Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології
Спеціальність 123 –Комп'ютерна інженерія

на тему Метод та програмно-технічні засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок»

КвРКІ. 180162.20.16.02 ПЗ

Виконав: студент 2 курсу, група КІ2м-20-1 _____ Ковтонюк І.П
Підпис Ініціали, прізвище

Керівник доктор техн.наук, професор _____ Говорущенко.Т.О
Науковий ступінь, вчене звання Підпис Ініціали, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н., проф.
Т.О. Говорущенко
12 05 2022 р.

Хмельницький, 2022

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прий
Нормоконтроль	Лисенко С.М., професор кафедри КІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІС		

7. Дата видачі завдання «_06_»_____09_____2021 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Прим
1	Вибір напряму дослідження та узгодження тематики ДРМ з керівником	06.09.2021	викон
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	06.10.2021	викон
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	05.11.2021	викон
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	06.12.2021	викон
5	Робота над тезами доповіді	01.02.2022	викон
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2022	викон
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	04.04.2022	викон
8	Оформлення пояснювальної записки згідно вимог	18.04.2022	викон
9	Попередній захист ДРМ	28.04.2022	вик
10	Захист ДРМ на засіданні ЕК	До 15.05.2022	

Студент _____ Ковтонюк І.П.
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Говорущенко Т.О.
Підпис Ініціали, прізвище

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень магістр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма освітньо-наукова програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"01" 09 2021 р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ)

Ковтонюку Івану Петровичу

Прізвище, ім'я, по батькові студента

Тема проекту (роботи) Метод та програмно-технічні засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок»

Керівник проекту (роботи) Говорущенко Т.О., д.т.н., професор

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 06.01.2022 р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 03.05.2022 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих моделей ,методів та засобів

Моделі та методи для вирішення задачі

Алгоритми та технології для вирішення задачі

Реалізація програмного забезпечення для вирішення задачі

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

РЕФЕРАТ

Тема дипломної роботи: Метод та програмно-технічні засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

Автор роботи: Ковтонюк І.П., студент групи КІ2м-20-1.

Керівник роботи: Говорущенко Т.О., доктор технічних наук, професор, завдіувач кафедри комп'ютерної інженерії та інформаційних систем.

Пояснювальна записка: 92 с., 46 Рисунків, 14 табл., 3 дод., 50 джерел.

РОЗУМНИЙ БУДИНОК, ДАТЧИК, ARDUINO,СИСТЕМА ,ВОДА , ЗАХИСТ ,НАДІЙНІСТЬ.ГАЗ.

Об'єктом дослідження є процес контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

Предметом дослідження є метод та засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

Метою кваліфікаційної роботи є підвищення ефективності контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

Для розв'язання поставлених задач використовуються основні положення загальної теорії систем, системного аналізу (ієрархічності, декомпозиції та ін.), теорії моделювання процесів. Внаслідок проведення моделювання процесу та розроблення методів контролю витоку води і газу використано теоретико-множинні підходи, алгебру систем, апарат модельно-орієнтованих підходів, методи концептуального моделювання, принципи побудови баз знань та формування логічного висновку, евристичні оцінки.

Наукова новизна отриманих результатів:

1) вперше розроблено метод контролю витоку води і газу в кіберфізичній системі «Розумний будинок» для підвищення захищеності ІТ-систем «Розумного будинку» із застосуванням натурного моделювання для перевірки працездатності пропонованих рішень щодо захисту «Розумного будинку».

Практична значущість отриманих результатів полягає у:

1) розробленні програмно-технічного засобу контролю витоку води і газу в кіберфізичній системі «Розумний будинок» з використанням Arduino в якості апаратно-програмної платформи проектованої системи.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ПЗ – програмне забезпечення

СПЗ – сервіс програмного забезпечення

CS – референса реалізація системи (CleanSlate)

XP – екстремальне програмування (eXtreme Programming)

RAD – швидка розробка додатків (Rapid Application Development)

RUP – раціональний уніфікований процес (Rational Unified Process)

UI – графічний інтерфейс (User Interface)

RPC – віддалений виклик процедур (Remote Procedure Call)

AMQP – протокол черги повідомлень (Advanced Message Queueing Protocol)

АРМ – автоматизоване робоче місце

IoC – інверсія контролю (Inversion of Control)

EF – засіб для відображення реляційних даних у об’єкти (Entity Framework)

НФ – нормальна форма

TDD – розробка через тестування (Test-Driven Development)

ВСТУП

Актуальність роботи обумовлена повсюдним розвитком інформаційно-технологічної (ІТ) інфраструктури та її застосуванням для забезпечення комфортного проживання громадян у помешканнях багатоквартирного чи індивідуального типу. Використання ІТ-технологій дозволяє створити т.зв. «Розумний будинок», тобто сукупність програмно–апаратних систем, безпосередньо керуючих інженерно–технічними, енергетичними, комунікаційними та іншими підсистемами житлового приміщення. Однак використання ІТ-інфраструктури, зокрема інформаційних систем управління нерозривно пов'язане з вирішенням питань забезпечення безпеки такої інфраструктури.

Практична значимість проблеми забезпечення безпеки «Розумного будинку» полягає в реалізації заходів щодо захисту ІТ–інфраструктури для забезпечення особистої безпеки проживаючих громадян, забезпечення їх здоров'я та необхідних санітарно–гігієнічних умов, захисту майна. Існує проблема, пов'язана з неповним або недостатнім опрацюванням і дослідженням загроз насамперед інформаційної безпеки «Розумного дому» і, відповідно, недостатніми механізмами її протидії. Наприклад, фахівці компанії «BullGuard» у вересні 2016 року [1] виявили одну з найбільших розподілених інформаційних мереж, що використовувалася для DDoS атак (Distributed Denial of Service, розподілена відмова від обслуговування) на провайдерів і великі компанії в галузі телекомунікацій. Більшість пристроїв, що використовувалися, виявилися скомпрометованими «розумними» пристроями, такими як IP-камери та цифрові відеомагнітофони. Тому очевидна актуальність роботи, пов'язана з дослідженням питань в області захисту інформації пристроїв «Розумного будинку».

Об'єктом дослідження є процес контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

Предметом дослідження є метод та засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

Метою дослідження є підвищення ефективності контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

Для досягнення мети необхідно вирішити наступні завдання дослідження:

1) вивчити основні характеристики і виявити основні уразливості ключових систем «Розумного будинку»;

2) провести оцінку ризиків інформаційної безпеки «Розумного будинку» і виробити заходи захисту для їх зниження;

3) розробити і виконати прототип фрагмента системи «Розумний будинок»;

4) оцінити вразливість і захищеність системи «Розумного будинку» за допомогою експериментального дослідження функціонування розробленого прототипу фрагмента системи «розумний будинок».

