можливості кожної плати Arduino. У рамках цього проекту буде використовуватися звичайний невеликий макет для більш зручного підключення деяких елементів системи.

Резистор. Для підвищення загальної надійності у системах безпеки резистори реалізовують роль елементів.

У той же час плата Arduino Uno менша, ніж інші популярні плати Arduino Mega, з її новою версією, Arduino Mega 2560, і її USB-сумісною модифікацією, Arduino Mega ADK, розміром 10,2 см в довжину і 5,3 см в ширину, з більшою кількістю входів/виходів.

Зате такий розмір і потужність зазвичай надлишкові і використовуються лише у великих системах з великою кількістю непростих компонентів.

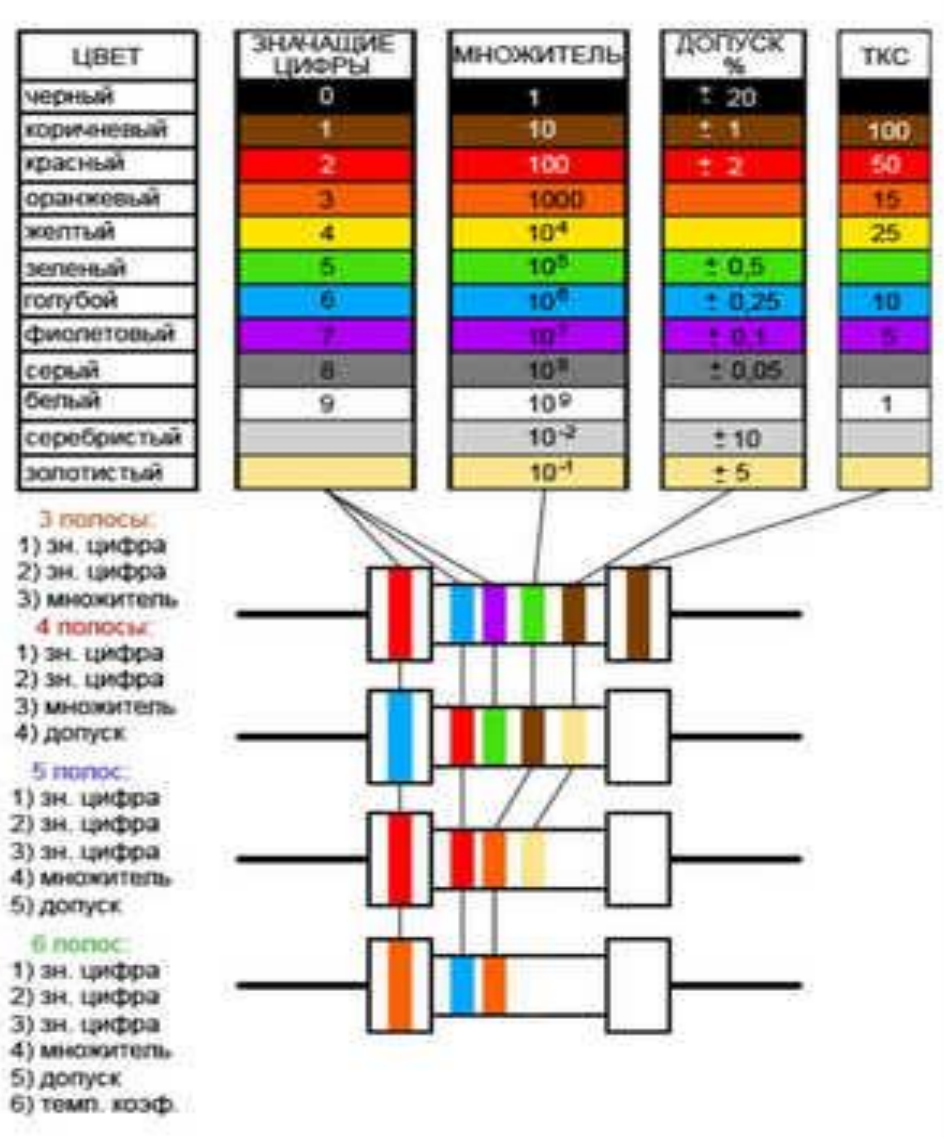

Рисунок 3.5 - DIP резистор і таблиця його кольорів [8]

Резистори дають обмеження на напругу, яку можна подавати на компоненти системи, пристрої та світлодіоди, зменшуючи ймовірність пошкодження. У розробленій протиугінній системі використовуються резистори DIP в яких незмінний опір і ноінали яких можна визначити за кольором проводки на корпусі і самому корпусі (рис. 3.5).

Мембранна клавіатура 4x4. Використовується для перемикання системи «Розумний дім» із звичайного режиму в режим роботи системи безпеки (рис. 3.6).

Рисунок 3.6 - Мембранна клавіатура 4x4

Для роботи клавіатури потрібна бібліотека Keypad Arduino. Цю бібліотеку потрібно використовувати з будь-якою клавіатурою матричного типу. Ця бібліотека має на меті забезпечити рівень абстракції для обладнання. Код можна писати та читати легше, якщо приховати від користувача виклики функцій в останній версії pinMode і digitalRead.

Рисунок 3.7 – LCD1602рідкокристалічний дисплей

Починаючи з версії 3.0, бібліотека була переписана та модифікована для підтримки кількох клацань без написання додаткового коду. При цьому

бібліотека не втратила свій основний функціонал і залишається повністю сумісною з кодом, написаним для попередніх версій. LCD 1602 Рідкокристалічний дисплей (рис. 3.7). Для відображення символів є 2 рядки та 16 стовпців.

Даний компонент застосовується для зміни режиму роботи системи та передачі даних з клавіатури та легшого введення кодів. Єдине, що залишилося зробити після зв'язку бібліотеки, це автоматично змінюється доданий вхід посилання на той, що використовується в проекті, як показано в лістингу 3.1.

Лістинг 3.1. Замініть входи, автоматично встановлені бібліотекою, входами, які використовуються в ідеї.

```
LiquidCrystal lcd(12, 11, 5, 4, 3, 2); //автоматично задані
входи
LiquidCrystal lcd(4, 5, 10, 11, 12, 13); //входи використані у
проекті
```

DFRobot Rotary Sensor V2— це потенціометр, призначений для регулювання напруги в ланцюгах. При включення змінює опір свій, діє як змінний резистор, таким чином регулюючи напругу.

У рамках цього як регулятор яскравості використовується цей пристрій для РК-дисплея. Реалізація системи здійснюється на емуляторі мережі, призначеному для імітації фізичної частини системи на базі Arduino та надання можливості її програмування. Сервіс Tinkercad Arduino використовується для максимально точного відображення того, що відбувається з системою в реальному часі.

3.2 Опис системи безпеки «Розумного дому»

Система безпеки, розроблена в рамках сертифікації, має кілька основних особливостей. Система «Розумний дім» має два різних режими роботи.

У першому режимі він виконує основні функції «розумного будинку», покликані полегшити повсякденну діяльність. Система за допомогою магнітних контактних датчиків вмикає світло при відкритті вхідних дверей, а за допомогою датчиків руху вмикає освітлення коридору, коли поруч є власник.