Наукова новизна отриманих результатів:

1) вперше розроблено метод контролю витоку води і газу в кіберфізичній системі «Розумний будинок» для підвищення захищеності ІТ-систем «Розумного будинку» із застосуванням натурного моделювання для перевірки працездатності пропонованих рішень щодо захисту «Розумного будинку».

Практична значущість отриманих результатів полягає у:

1) розробленні програмно-технічного засобу контролю витоку води і газу в кіберфізичній системі «Розумний будинок» з використанням Arduino в якості апаратно-програмної платформи проектованої системи.

Методи дослідження. Для розв’язання поставлених задач використовуються основні положення загальної теорії систем, системного аналізу (ієрархічності, декомпозиції та ін.), теорії моделювання процесів. Внаслідок проведення моделювання процесу та розроблення методів контролю витоку води і газу використано теоретико-множинні підходи, алгебру систем, апарат модельно-орієнтованих підходів, методи концептуального моделювання,

принципи побудови баз знань та формування логічного висновку, евристичні оцінки.

За темою дипломної роботи опубліковано 1 тези доповіді та взято участь у Всеукраїнській науково-практичній конференції «Актуальні проблеми комп’ютерних наук», що проходила 15-16 жовтня 2021 р. в Хмельницькому національному університеті:

1) Рей К., Ковтонюк І., Грищук І. Дослідження методів керування ресурсами кіберфізичної системи «Розумний будинок». Збірник наукових праць за матеріалами Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук» АПКН–2021 (Хмельницький, 15-16 жовтня 2021). С. 191-193.

1 АНАЛІЗ ВІДОМИХ МОДЕЛЕЙ, МЕТОДІВ ТА ЗАСОБІВ

1.1 Основні положення щодо організації системи «Розумного дому»

На сьогоднішній день великого поширення набувають системи автоматизованого управління характеристиками систем життєзабезпечення і комфортного проживання для наступних об'єктів:

- житлового (індивідуального) будинку;

- житлового приміщення або квартири в багатоквартирному житловому будинку;

- комплексу приміщень у будівлі, не призначеному для проживання, включаючи офісні центри, установи, лікувальні заклади, будівлі органів влади та управління, об'єкти соціально-культурного призначення, торговельні заклади та комплекси [2].

Розглянута система або системи автоматизованого управління в цілому дозволяють створити систему під умовним позначенням «Розумний будинок» (smart home).

Як об'єкт захисту "Розумний будинок" являє собою житлове або нежитлове (приміщення що не використовується для проживання) приміщення, оснащене засобами обчислювальної техніки та управління, що підтримують інформаційні технології, які здатні активно діяти з метою задоволення потреби користувача в комфортному і безпечному проживанні.

Зазначений комплекс засобів обчислювальної техніки, управління (у вигляді виконавчих реле, актуаторів) здатний реагувати на мінливі потреби людини, шляхом створення і підтримки нормативних санітарно–гігієнічних умов для повсякденної діяльності людини, а також забезпечення особистої безпеки, зниження ризику нанесення шкоди здоров'ю громадян та їх майну. Таким чином, мета управління в рамках «Розумного будинку» - забезпечення комфортних і безпечних умов проживання або життєдіяльності, що досягається за допомогою автоматизованого управління системами життєзабезпечення

всередині будинку/житлового приміщення, в тому числі шляхом комунікації з навколишнім середовищем за допомогою інфокомунікацій.

Застосування комплексу засобів автоматизації та інформаційних технологій «Розумного будинку» дозволяє забезпечити безпечну і ефективну експлуатацію, запобігти ризику нанесення шкоди, що приводить до відмови або аварії обладнання інженерних комунікацій, систем енергозабезпечення, газопостачання, вентиляції, опалення, холодного і гарячого водопостачання, водовідведення, систем зв'язку, охоронних та інших систем будівель, і споруд.

Як уже зазначалося, під терміном "Розумний будинок" мають на увазі приміщення в офісних і житлових будівлях, будинках, квартирах з єдиною автоматизованою системою управління і моніторингу всіх підсистем життєзабезпечення і безпеки [3].

Більш детальний список підсистем, контрольованих і керованих в рамках "Розумного будинку", виглядає наступним чином:

- управління опаленням і гарячим водопостачанням;
- управління холодним водопостачанням і контроль протікання трубопроводів;
- управління освітленням;
- управління електричними мережами для подачі електроенергії та вторинними джерелами електроживлення;
- управління медичними системами життєзабезпечення (в разі їх установки в будинку);
- домашній кінотеатр і системи аудіо-та відеорозваг;
- система супутникового та/або ефірного та/або кабельного телебачення;
- система інтернет-доступу (локальна обчислювальна мережа) обладнання доступу;
- система телефонного зв'язку, включаючи бездротові телефони DECT і радіотелефонні трубки;
- система охоронно-пожежної сигналізації;
- система відеоспостереження;

- система контролю та управління доступом в приміщення;

- система кондиціонування та вентиляції;

- системи інженерної безпеки та захисту від перевантажень;

- віддалене управління «Розумним будинком»;

- управління прибудинковою інфраструктурою (освітлення, датчики контролю периметра будівлі/ділянки, дистанційне керування воротами в гараж або в'їзними воротами) [4].

У той же час можна зустріти використання терміна «Інтелектуальна будівля» (intellectual building), який вживається, коли мова йде про комплексну автоматизацію управління будівлями, не призначеними для проживання або багатоквартирних житлових будинків.

Таким чином, термін «Розумний будинок» тут і далі буде вживатися перш за все щодо житлових (індивідуальних) будинків, квартир в багатоквартирному будинку або для ізольованих приміщень в будівлях, не призначених для проживання, які не входять в контур управління «інтелектуальною будівлею».

За способом організації та побудови систем «Розумний будинок» можна виділити два способи або підходи [5]:

- централізований спосіб;

- децентралізований спосіб.

Система "Розумний будинок", побудована за централізованим способом, складається з елемента управління, центрального контролера і керованого обладнання, об'єднаних в єдину телекомунікаційну мережу для прийому і передачі сигналів або команд управління (Рисунок 1.1) [6].

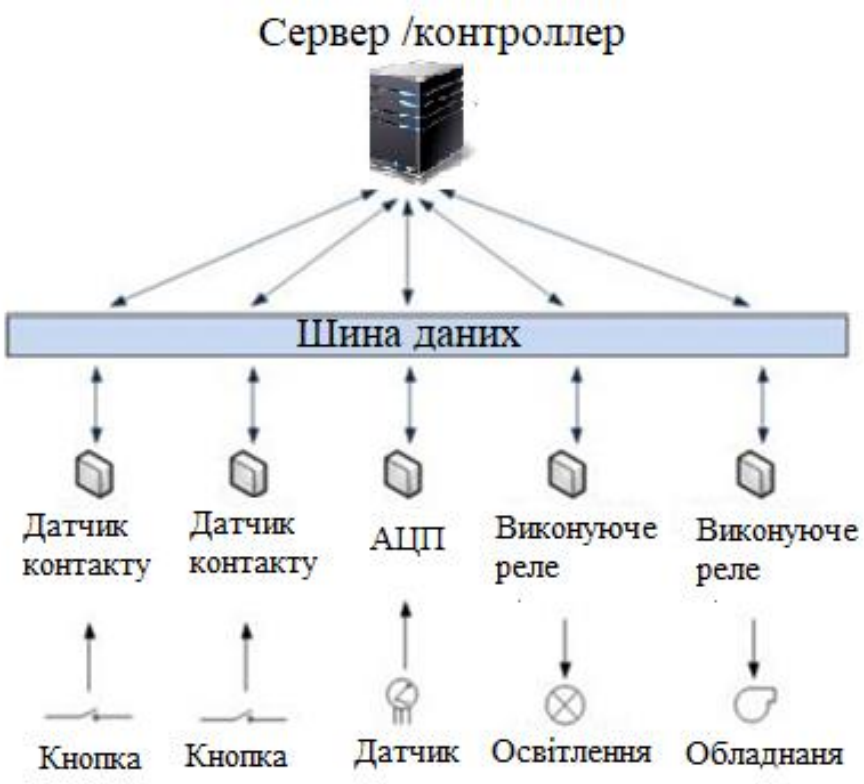


Рисунок 1.1 – Схема централізованої системи "Розумного будинку" з головним комп'ютером

Елемент управління - це обчислювальний або командний пристрій (пульт), за допомогою якого можна передати виконавчу команду системі «розумного будинку». Елементом управління може бути пульт управління, touch-панелі, смартфони і різні датчики (освітленості, присутності, температури, вологості і т.д.).

Центральний контролер управляє системою в цілому і кожним окремим елементом. Це обчислювальний пристрій, який зберігає в пам'яті і виконує всі команди від користувача або по виконуваній програмі. До керованого обладнання "Розумного будинку" в цілому відносяться всі побутові прилади і домашня техніка, починаючи від електролампочки і закінчуючи складними системами охорони і контролю складу повітря[7].

Децентралізований підхід передбачає розгортання системи з розподіленою логікою виконання команд. На відміну від централізованого підходу, в децентралізованому підході відсутній центральний контролер. У

цьому випадку система складається з датчиків, сенсорів і активаторів (Рисунок 1.2) [6]. Датчики виявляють зміну будь-яких характеристик в будинку, руху або зміни заданих в програмі параметрів, і реагують на ці зміни командою виконуючих пристроїв, які включаються активаторами.

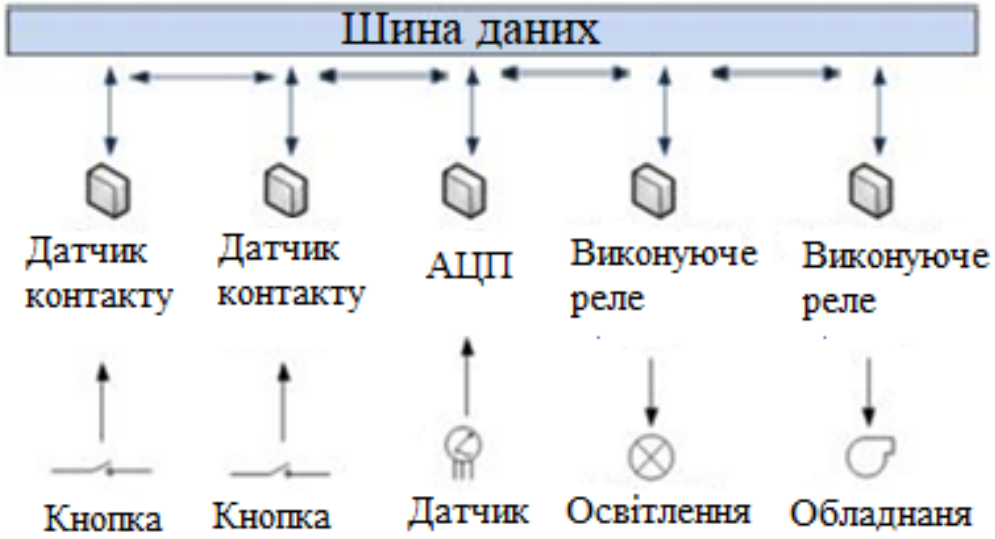


Рисунок 1.2 – Схема децентралізованої системи "Розумного будинку" без керуючого контролера

1.2 Дослідження характеристик основних підсистем «Розумного будинку»

Як вже говорилося раніше, до основних підсистем «Розумного будинку» відносяться системи: освітлення, клімат-контролю, безпеки та моніторингу, комунікаційних мереж і мультимедіа (рис 1.3). Для визначення та аналізу загроз інформаційній безпеці потрібно визначити характерні особливості підсистем «Розумного дому» [7].

Рисунок 1.4 – Основні системи «Розумного будинку»

Розглянемо кожну з цих підсистем докладніше.

Підсистема освітлення (Lighting control systems, LCS), об'єднує всі освітлювальні прилади в приміщенні і на прилеглій території в єдину мережу. Це забезпечує контроль над процесом їх взаємодії і гарантує значну економію енергоресурсів.

Можливості підсистеми освітлення "Розумного будинку" великі, в їх число входить:

- економія енергоресурсів, коли "Розумний будинок", завдяки інтелектуальному автоматичному управлінню освітленням дозволяє значно збільшити термін служби електроламп і знизити використання електроенергії;

- дистанційний і централізований контроль над освітленням, коли включення і відключення всіх освітлювальних приладів в системі "Розумний будинок" може здійснюватися за сигналом, що відправляється з одного автоматизованого пристрою, використовуючи які можна безпосередньо біля виходу з дому відключити світло у всіх кімнатах;

- регулювання яскравості світіння ламп, коли в «Розумному будинку» автоматизовані освітлювальні прилади, як правило, оснащуються дим мерами.