У другому режимі включається система безпеки «розумний дім» для виявлення вторгнень. У цьому режимі датчик, призначений для включення світла, активує охоронну сигналізацію. Рішення системи безпеки «розумний дім» показано на рисунку 3.8.

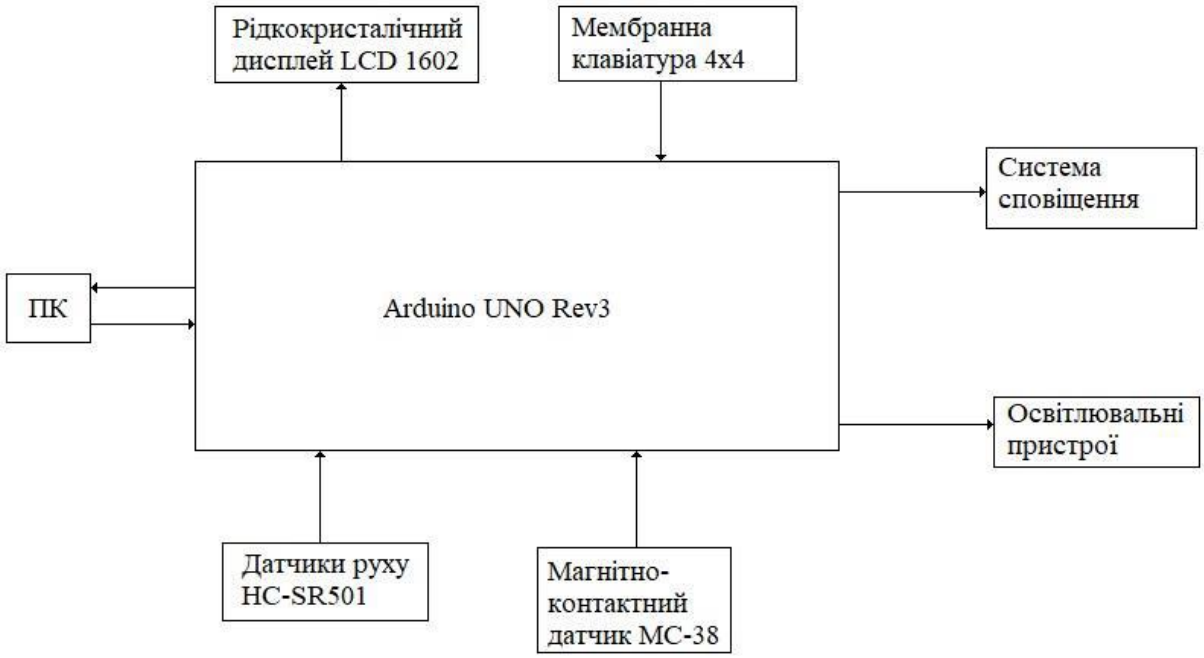

Рисунок 3.8 – Схематичне системне рішення «Розумний дім»

Плата Arduino Uno Rev3 повинна бути підключена до джерела живлення, бажано до комп’ютера, щоб контролювати її стан. Через цифрові порти 13-8 до плати підключений рідкокристалічний дисплей LCD 1602. Розрахований він для відображення кодів, даних про стан системи за допомогою клавіатури

Через цифрові порти 7-0 підключається мембранна клавіатура 4x4. Для введення кодів в систему клавіатура необхідна, змінюючи режим її

працездатності. За умови введення правильного коду система переходить із звичайного режиму в безпечний, а при введенні неправильного коду система сигналізує про загрозу.

Магнітно-контактний датчик МС-38 і датчик руху HC-SR501 відповідають за реакцію системи на певні дії в будинку і передавала відповідні сигнали в систему. Датчик руху в домашньому режимі подає системі освітлення сигнал для її активації, коли в його робочій зоні присутній рухомий об’єкт. У безпечному режимі датчик сигналізує про загрозу. На вхідних дверях встановлені магнітно-контактні датчики, які активують освітлення при відкриванні в домашньому режимі.

Якщо двері відкриваються в безпечному режимі, надсилається, сигналізує про загрозу. Системи освітлення можуть бути встановлені приналежній основі кімнат і побажань власника.

При необхідності систему освітлення можна модифікувати або оснастити забезпечення більш стабільної роботи додаткових активаторів, які безпосередньо не підключаються або підключаються до системи. Слід налаштувати систему сповіщення згідно потреб та вимог конкретних ситуацій. Сигналом може бути звукова «сирена» або передавач, який посилає сигнал тривоги власнику будинку або охоронцю.

3.3 Реалізація пристрою

Комплекс систем безпеки «Розумний дім», створена на основі Tinkercad Arduino Services. Сервісу не вистачає деяких компонентів, необхідних для забезпечення охоронної системи, тому їх замінюють інші з подібною функціональністю та вихідними даними.

Датчики руху замінені кнопками, а контактні – перемикачами. Остаточну поставу системної моделі показано на Рисунок 3.9.

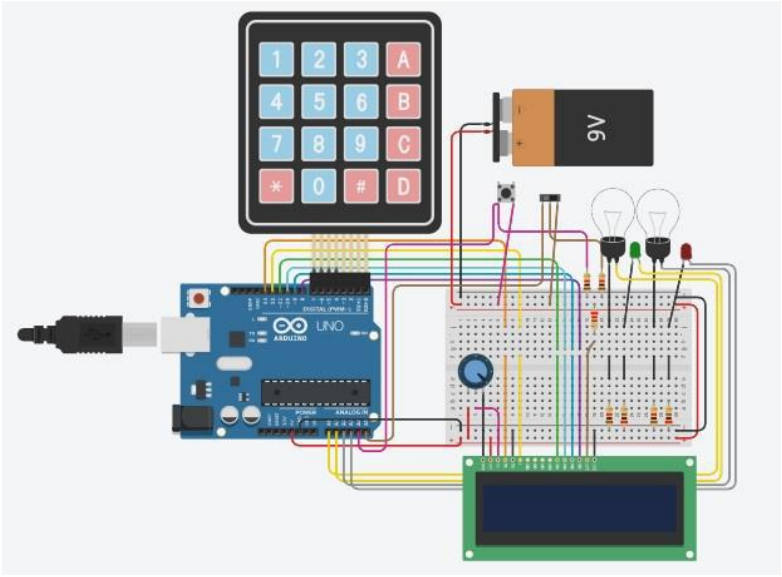

Рисунок 3.9 - Рішення системи безпеки «Розумний дім» у Tinkercad Arduino Services

Акумулятор 9 В на рисунку є зовнішнім джерелом живлення, яке призначене лише для демонстрації. У процесі написання програми використовуються 2 бібліотеки. З'єднання для необхідних бібліотек є такими:

```
#include <Keypad.h>
#include <LiquidCrystal.h>
#define NUM_KEYS 4
```

Лістинг показує виконання: основний цикл програми, тут викликаються всі бібліотеки, необхідні для роботи системи. Вони відповідають за спрощення підключення клавіатури, а також бібліотек підключення, необхідних для полегшення підключення РК-дисплея до системи. Теж був створений макрос, який буде потрібний для подальших маніпуляцій коректного вводу коди з клавіатури для аналізу роботи системи. [5]

Значення та кількість клавіш для налаштування мембранної клавіатури 4x4 наведено в лістингу 3.2.