"Розумний будинок" з системою диммерування дозволяє робити світло більш яскравим, коли це необхідно, або приглушеним, коли не потрібно, щоб лампи працювали на повну потужність;

- автоматична робота, коли «Розумний будинок» виходячи з тих даних, які надходять з датчиків присутності, руху і освітленості, або в залежності від часу доби автоматично регулює освітлення в будинку (включення вуличних світильників відбувається у вечірній час, а поступове зменшення їх яскравості до повного відключення – рано вранці, включення/вимикання освітлення за фактом наявності/відсутності людей в приміщенні) [8].

Підсистема клімат-контролю, де реалізація цієї системи досягається шляхом інтеграції та узгодження роботи трьох кліматичних систем – опалення, вентиляції та кондиціонування (Heating, Ventilation and Air Conditioning, HVAC). Підсистема забезпечує підтримку температури, вологості і надходження свіжого повітря в приміщеннях в заданих межах, спираючись на показання датчиків, контрольно-вимірювальних приладів і обладнання.

Також можлива настройка зонального Еко-клімату для різних кімнат житлового будинку. У кожному приміщенні "Ррозумного будинку" може бути заданий власний режим життєзабезпечення, згідно з наступними припущеннями (для зимового періоду):

- на кухні досить нагрівати повітря до + 19 °С, але при цьому вентиляція повинна працювати більш інтенсивно, ніж у вітальні або спальні.

- нормальний сон при +25 °С некомфортний, тому вночі в спальних приміщеннях краще знизити температуру повітря до 18 °С;

- у передпокої, в коридорах і на сходових майданчиках мешканці зазвичай надовго не затримуються, тому з метою економії енергії, піднімати там температуру вище +17, +18 °С нераціонально;

- у підсобних приміщеннях, таких як гараж і бойлерна, комора досить підтримувати плюсову температуру на рівні +7...+9 градусів[9].

Підсистему безпеки і моніторингу умовно можна розділити на наступні підсистеми:

- система відеоспостереження пропонує здійснення візуального контролю за внутрішніми приміщеннями житла та / або дворовою територією. Алгоритм включення камер може бути різним: безперервна робота або реакція на рух (при спрацьовуванні відповідного датчика - автоматично включати запис і сповіщати тривожним сигналом). Також зображення з відеокамер можна переглядати віддалено через Інтернет;

- система контроль доступу та охорони периметра покликана обмежувати і реєструвати людей, що входять в приміщення і/або на вашу ділянку, за рахунок встановлених датчиків (руху, розбиття скла і т. п.) і відеоспостереження;

- система охоронно-пожежної сигналізації (ОПС) призначена для цілодобового контролю об'єкту, що охороняється, а зокрема для раннього оповіщення власника про виявлення ознак пожежі або задимлення і включення засобів пожежогасіння;

- система контролю витоків газу і захисту від протікання води - автоматичне блокування газоводопостачання при виявленні протікання;

- GSM / UMTS моніторинг - віддалене інформування про інциденти в будинку (квартирі, офісі, об'єкті) і управління системами «Розумного будинку» через смартфон.

Підсистема комунікаційних мереж, яка заснована на телекомунікаційній мережі, яка є основним елементом, що забезпечує функціонування системи «Розумного будинку». Через неї здійснюється збір інформації з різних датчиків і передача їх головному серверу для обробки (при централізованому підході в побудові «Розумного будинку»). Сервер після обробки інформації передає сигнали управління на виконавчі елементи (датчики перекриття води, включення засобів пожежогасіння, блокування дверей і т.д.) [10].

Така телекомунікаційна мережа може бути побудована з використанням як дротових, так і бездротових каналів зв'язку. Для бездротового зв'язку застосовуються технології Wi-Fi, Bluetooth, LTE, що є основою для таких протоколів передачі інформації як ZigBee, WirelessHART, LPWAN і т.п. Серед

дротових технологій виділяють Ethernet і PLC рішення (Power line communication) - технологія побудови мереж передачі даних по лініях електропередач [11].

Підсистема розваг (мультимедіа) надає єдиний інтерфейс, за допомогою якого можна управляти різними цифровими пристроями і відтворювати на них фільми, музику, переглядати метеозведення або інший контент. Дану систему можна розділити на 4 підсистеми:

- мультирум - система розподілу аудіо-або відеосигналів (A/V) С різних джерел в безліч зон.

В даному випадку під зонами розуміються не тільки приміщення всередині будинку, але і прилегла територія;

- телебачення - система домашньої автоматизації поширюється також на супутникове і ефірне телебачення, яке в «Розумному будинку» розподіляється за допомогою одного ресивера на всі пристрої відображення;

- медіасервер – сукупність програмного і апаратного забезпечення, яка дозволяє комутувати, зберігати і транслювати медіа контент (аудіозаписи, відеозаписи, зображення) на різні пристрої (телевізори, проектори, акустичні системи і т. д.);

- джерела контенту - це різні цифрові пристрої, які необхідні для відтворення, передачі та зберігання відео та аудіоданих (кіно, музика, телебачення, радіо).

Таким чином, основою системи "Розумний дім" є телекомунікаційна (комп'ютерна) мережа, тому загрози інформаційній безпеці в першу чергу можуть виникати за рахунок вразливостей мережевої структури:

- коди операційної системи (наприклад, вразливість при переповненні пам'яті, управління оновленнями операційної системи);

- транспортні протоколи, наприклад, протокол TCP, DNS, SMTP або ICMP;

- дефекти прикладних програм (firmware, наприклад, Apache);

- помилки в програмах користувача;

- програмне забезпечення, вбудоване в апаратні пристрої, наприклад, в маршрутизатори, BIOS;

- перехоплення повідомлень і управління в бездротових системах[12].

1.3 Аналіз вразливостей і факторів, що впливають на датчики контролю і захисту в системі «Розумний будинок»

Ефективна і багатофункціональна система "Розумного будинку" включає в себе різноманітні датчики, що реєструють і передають параметри середовища, і іншу важливу інформацію. Датчики автоматизації являють собою конструктивно автономний самостійний пристрій, що змінює свій сигнал відповідно відстежуваному параметру .

Ці обов'язкові елементи "Розумного будинку" розрізняються за призначенням і принципом дії, умовно їх можна умовно розділити на дві групи: датчики, що відстежують рух і датчики, що реагують на параметри середовища [13].

Датчики, що відстежують рух, які використовуються в охоронних системах і для побудови інтелектуального освітлення. Такі датчики поділяються на датчики руху і датчики присутності. Датчики присутності відрізняються від датчиків руху тим, що фіксують навіть дуже дрібні рухи, що відбуваються в межах робочої зони датчика, в іншому принцип їх роботи однаковий.

В даний час найбільшого поширення набули наступні види датчиків руху і присутності:

1) інфрачервоні датчики (ІК) (Рисунок 1.5).

Рисунок 1.5 – Приклад загального вигляду інфрачервоного датчика

Принцип роботи інфрачервоних датчиків руху полягає у виявленні змін інфрачервоного (теплового) випромінювання навколишніх об'єктів. Кожен об'єкт має температуру випускає інфрачервоне випромінювання, яке через систему лінз або спеціальних увігнутих сегментованих дзеркал, потрапляє на розташований всередині датчика руху чутливий сенсор, який реєструє це.

Вразливістю даного датчика є т.зв. «сліпа зона», при якій він не зможе фіксувати об'єкти певної висоти. Крім того, датчик має обмеження по діапазону робочих температур, наприклад, тільки в діапазоні від -10 ^{0}C до + 40 ^{0}C;

2) ультразвукові датчики (УЗ) (Рисунок 1.6).

Рисунок 1.6 – Приклад загального вигляду ультразвукового датчика

Принцип роботи ультразвукового датчика руху полягає в дослідженні навколишнього простору за допомогою звукових хвиль, частотою, що знаходиться за межами чутності людським вухом - ультразвуком (в залежності

від виробника і моделі зазвичай генерується частота звукової хвилі 20-60 кГц). При виявленні зміни частоти відбитого сигналу, внаслідок руху об'єктів, датчик запускає закладену в неї функцію, це може бути включення освітлення або розрив сигнальної мережі охоронної системи.

Вразливістю даного датчика є обмежений по відстані діапазон чутливості, наприклад, від 200 мм до 8 м. Якщо об'єкт знаходиться на відстані менше 200 мм, відбуваються помилкові спрацьовування. Якщо кілька датчиків знаходяться в безпосередній близькості, що може зробити їх уразливими для перехресних перешкод, що запобігається спеціальним контролером для включення датчиків по одному;

3) мікрохвильові датчики (СВЧ) (Рисунок 1.7).

Рисунок 1.7 – Приклад загального вигляду мікрохвильового датчика

Мікрохвильовий датчик руху випромінює високочастотні електромагнітні хвилі (частота хвиль може бути різною в залежності від виробника, зазвичай вона становить 5,8 ГГц), які відбиваючись від навколишніх об'єктів, реєструються сенсором і в разі виявлення найменших змін відбитих електромагнітних хвиль, мікропроцесор пристрою приводить в дію закладену в нього функцію.

Вразливістю мікрохвильового датчика є невірне визначення порога чутливості.

Поріг - значення, нижче якого сигнали інтерпретуються як шуми. Поріг регулюється під час налаштування датчика. Чим більше чутливість, тим більша ймовірність виявлення. Але при збільшенні чутливості зростає і частота помилкових тривог, що знижує довіру до системи в цілому. Також поява помилкових тривог може бути викликана недоліками конструктивних і схемотехнічних рішень; неправильною установкою і налаштуванням датчика; недоліками алгоритму обробки сигналів [14].

Недоліки конструктивних і схемотехнічних рішень можуть привести до наведень в ланцюгах передачі даних, наприклад, через погане екранування, погану фільтрацію, застосування дешевої неякісної елементної бази. Типовою проблемою є зміна параметрів електронних компонент при наближенні до меж допустимого температурного діапазону. Для вирішення цієї проблеми доводиться розробляти спеціальні схеми термостабілізації параметрів і т.д. [14].

Неправильна настройка датчика може привести до виходу зони виявлення датчика за межі охоронюваної зони, особливо в приміщеннях зі складною конфігурацією. Це призведе до того, що такий датчик буде спрацьовувати, наприклад, при знаходженні людей в сусідніх приміщеннях.

Уразливість датчика може бути обумовлена збуреннями середовища, в тому числі електромагнітними наведеннями, паралельною роботою декількох датчиків.

Далі розглянемо т. зв. комбіновані датчики, які мають можливість об'єднувати в системі безпеки функції різних методів реєстрації зміни стану навколишнього середовища, розглянуті вище;

4) комбіновані датчики (Рисунок 1.8).

Рисунок 1.8 – Загальний вигляд комбінованого датчика

Комбіновані датчики руху поєднують в собі відразу кілька технологій виявлення рухів, наприклад, інфрачервоний датчик і мікрохвильовий. Це найбільш вдале рішення, якщо потрібно більш точне визначення переміщень в зоні дії датчика.

Також існують магнітноконтактні датчики, що діють при зміні відстані між магнітом і герконом (змикання і розмикання складових частин) і датчики розбиття скла.

За принципом дії датчики пошкодження скла класифікуються:

- електроконтактні датчики - сповіщають про порушення цілісності скляного полотна за допомогою механічного впливу, наприклад, удару або вирізання отвору;

- п'єзоелектричні датчики, які реєструють механічні коливання, що виникають при ударі скла;

- акустичні датчики, що реагують на звукові коливання, що видаються при руйнуванні скла.

Датчики, що реагують на параметри навколишнього середовища. Дані пристрої застосовуються для регулювання роботи інженерних систем і комунікацій будівель. Існує кілька типів даних датчиків:

- датчики температури;

- датчики рівня освітленості;

- датчики витоку газу;

- датчики протікання води;

- протипожежні датчики (датчики задимлення, датчики температури);

- датчики тиску води, газу;

- датчики дощу та атмосферних опадів;

- датчики-індикатори вогкості / вологості;

- комбінований.

Всі типи цих датчиків знімають показання навколишнього середовища і передають інформацію про неї, в систему «Розумного будинку». Перераховані вище датчики можуть передавати цю інформацію по різних каналах зв'язку, як дротовим, так і бездротовим, використовуючи різноманітні протоколи передачі інформації.

В цілому для всіх перерахованих типів датчиків характерні уразливості, пов'язані з обмеженням конструкції датчиків, використовуваними фізичними принципами, невірною установкою.

Уразливості проявляються в зв'язку з впливом наступних факторів:

- електромагнітного випромінювання;

- електричні перешкоди;

- акустичні перешкоди;

- перепади освітленості;

- перепади вологості;

- наявність в повітрі хімічних речовин;

- наявність в повітрі пилу і суспензій;

- екранування поля, випромінюваного активними датчиками і об'єктами в зоні виявлення [15].

Серед перерахованих загроз відсутні в явному вигляді загрози інформаційній безпеці. Проте, захист розглянутих датчиків у зв'язку з виділеними вразливостями необхідний, оскільки загроза імітації помилкових спрацьовувань є закономірним наслідком реалізації розглянутих вразливостей і

являє собою спосіб впровадження в ІТ-систему "Розумного будинку" помилкової або зловмисно–спотвореної інформації.