Лістинг 3.2 – Встановлення значення та кількість клавіш мембранної клавіатури 4x4

```
const byte ROWS = 4;
const byte COLS = 4;
char keys[ROWS][COLS] = {
{'1','2','3','A'},
{'4','5','6','B'},
{'7','8','9','C'},
{'#','0','*','D'}
};
byte rowPins[ROWS] = {7, 6, 5, 4};
byte colPins[COLS] = {3, 2, 1, 0};
Keypad keypad = Keypad( makeKeymap(keys), rowPins,
colPins, ROWS, COLS );
```

Елемент коду встановлює значення кожної клавіші, яка підключена до системи мембранної клавіатури, і кількість самих клавіш. Перші два рядки вказують кількість ключів, вказуючи кількість рядків і стовпців ключа. У даному варіанті це клавіатура 4x4 з 16 клавішами.

Наступні п'ять рядків коду описують значення кожного ключа безпосередньо з його позиції в попередньо визначених стовпцях і рядках. Далі налаштуйте входи в двох рядах, з яких клавіатура підключена до плати.

Наступні рядки коду необхідні для реалізації клавіатури як програмного об’єкту, для подальшого використання. Він застосовує попередньо визначену схему клавіш за допомогою функції makeKeymap() бібліотеки Keypad.

Перший рядок лістингу 3.3 визначає входи, які використовуються для підключення РК-дисплея до системи. Наступний рядок визначає змінну, яка зберігатиме натиснуті клавіші на клавіатурі. У третьому рядку потрібно вказати масив символів, який зберігає дійсні паролі слід замінити для стану системи.

Слідом вказати масив, в якому будуть зберігатися дані про символи, введені з клавіатури. Потім вводяться дві змінні, які підраховують кількість звернень (k) і кількість символів, які відповідають правильному значенню (s).

Лістинг 3.3 – Налаштування входу, який використовується для підключення РК-дисплея, і встановіть змінні

```
LiquidCrystal lcd(13, 12, 11, 10, 9, 8);
char key;
char myarray[NUM_KEYS]={'1','2','3','4'};
char button_pressed[NUM_KEYS];
int k=0;
int s=0;
```

Лістинг 3.4 Включає функції налаштування. У третьому рядку вказується кількість стовпців і рядків РК-екрану, яка необхідна для коректного відображення символів у майбутньому.

Лістинг 3.4 – Налаштування параметрів екрана та аналогових входів

```
void setup()
{
lcd.begin(16, 2);
pinMode(A0,OUTPUT);
pinMode(A1,OUTPUT);
pinMode(A2,OUTPUT);
pinMode(A3,OUTPUT);
pinMode(A4,INPUT);
pinMode(A5,INPUT);
}
```

Наступні рядки визначають аналоговий вхід і вихід. У цьому випадку введенням будуть числа. Необхідно позначити порт як вхід (2) і вихід (4) залежно від їх майбутнього використання.

Лістинг у Додатку А показує основний цикл обробки показників датчиків, а саме керування екраном і освітленням, рядки 3–18.

Перший рядок коду встановлює курсор, який буде вводити текст у другій позиції першого рядка на екрані. Це необхідно для запуску відображення символів на екрані, оскільки без цього параметра система не зможе розпочати відображення символів без початкової позиції. Згодом у наступному рядку текст виводиться на екран. Наступна частина коду призначена для визначення розумного домашнього освітнього процесу системою датчиків. Коли сигнал надходить від датчика до вхідного порту, реагує відповідна частина системи освітлення. Коли сигнал надходить з порту A4 (датчик руху), сигнал надходить на порт A0 (світло), а коли сигнал надходить з порту A5 (контактний датчик), сигнал надходить на порт A1. Процес показано в рядках з 5 по 17. Рядок 18 у списку є причиною затримки. Це необхідно для того, щоб освітлення, яке працює після отримання сигналу, перестало працювати, якщо сигнал переривається.

Лістинг додатку А, рядки 20–33, демонструє читання даних із клавіатури та їх аналіз. Метою рядка 20 лістингу є надання можливості читати дані з клавіатури. Ці дані важливі та потрібні для подальшої роботи системи. Наступний рядок використовує ці дані для виконання подальших операцій у наступній операції. У рядку 23 змінній k присвоюється значення, що відповідає кількості натискань клавіш, а в наступному рядку змінюється значення змінної відповідно до даних попереднього рядка. Рядок 25 встановлює курсор на РК-екрані. Після кожної зміни значення змінної k курсор переміщується на одне значення в рядку. Рядок 26 відповідає за виведення на екран символів, введених з клавіатури.

Наступна частина перевіряє правильність символів, введених з клавіатури. Це робиться шляхом перевірки змінних і порівняння і даних, введених і змінених у попередніх рядках. Рядок 27 порівнює кількість щоб було введено правильну кількість символів. Якщо дані збігаються, введені дані дійсні. Ця перевірка виконується шляхом збільшення значення змінної s,

яка діє як лічильник. Рядок 34 лістингу відповідає за порівняння кінцевого значення після введення чотирьох символів.

Далі відбувається налаштування React для введення правильного коду. Рядок 35 очищає екран від раніше введених символів, а потім встановлює курсор у початкову позицію. Далі вимкніть освітлення, якщо було не вимкнене при зміні режимів системи. Після цього на екрані з’явиться нове повідомлення («Завершення роботи системи»). Наступний рядок відповідає за управління системою безпеки. При отриманні сигналу від будь-якого датчика світлодіод реагує, показуючи, що система сигналізації активована. Коли систему деактивовано, світлодіоди вимикаються (якщо вони активні), а екран очищається. Змінні також очищаються, а їх значення встановлюються на нуль. Це необхідно для подальшої роботи системи і забезпечує можливість повторного введення коду без повного перезавантаження системи.

В іншому випадку система відреагує на неправильне введення пароля інакше, рядки 59 - 73. Початковий алгоритм узгоджується з роботою при вході в систему введених правильних даних. Система очищає екран і переміщує курсор у початкове положення.

Однак згодом з’являється інше повідомлення («Код помилки»). Потім курсор переходить до наступного рядка в тому ж стовпці та відображає інше повідомлення ("Alarm!").

Крім того, обидва світлодіоди активовані, вказуючи на те, що тривога спрацювала. Після цього система повертається в початковий режим.

3.4 Дослідження продуктивності системи

Система безпеки розумного дому тестувалася за допомогою послуги Tinkercad Arduino. На рисунку 3.10 показано систему безпеки розумного будинку, яка успішно працює в домашньому режимі.