Внаслідок цього при розробці і впровадженні прикладного і вбудованого програмного забезпечення в рамках ІТ–систем «Розумного будинку» слід передбачити програмні процедури перевірки працездатності і режиму функціонування датчиків і реалізувати механізм верифікації оброблюваних показань згідно з вимогами ГОСТ Р МЕК 61508-3 -2007 «Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою. Частина 3. Вимоги до програмного забезпечення». Відповідно до розглянутого завдання до плану верифікації згідно з п. 7.9.2 ГОСТ Р МЕК 61508-3-2007 потрібно внести положення, що стосуються перевірки достовірності оброблюваних показань для розробленої моделі інформаційної безпеки. Зокрема, згідно п. 7.9.2. 13 ГОСТ Р МЕК 61508-3-2007 структури даних, специфіковані під час проектування, повинні бути перевірені на захист від зміни або пошкодження [16].

Всі параметри ІТ-системи, які пов'язані з обробкою показань датчиків, які можуть бути змінені, повинні бути перевірені на захист:

- від помилкових, несумісних або необґрунтованих значень;
- несанкціонованих змін;
- пошкодження даних.

1.4 Аналіз вразливостей і факторів, що впливають на виконавчі пристрої «Розумного будинку»

Виконавчі пристрої призначені для перетворення керуючих (командних) сигналів в регулюючі впливи на об'єкт управління. Сигнальна сирена, сервоприводи, що перекривають подачу води або газу, відкривають вентиляційні вікна, різні силові реле і таймери - відносяться до виконавчих пристроїв. Розглянемо кілька з цих пристроїв докладніше в контексті аналізу загроз «розумному дому».

Електромагнітні клапани (Рисунок 1.9) встановлюються на трубопроводах подачі води і газу для дистанційного керування відкриттям або закриттям потоку робочого середовища, як правило, рідини.

Рисунок 1.9 – Загальний вигляд електромагнітного клапана «гідролокатор»

Варіанти застосування електромагнітних клапанів:

1) в якості аварійного крана в системі подачі води. В цьому випадку управління здійснюється від датчика, вмонтованого в підлогу і спрацьовує від попадання води;

2) в системі клімат-контролю електронний (електромагнітний) кран буде регулювати подачу гарячої води, в залежності від температури в кімнаті (керуючий сигнал подається від датчика температури в приміщенні);

3) електромагнітний клапан може використовуватися в системі поливу присадибної ділянки. Подача води буде здійснюватися відповідно до встановленого часовим графіком або від сигналу датчика вологості;

4) також існують електромагнітні клапани для установки на трубопроводах подачі газу. Такий клапан, підключений до датчика загазованості, перекриє подачу газу і при аварійній ситуації [17].

Вразливістю є можливість виведення датчика з ладу шляхом зовнішніх електромагнітних випромінювань.

Електромеханічні приводи відкриття / закриття воріт, хвірток, дверей (рис 1.10), вікон, жалюзі і штор і т. п.

Рисунок 1.10 – Загальний вигляд електромагнітного замка компанії Samsung

Робота приводів може здійснюватися за сценарієм, наприклад, вночі-закриття жалюзі і приглушення світла; при постановці на сигналізацію – закриття всіх вікон і дверей, включення датчиків руху.

Вразливістю приводу є недостатній захист від механічних пошкоджень. Також вразливість таких приводів істотно зростає при відключенні напруги електроживлення.

1.5 Аналіз вразливостей і факторів, що впливають на безпеку центральних пристроїв «Розумного будинку»

Центральний пристрій "Розумного будинку" координує всі його функції і управляє всіма його компонентами. В якості обчислювальної платформи центрального пристрою можуть виступати: персональні комп'ютери, ноутбуки, сервера, але найбільш часто використовуються контролери різних типів.

Завдання контролера полягає в зборі інформації про функціонування обладнання, перевірці отриманих параметрів, пошук аварійно-функціонуючих пристроїв і виведення обробленої інформації на панелі управління. Сьогодні на ринку представлена велика кількість контролерів для «Розумного будинку» від різних фірм виробників, нижче розглядаються типові контролери і їх вразливості.

Контролер виробництва фірми AMX NX - 1200 (Рисунок 1.11) створений для вирішення завдань управління і автоматизації невеликих систем «Розумного будинку», цей контролер обладнаний дев'ятьма портами управління для підключення до чотирьох пристроїв у вигляді, наприклад, інфрачервоних датчиків (ІД) і одного послідовного пристрою сторонніх виробників, а також може підтримувати шину типу Ethernet [18].

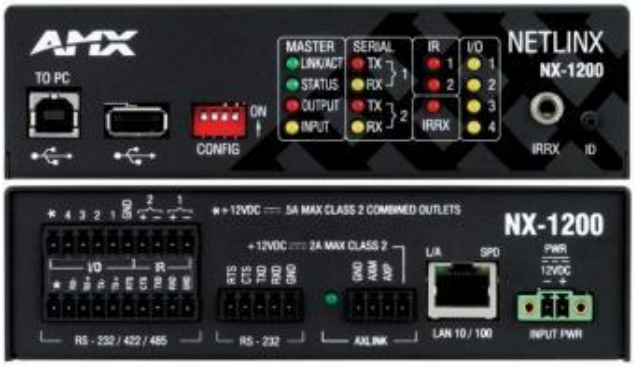


Рисунок 1.11 – Загальний вигляд контролера AMX NX-1200

Уразливість даного контролера була виявлена експериментальним шляхом в ході перевірки процедури аутентифікації: дослідники виявили у внутрішній базі даних користувачів прихований адміністративний обліковий запис, для якого були задані незмінний логін і пароль. Отримавши доступ до цього облікового запису можна отримати контроль над пристроєм, оскільки даний адміністративний акаунт дозволяє отримати доступ до web-консоль управління, а також інтерфейсу командного рядка і здійснювати різні дії, наприклад, перехоплення і підміну трафіку [18].

Інший типовий зразок, контролер фірми X10 MT10[19] (Рисунок 1.12), використовується для управління за часом електропобутовими та освітлювальними приладами в мережі X10[20], підключається по електропроводці.

Рисунок 1.12 – Загальний вигляд контролера X10 MT10

Можливі наступні режими роботи приладу:

- автоматичний режим-контролер включає і вимикає електроприлади за заздалегідь введеною програмою;

- ручний режим – в будь-який момент можливо безпосереднім натисканням кнопок на приладі управляти підключеними електроприладами;

- режим безпеки (імітація присутності господарів в будинку) - автоматичний режим з довільними моментами включення і виключення електроприладів в межах встановленого інтервалу часу.

Контролер вразливий при електромагнітних перешкодах або розриві зовнішньої електропроводки, пропажі електроживлення.