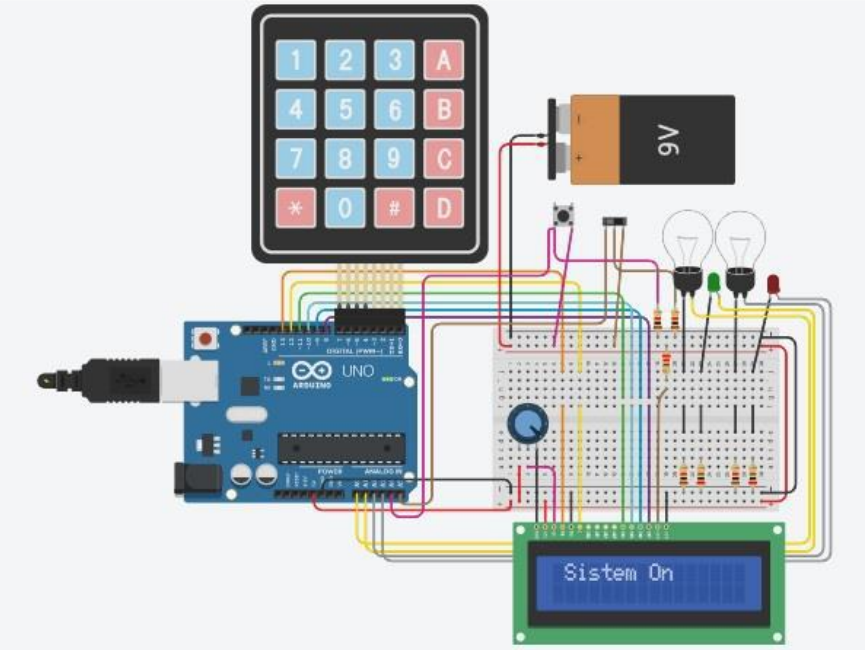

Рисунок 3.10 - Система безпеки «Розумний дім» у домашньому режимі на симуляторі служби Tinkercad Arduino

Після підключення система виглядає так: відображає на екрані повідомлення «System On» (Система ввімкнено), інформуючи користувачеві про активність системи в режимі «Smart Home».

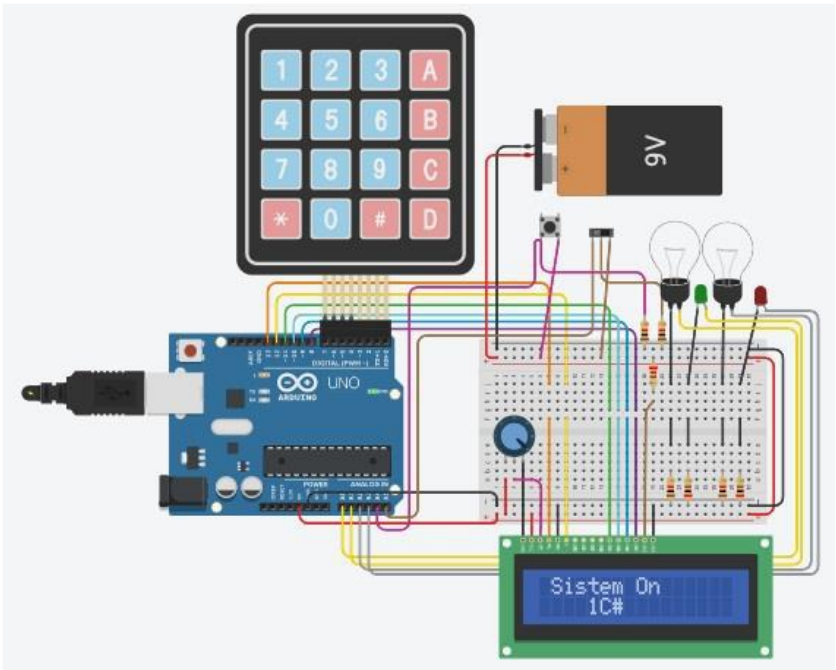

Рисунок 3.11 – Перевірте роботу клавіатури та правильність виведення символів

На рисунку 3.11 показано приклад тестування функціональності клавіатури, правильності відображення символів. Клавіатура передає сигнали про символи, які необхідно відобразити. Це потрібно, щоб допомогти ввести правильний код.

Перевірте роботу системи освітлення в домашньому режимі при активації кнопки (замість датчика руху), як показано на рисунку 3.12.

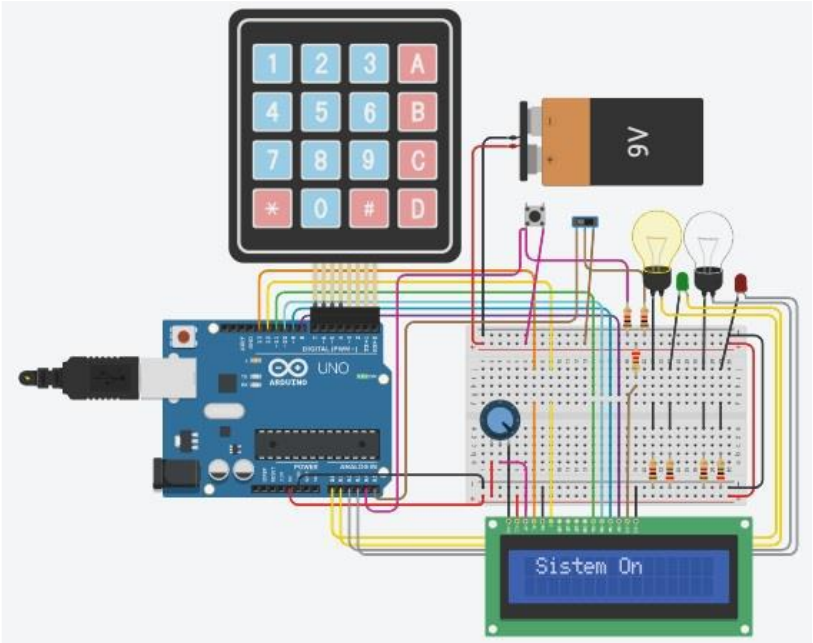

Рисунок 3.12 - Перевірка роботи системи освітлення у побутовому режимі 1

Після отримання сигналу від кнопки система активує перший освітлювальний прилад (у вигляді лампочки). Поки кнопка не натиснута, сигнал не надсилається, і система інтерпретує це як отримання значення 0, тому система не активує освітлювальний прилад.

При натиску на аналоговому порту, налаштованому для отримання сигналу, він отримає значення 1023, що є стандартним максимумом для аналогових портів. Будь-яке значення більше 0 призведе до того, що система негайно активує освітлення 1 у відповідь.

Перевірити роботу системи освітлення в побутовому режимі при активації повзунковим перемикачем (замість сенсорного датчика), як показано на рисунку 3.13.

Принцип дії процесу, перевіреного під час цього випробування, за своїм механізмом не відрізняється від попередніх випробувань. Різниця полягає в тому, що сенсорний датчик, який замінює повзунок, має лише два положення, коли двері закриті та коли двері відкриті. Якщо він досягне активної позиції, система отримає ненульове значення 1023.

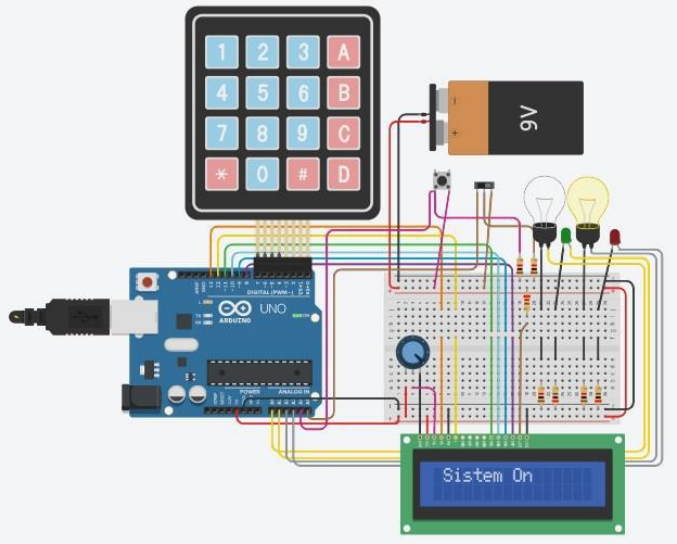

Рисунок 3.13 - Перевірка роботи системи освітлення у побутовому режимі 2

Зараз вмикається другий освітлювальний прилад, незалежний від першого. Перевірте роботу системи освітлення в домашньому режимі при активації кнопкою та перемикачем, як показано на рисунку 3.14.

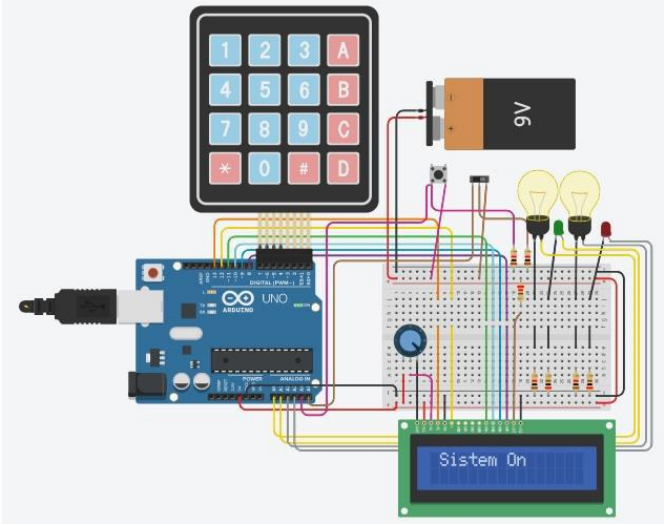

Рисунок 3.14 - Перевірка роботи системи освітлення у побутовому режимі 3

Цей тест перевіряє здатність системи реагувати на два одночасних сигнали від різних датчиків і реагувати відповідно. При отриманні сигналу від вимикача система активує освітлення так само, як і в іншому випадку.

На рисунку 3.15 показано правильний вихід для перевірки повідомлень про введення коду помилки та активацію сигналізації (діода). При введенні коду помилки система виведе на дисплеї в першому рядку текст «Код помилки», а в другому – «Alarm!»

Це потрібно для оповіщення користувача про неправильний введення пароля та активації сповіщення. Діод також активується, що відображає негайне включення сигналізації. Правильність введення коду можна перевірити лише після того, як усі 4 символи будуть введені та відображені на РКІ.

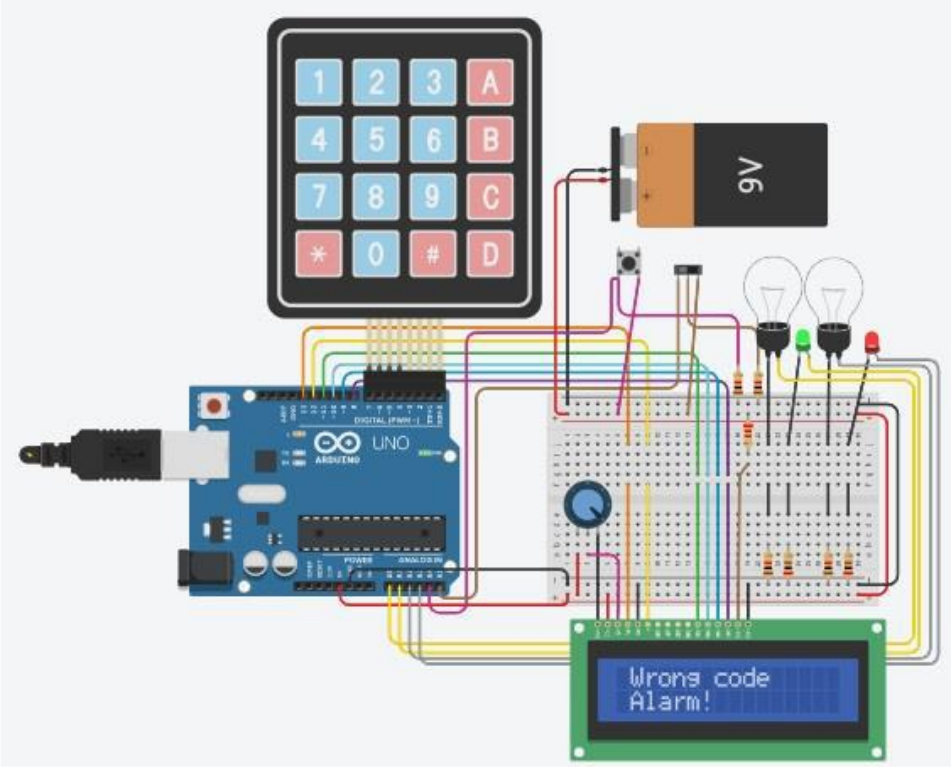

Рисунок 3.15 – Перевірка виходу повідомлення щодо введення коду помилки та активації тривоги (діод)

На рисунку 3.16 показано спрацьовування системи безпеки при активації кнопкою (замість датчика руху).

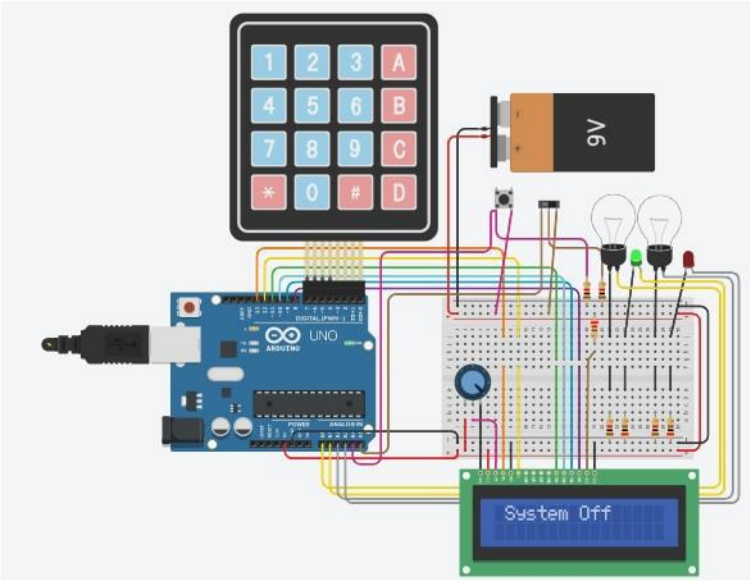

Рисунок 3.16 – Перевірка системи в захищеному режимі 1

Коли система перебуває в режимі охорони, сигнал від кнопки також аналізується системою, але потім система видає команду на включення сигналізації замість освітлення.