Контролер фірми Honeywell Tuxedo Touch (Рисунок 1.13) забезпечує централізоване управління освітленням, термостатом, замками, камерами, і т.п., використовуючи бездротову технологію Z-Wawe[21].

Рисунок 1.13 – Контролер Honeywell Tuxedo Touch

У контролера є ряд вразливостей, що істотно впливають на безпеку використання, в тому числі обхід аутентифікації користувача і підміна міжсайтових запитів.

Як видно з перерахованих вище прикладів, центральні контролери "Розумного будинку" схильні до різних видів вразливостей, реалізація яких може привести до виведення з ладу фрагмента або всієї системи в цілому.

1.6 Аналіз вразливостей і факторів, що впливають на систему зв'язку «Розумного будинку»

В даний час з усіх представлених на ринку технологій побудови IT-систем «Розумний будинок», можна виділити кілька готових до застосування комплексних систем, які є типовими представниками в своєму класі:

- централізовані, наприклад, системи фірми Creston;
- децентралізовані системи, наприклад, EIB.

Також системи можна класифікувати на:

- провідні, наприклад, X10;
- бездротові, наприклад, Z-Wave.

На прикладі цих комплексних систем розглянемо основні фактори, що впливають на безпеку інформації «Розумного будинку», побудованого на основі готових систем.

Відповідно зазначені фактори поділяються на:

1) за ознакою ставлення до природи виникнення:

- об'єктивні;

- суб'єктивні.

2) по відношенню до об'єкта інформації:

- внутрішні;

- зовнішні.

Система управління будинком фірми Crestron - це централізована система управління. Як правило, вона будується на основі застосування широкого спектру керуючих центральних контролерів і безлічі виконавчо-командних блоків. Керуючі контролери Crestron володіють великим набором вбудованих можливостей, сумісні з безліччю поширених протоколів передачі інформації.

Для даної системи фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 1.1 і табл. 1.2.

Таблиця 1.1 – Об'єктивні фактори, що впливають на безпеку інформації централізованої системи управління «Розумним будинком»

Внутрішні фактори	Зовнішні фактори
Випромінювання акустичних сигналів, супутні технічним засобом (ТЗ) мови	Збої, відмови та аварії систем забезпечення об'єкта інформації (ОІ)
Модуляція паразитного електромагнітного випромінювання інформаційними сигналами	Термічні фактори (пожежі і т. д.)
Дефекти, збої і відмови, аварії ТЗ і систем обробки інформації	Кліматичні фактори (повені і т. д.)

Таблиця 1.2 – Суб'єктивні фактори, що впливають на безпеку інформації централізованої системи управління будинком

Внутрішні фактори	Зовнішні фактори
Розголошення інформації, що захищається особами, які мають до неї право доступу через передачу інформації по відкритих лініях зв'язку	Доступ до інформації, що захищається із застосуванням ТЗ знімання інформації
Несанкціонований доступ до інформації шляхом підключення до технічних засобів і систем ОІ	Несанкціонований доступ до інформації шляхом використання закладних засобів
Використання програмного забезпечення (ПЗ) технічних засобів ОІ через внесення програмних закладок	Блокування доступу до інформації, що захищається шляхом перевантаження ТЗ обробки інформації помилковими заявками на її обробку

Система управління будинком EIB – European Installation Bus - це децентралізована відкрита мережева технологія, підтримана десятками провідних компаній виробників електротехнічної продукції-членів Європейської неурядової організації EIBA (European Installation Bus Association (Рисунок 1.14).

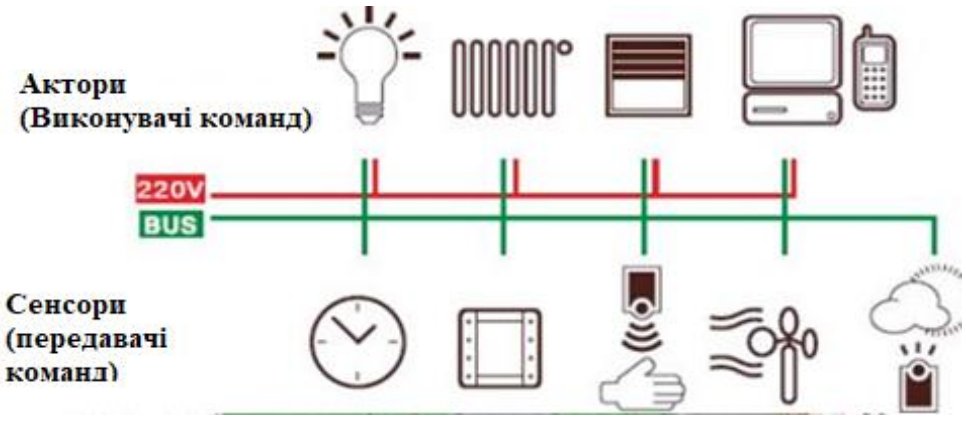


Рисунок 1.14 – Загальна схема підключення системи EIB

Пристрої (передавачі або приймачі) в EIB зв'язуються один з одним безпосередньо, без ієрархії або центрального контролюючого приладу. Компоненти здійснюють передачу послідовно, асинхронно, конфлікти при передачі повідомлень вирішуються розстановкою пріоритетів повідомлень. Призначена для передачі інформація збирається в пакети - "телеграми" і через шину передається приймачу або групі приймачів. Повідомлення отримують всі абоненти, але реагують на нього тільки ті, кому воно адресоване . Сьогодні EIB-протокол підтримує обмін по крученій парі, безпосередньо по силовій лінії, по радіо і по ІЧ-каналу. До децентралізованих систем також відносяться такі готові системи, як Gira, Berker, Bticino, Vimar та ін.[22].

Для систем з децентралізованим управлінням фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 1.3 і табл. 1.4

Таблиця 1.3 – Об'єктивні фактори, що впливають на безпеку інформації децентралізованої системи управління «Розумним будинком»

Внутрішні фактори	Зовнішні фактори
Дефекти, збої і відмови ПО	Збої, відмови та аварії систем забезпечення ОІ
Наведення в лініях зв'язку, викликані побічними електромагнітними випромінюваннями, що несуть інформацію	Термічні фактори (пожежі і т. д.)
Наявність акустоелектричних перетворювачів в Елементах ТЗ ОІ	Кліматичні фактори (повені і т. д.)