Це свідчить про його спрацьовування і виявлення порушення датчиком руху (замість кнопки) в одній з кімнат. Про активацію системи свідчить активація жовтого світлодіода. На рисунку 3.17 показано роботу захисної системи при активації перемикачем (замість контактного датчика).

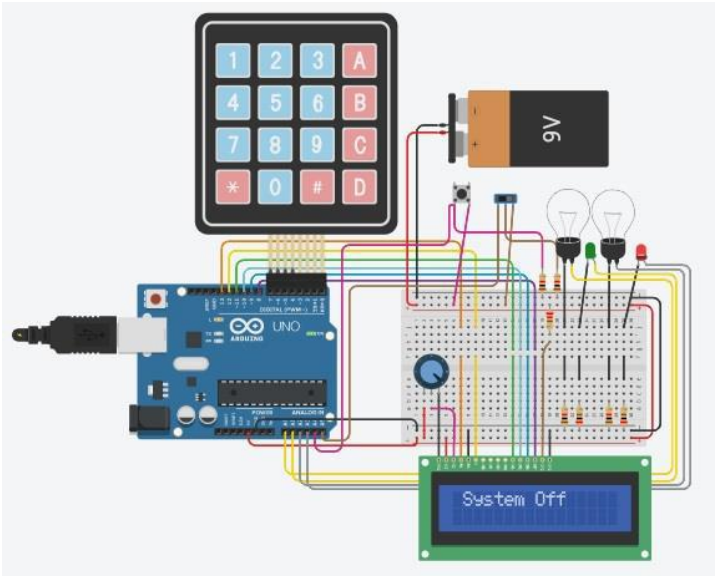

Рисунок 3.17 – Перевірка системи в захищеному режимі 2

У цьому випадку система реагує на сигнал датчика про те, що двері в будинок відкриті. Замість включення освітлення система посилає сигнал на сигналізацію про порушення. Про активацію системи свідчить активація червоного світлодіода.

На рисунку 3.18 показано включення системи безпеки за допомогою двох датчиків. Необхідно перевірити, чи система при спрацьовуванні знаходиться в режимі захисту, щоб перевірити реакцію системи на одночасний прийом сигналів від обох датчиків. Кількість діодів не грає ніякої ролі в системі, крім правильності реакції системи на сигнал, отриманий від певного датчика.

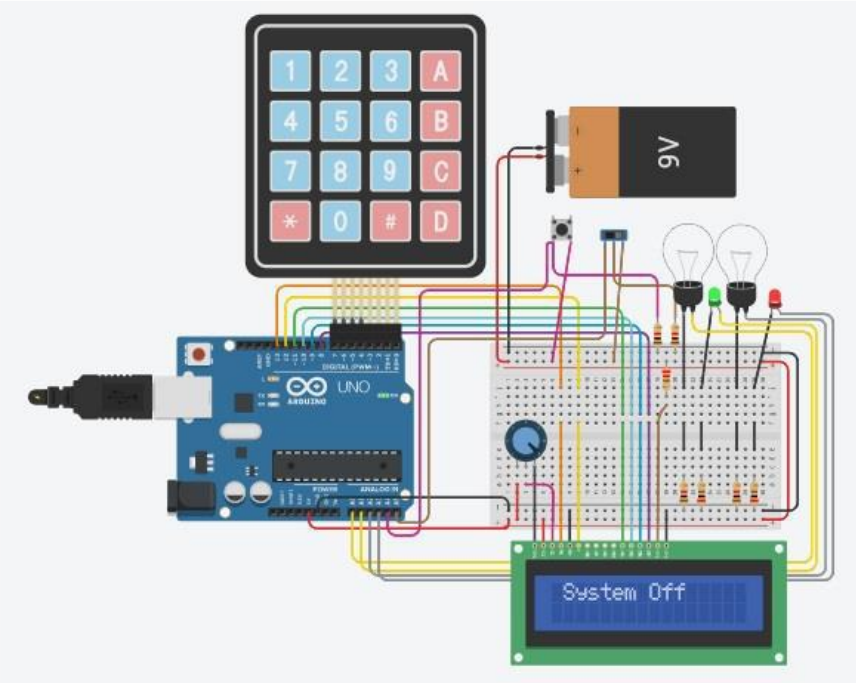

Рисунок 3.18 – Перевірте, чи система перебуває в захищеному режимі під час активації

3.5 Аналіз результатів моделювання

Моделювання показало, що всі системи поводяться відповідно до визначених функцій і реагують на задані дії. Система коректно реагує на зовнішні впливи на датчики і безперебійно змінює стани датчиків [6].

У властивостях системи немає відмінностей від запланованого. Після переведення системи в захищений режим система освітлення більше не залишається включеною, при зміні режиму сигнал частково вимикається. Колізії немає, коли сигнали надходять від двох датчиків одночасно, або система некоректно реагує на цю ситуацію.

Система має багато можливостей для архітектурних і функціональних змін без істотних змін базової моделі. Таким чином датчики можна замінити іншими датчиками з мінімальним впливом на їх функціональність у програмі.

Крім того, чутливість датчика для передачі різних рівнів сигналу можна регулювати залежно від експозиції датчика.

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОХОРОНА ПРАЦІ

4.1 Вплив комп’ютерної техніки на екологію

В дипломній роботі використано різноманітні датчики, у вигляді окремих модулів, поєднаних в системи. Ці системи відносять до комп’ютерної техніки. Деякі з цих систем взаємодіють між собою за допомогою радіозв’язку. Тому в роботі буде описано вплив сучасної комп’ютерної техніки на екологію [7].

Сучасний світ важко уявити без портативних і настільних комп'ютерів, планшетів і смартфонів. Відповідаючи на питання, що знаходиться у них всередині, користувачі найчастіше називають жорсткий диск, флешпам'ять, оперативну пам'ять або процесор. Більшість існуючих пристроїв містять хімічні елементи і речовини, що представляють серйозну небезпеку для людей і навколишнього середовища.

При роботі комп'ютер утворює навколо себе електростатичне поле, яке деіонізує навколишнє середовище, а при нагріванні плати і корпусу монітору випускають в повітря шкідливі речовини. Все це робить повітря дуже сухим, слабко іонізованим, зі специфічним запахом і в загальному «важким» для дихання.

Природно, що таке повітря не може бути корисним для організму і може привести до захворювань алергічного характеру, хвороб органів дихання і інших розладів. Комп’ютер, смартфон, телевізор та інші технічні іграшки, напевно, містять берилій, кадмій, миш'як, полівінілхлорид, ртуть, свинець, фталати, вогнезахисні склади на основі брому і рідкоземельні мінерали.

Але якщо володіти необхідними знаннями про шкідливий вплив цих речовин, то можна заздалегідь вжити необхідних заходів для того, щоб убезпечити свою техніку і себе.

Життєвий цикл продукту: три найбільш небезпечні моменти.

Видобуток. Видобувні виробництва руйнують поверхню Землі і часто забруднюють навколишнє повітря і воду. Видобуток рідкоземельних мінералів

неможливий або нерентабельний без використання процесів, які завдають серйозної шкоди навколишньому середовищу.

Виробництво. Фактично не стикаєтеся з основними компонентами, що знаходяться всередині обладнання. Але деякі люди вступають з ними в прямий контакт. Причому найчастіше це відбувається при високій температурі, внаслідок чого в повітря потрапляють токсичні речовини.

Видобуток рідкоземельних елементів робить смартфони серйозним джерелом забруднення навколишнього середовища.

Полівінілхлорид поширений повсюдно - кабелі, що підключаються до електронних пристроїв, виготовляються з ПВХ і фталатів.

Свинець. Шкідливий вплив цього елемента призводило до виникнення у людей різних захворювань ще з часів стародавнього Риму. У наші дні виробники використовують свинець для пайки електронних схем. Потрапляючи в організм людини, свинець пошкоджує нервову систему і нирки, порушує функціонування репродуктивних органів. Вкрай негативний вплив він робить на дітей, у яких починає сповільнюватися мозковий розвиток.

Ртуть. Компактні флуоресцентні лампи, помітно скорочують енергоспоживання і викид парникових газів, стали справжнім символом екологічно чистих технологій. Але в таких лампах міститься ртуть, і якщо вони розбиваються, навколишні піддаються серйозному ризику. Не менш небезпечні і флуоресцентні лампи, які використовуються для підсвічування ЖК-екранів.

Велика кількість ртуті, перейнявшись в організм, чинить деструктивний вплив на центральну нервову систему, систему травлення та нирки. На щастя, зараз все більше і більше рідкокристалічних екранів оснащуються світлодіодним, а не флуоресцентної підсвічуванням. Разом з тим в різних продуктах харчування залишається ще досить велика кількість ртуті, і частина з них цілком може потрапити до вас на стіл.

Миш'як. Цей елемент вже давно асоціюється з отрутами, і історії загадкових отруєнь досить часто пов'язані з миш'яком. Навіть в кількостях,

яким далеко до дози, що викликає миттєву смерть, миш'як може завдати непоправної шкоди. Проникаючи в організм людини, цей елемент, що відноситься до неметалів, послаблює імунну систему і пошкоджує нирки. Крім того, він викликає рак легенів, шкіри та сечового міхура.

Берилій - токсичний, канцерогенний рідкоземельний компонент електронних друкованих плат. Додавши трохи берилію до міді, в результаті вийде сплав, який в 6 разів міцніше чистої міді. Такі властивості роблять його придатним для виготовлення пружин, з'єднувачів і друкованих плат.

Електромагнітне забруднення навколишнього середовища входить до числа найбільш актуальних проблем людства. Кожен день при включенні мікрохвильової печі, розмов по мобільному телефону, працюючи за комп'ютером, не замислюючись про те, що кожне з цих технічних винаходів чинить свій негативний вплив. Сигнали про підвищений рівень забрудненості електромагнітними хвилями можна також отримати без допомоги спеціальної техніки.

Учені припускають, що низькочастотні поля, які супроводжуються у метрополітені, провокують загострення серцево-судинних захворювань. Низькочастотні електромагнітні поля можуть також сприяти розвитку жіночого безпліддя. До такого висновку прийшли італійські вчені, що вивчали вплив низькочастотних полів на мишах. Здоровою залишалася лише одна з трьох піддослідних. Однак достеменно невідомо, чи буде вплив полів таким же і на людину.

Досліди на людях поки що не проводяться з етичних міркувань. Потужним генератором шкідливого випромінювання є комп'ютер, за яким багато людей проводять більшу частину свого дня. Випромінювачами в даному випадку є і процесор, і монітор.

Випромінювання останнього значно вищі, особливо його бічні і задні стінки, адже вони не мають спеціального захисного покриття, як у лицьовій частині монітора.

Захистити своє здоров'я в цьому випадку нескладно. Досить виходити на прогулянки і робити перерви в роботі з комп'ютером. Дітям не варто

проводити за комп'ютером більше 2-3 годин без перерви, адже вони особливо піддаються шкідливому впливу. Ще один масовий шкідник - мобільний телефон. При дії цього апарата прийнято виділяти два ефекти: термічний (тобто тепловий) і нетермічний.

Тепловий ефект виявляється, коли електромагнітна енергія поглинається організмом і перетворюється в тепло. Від цього можна спостерігати нагрівання деяких органів, наприклад вуха, від довгої розмови. Але, з огляду на безпосередню близькість телефону до голови, деякі ділянки мозку також нагріваються.

Другий ефект, нетермічний, виявляється в тому, що низькочастотне випромінювання телефону впливає на власну біоелектричну активність головного мозку, що може призвести до порушення його функцій. Для людей, які оточують розмовляючого по мобільному телефону, ніякої шкоди від електромагнітних полів немає. А найпростіший спосіб убезпечити себе і своїх дітей від негативного впливу мобільного телефону - використовувати гарнітуру.

Також не варто користуватися мобільним телефоном без особливої необхідності і розмовляти безперервно більше 3-4 хвилин. Відмовлятися від винаходів, що полегшують життя, звичайно ж, не варто.

4.2 Заходи щодо умов пожежонебезпеки

Пожежна безпека є складовою національної безпеки, що полягає у захищеності життя та здоров'я людей, майна та інших цінностей фізичних і юридичних осіб, національного багатства і навколишнього природного середовища, за якої забезпечуються своєчасне попередження, виявлення, припинення і нейтралізація пожеж та їх наслідків.

Аналітичні дослідження показали, що система пожежної безпеки в сучасних будівлях - це складна автоматизована мережа оповіщення, гасіння та запобігання загоряння. Невід'ємною частиною даної системи є нормативні документи, що передбачають інструктаж персоналу і клієнтів закладу, а також

заходи, спрямовані на попередження надзвичайних ситуацій і порядок дій при їх виникненні.

Основним методом вирішення даних завдань у сучасних приміщеннях стає встановлення автоматизованих протипожежних систем, що є частиною загальної системи безпеки комплексу.

Системи протипожежного захисту включають:

— засоби пожежогасіння, у тому числі пожежну техніку;

— автоматичні установки пожежної сигналізації та пожежогасіння;

— використання будівельних матеріалів з нормованими показниками пожежної безпеки; застосування вогнезахисних фарб;

— пристроїв обмеження розповсюдження загоряння;

— систем оповіщення та евакуації людей;

— індивідуальні засоби захисту від шкідливих факторів загоряння;

— засоби колективного захисту; системи димовидалення.

Для забезпечення ефективності роботи протипожежної системи необхідне виконання заходів з пожежної безпеки на базі сучасних наукових розробок.

Система «Розумний дім» (Smart House) - це інтелектуальна система управління, яка забезпечує узгоджену і автоматичну роботу всіх інженерних мереж будинку. Така система грамотно розподіляє ресурси, знижує експлуатаційні витрати і забезпечує зрозумілий інтерфейс контролю і управління.

Сучасний «Розумний дім» - це надійна автоматизована система, що є не лише управління освітленням, приводами і аудіо/відео сигналами, а й засобами охоронно-пожежної сигналізації, систем контролю доступу і навіть систем локалізації протікань води з подальшим перекриванням клапанів.

Система «Розумний дім» забезпечить жителям будинку необхідний комфорт, а будинку - додаткові засоби пожежної безпеки. При цьому важливо, щоб пристрої пожежної сигналізації, інстальовані в «розумний дім», були максимально взаємопов'язані з усіма паралельними системами автоматизації,

адже тільки в цьому випадку можна побудувати якісну систему оповіщення при пожежі.

На даному етапі технічного розвитку складових пожежної безпеки впроваджують більш динамічну систему оповіщення про пожежу. Тим більше, що при зміні інтер'єрів пожежна сигналізація, як правило, встановлюється заново, це відбувається в рамках косметичного ремонту.

Серед технічних новинок в області протипожежного захисту пожежний датчик оптичний і тепловий. Такий датчик фіксує ознаки тління (горіння) на самій початковій стадії, коли ще не росте температура і практично немає диму.

Звичайні теплові та димові датчики в цьому випадку не спрацюють. Даний сигнал може бути також використаний для зміни режиму систем, що відповідають за якість повітря в номері або громадської зони.

Забезпечення пожежної безпеки базується на сукупності правових, економічних, технічних та інших заходів, які здійснюються державними та громадськими органами (організаціями), а також окремими особами під час виконання чи забезпечення виконання правил пожежної безпеки, згідно «Правил пожежної безпеки в Україні» (від 30.12.2014 р. №1417).

ВИСНОВКИ

В даний час системи безпеки розумного будинку дуже популярні і різноманітні. Рівень інтеграції з іншими системами комплексу може досягати досить високих рівнів без шкоди для функціональності. Розвиток і вдосконалення систем сенсорного виявлення значно збільшило різноманітність систем безпеки, збільшило їх модульність і збільшило кількість ситуацій, в яких вони можуть використовуватися.

В цьому випадку різні системи забезпечують методику вторгнення сайтів, а також різні способи сповіщення. Це забезпечує незмінну актуальність робіт у сфері вдосконалення та розвитку системи безпеки «розумного будинку».

Під час проведення сертифікаційних робіт враховуються системи безпеки, їх розвиток і сучасні тенденції. Розглянуті датчики використовуються в системі безпеки комплексу «розумний дім». Визначено найбільш часто використовувані системи безпеки та їх функції. Розглянуто та проаналізовано характеристики систем безпеки «розумний дім» з різними рівнями інтеграції, виділено їх основні переваги та недоліки.

Вибрані мікроконтролери та компоненти для систем безпеки, що розробляються. Для реалізації проекту була обрана платформа Arduino, а сам мікроконтролер Arduino Uno R-3 найкраще підходить для реалізації поставленого завдання під час розробки.

Побудовано охоронну систему «розумний дім» з інтеграцією датчиків інших систем та визначено функціональність системи в її рамках. Розробив рішення системи безпеки розумного будинку. Мова програмування Arduino C була обрана з онлайн-сервісу Tinkercad. Розроблено системне програмне забезпечення.

Проведено моделювання розробленої системи безпеки «розумний дім» у різних режимах роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://stb.sumy.ua/neruxomist/rozumnij-budinok-primxa-bagatix-chi-neobxidnist-dlya-yakisnogo-zhittya.html
2. Петін В.А. Практична енциклопедія Arduino / В. А. Петін, А. А. Біняковський. – Москва: ДМК Прес, 2020. –- 166 с.
3. Крамчанинов С.С., Черкесова Л.В. Розробка системи автоматизації будинку (Розумний будинок) / С.С. Крамчанинов, Л.В. Черкесова // Молодий дослідник Дона.– №6. – 2017. – С. 57-62.
4. Arduino Playground [Електронний ресурс]. Режим доступу https://playground.arduino.cc/
5. Forum Arduino [Електронний ресурс]. Режим доступу https://forum.arduino.cc/
6. Мельничук Р.А., Ларченко Л.В. Системи безпеки розумного будинку. / Р.А. Мельничук, Л.В. Ларченко // CXIII Міжнародна інтернетконференція «Розвиток науки та техніки під час воєнного стану». – м. Херсон, 28 листопада, 2022.– С. 156-158.
7. Види датчиків руху [Електронний ресурс]. Режим доступу https://oxorona.com/motion-sensor-types/

ДОДАТОК А. Лістинг коду

```
1    void loop ()
2         {
3    lcd.setCursor(1, 0);
4    lcd.print("Sistem On");
5    if (analogRead(A4) > 0)    {
6    digitalWrite(A0, HIGH);
7    }
8
9    else   {
10   digitalWrite(A0, LOW);
11   }
12   if (analogRead(A5) > 0)   {
13   digitalWrite(A2, HIGH);
14   }
15   else    {
16   digitalWrite(A2, LOW);
17   }
18   delay(10);
19
20   key = keypad.getKey();
     21
22   if (key){
23   button_pressed[k] = key;
24   k = k+1;
25   lcd.setCursor(3+k, 1);
26   lcd.print(key);
27   if(k == NUM_KEYS){
28
29   for(uint8_t i = 0; i<NUM_KEYS; i++){
30        if(button_pressed[i] == myarray[i]){
31           s = s+1;
32   }
33   }
34   if(s == NUM_KEYS)  {
35   lcd.clear();
```

```
36   lcd.setCursor(1, 0);
37   digitalWrite(A0, LOW);
38   digitalWrite(A2, LOW);
39   lcd.print("System Off");
40      if (analogRead(A4) > 0)    {
41   digitalWrite(A1, HIGH);
42   }
43   else   {
44   digitalWrite(A1, LOW);
45   }
46   if (analogRead(A5) > 0)    {
47   digitalWrite(A3, HIGH);
48   }
49   else    {
50   digitalWrite(A3, LOW);
51   }
52   delay(10000);
53   digitalWrite(A1, LOW);
54   digitalWrite(A3, LOW);
55   lcd.clear();
56      k=0;
57      s=0;
58   }
59   else {
60   lcd.clear();
61   lcd.setCursor(1, 0);
62   lcd.print("Wrong code");
63   lcd.setCursor(1, 1);
64   lcd.print("Alarm!");
65   digitalWrite(A1, HIGH);
66   digitalWrite(A3, HIGH);
67   delay(1000);
68   digitalWrite(A1, LOW);
69   digitalWrite(A3, LOW);
70   lcd.clear();
71   k=0;
72   s=0;
73   }}}}
```