Таблиця 1.4 – Суб'єктивні фактори, що впливають на безпеку інформації децентралізованої системи управління «Розумним будинком»

Внутрішні фактори	Зовнішні фактори
Неправомірні дії з боку осіб, які мають право доступу до інформації, що захищається, шляхом	Доступ до інформації, що захищається із застосуванням ТЗ технічної комп'ютерної розвідки

Кінець таблиці 1.4 – Суб'єктивні фактори, що впливають на безпеку інформації децентралізованої системи управління «Розумним будинком»

несанкціонованої зміни інформації	
Недоліки організаційного забезпечення захисту інформації при завданні вимог щодо захисту інформації	Спотворення, знищення або блокування інформації шляхом розкрадання носія інформації
Несанкціонований доступ до інформації шляхом внесення програмних закладок	Спотворення, знищення або блокування інформації шляхом використання програмних або програмно-апаратних засобів при здійсненні мережевої атаки

Стандарт X10 визначає методи і протокол передачі сигналів управління електронними модулями, до яких підключені побутові прилади, з використанням звичайної електропроводки або бездротових каналів.

Мережа X10 включається в себе наступні основні компоненти: передавачі, приймачі, трансивери, пульти ДУ і лінійні компоненти. Системами, що використовують провідні технології побудови системи «Розумний будинок» (зокрема стандарт X10), притаманні фактори, що впливають на безпеку інформації, що захищається, представлені в табл. 1.5 і табл. 1.6.

Таблиця 1.5 – Об'єктивні фактори, що впливають на безпеку інформації дротової системи управління «Розумним будинком»

Внутрішні фактори	Зовнішні фактори
Модуляція паразитного електромагнітного випромінювання інформаційними сигналами	Ненавмисні електромагнітні опромінення ОІ

Кінець таблиці 1.5 – Об'єктивні фактори, що впливають на безпеку інформації дротової системи управління «Розумним будинком»

Наведення в електричних ланцюгах ТЗ викликана побічними електромагнітними випромінюваннями, що несуть інформацію	Електромагнітні фактори (грозові розряди і т. д.)
Наведення в ланцюгах заземлення викликана побічними електромагнітними випромінюваннями, що несуть інформацію	Кліматичні фактори (повені і т. д.)

Таблиця 1.6 – Суб'єктивні фактори, що впливають на безпеку інформації провідної системи управління «Розумним будинком»

Внутрішні фактори	Зовнішні фактори
Розголошення інформації, що захищається особами, які мають до неї право доступу через осіб, які не мають права доступу до інформації, що захищається	Доступ до інформації, що захищається із застосуванням ТЗ радіоелектронної розвідки
Несанкціонований доступ до інформації шляхом порушення функціонування ТЗ обробки інформації	Спотворення, знищення або блокування інформації шляхом навмисного електромагнітного впливу по мережі електроживлення
Помилки користувачів або обслуговуючого персоналу при експлуатації ТЗ	Спотворення, знищення або блокування інформації шляхом навмисного силового впливу фізичної природи

Система управління будинком Z-Wave є запатентованим бездротовим протоколом зв'язку, розробленим для домашньої автоматизації, зокрема для контролю і управління в житлових і комерційних об'єктах. Технологія використовує малопотужні і мініатюрні радіочастотні модулі, які вбудовуються в побутову електроніку і різні пристрої, такі як освітлювальні прилади, прилади

опалення, пристрої контролю доступу, розважальні системи і побутову техніку [23]. Більшість систем використовують бездротові канали зв'язку схильні до факторів, що впливають на безпеку інформації, що захищається, перерахованих в табл. 1.7 і табл. 1.8.

Таблиця 1.7 – Об'єктивні фактори, що впливають на безпеку захищається інформації бездротової системи управління «Розумним будинком»

Внутрішні фактори	Зовнішні фактори
Електромагнітні випромінювання і поля в радіодіапазоні	Ненавмисні електромагнітні опромінення ОІ
Побічні електромагнітні випромінювання на частотах роботи високочастотних генераторів пристроїв, що входять до складу ТЗ ОПІ	Радіаційні опромінення ОІ
Побічні електромагнітні випромінювання на частотах самозбудження підсилювачів пристроїв, що входять до складу ТЗ ОПІ	Природні явища, стихійні лиха

Таблиця 1.8 – Суб'єктивні фактори, що впливають на безпеку інформації бездротової системи управління «Розумним будинком»

Внутрішні фактори	Зовнішні фактори
Несанкціонований доступ до інформації шляхом підключення до ТЗ і систем ОІ	Доступ до інформації, що захищається із застосуванням ТЗ радіоелектронної розвідки
Розголошення інформації, що захищається особам, які не мають до неї право доступу	Доступ до інформації, що захищається, шляхом використання шкідливого ПЗ
Помилки обслуговуючого персоналу при експлуатації ТЗ	Спотворення, знищення або блокування інформації шляхом здійснення мережевої атаки

Таким чином розроблена система суб'єктивних і об'єктивних факторів, що впливають на систему «Розумного будинку». Надалі ця система буде використана для аналізу загроз «розумного будинку».

1.7 Висновки

"У даном розділі проведено аналіз та дослідження технології " Розумний будинок" що являє собою житлове або нежитлове (не використовується для проживання) приміщення, оснащене засобами обчислювальної техніки та управління, що підтримують інформаційні технології, які здатні діяти проактивно з метою задоволення потреби людини в комфортному і безпечному проживанні.

Застосування комплексу засобів автоматизації та інформаційних технологій «Розумного будинку» дозволяє забезпечити безпечну і ефективну експлуатацію, запобігти ризику нанесення шкоди, що приводить до відмови або аварії обладнання інженерних комунікацій, систем енергозабезпечення, газопостачання, вентиляції, опалення, холодного і гарячого водопостачання, водовідведення, систем зв'язку, охоронних та інших систем будівель, і споруд.

В роділі було досліджено найпопулярніші рішення щодо проектування та оптимізація взаємодії компонентів, розглянуто технології такі як Z-Wave та X10 основні фактори, що впливають на безпеку інформації «Розумного будинку», побудованого на основі готових систем, було виявлено переваги та недоліки.

Розглянуто також основні фактори, що впливають на безпеку інформації «Розумного будинку», побудованого на основі готових систем.

Таким чином розроблена система суб'єктивних і об'єктивних факторів, що впливають на систему «Розумного будинку». Надалі ця система буде використана для аналізу загроз «розумного будинку».

2 МОДЕЛІ ТА МЕТОДИ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ

2.1 Розробка структурної схеми

У системах захисту від протікання води і витоків газу ключову роль відіграють виконавчі механізми, які відсікають подачу, відповідно, води або газу. Крім того, якщо системи захисту від даних аварійних ситуацій пов'язані з системою електропостачання будинку, то в разі виникнення аварійної ситуації є можливість відключити подачу електрики на всі побутові прилади в будинку, а системи захисту від протікання води або витоку газу продовжать роботу від вбудованих акумуляторів.

Типовий приклад побудови системи захисту від протікання води представлений на малюнку 2.1.

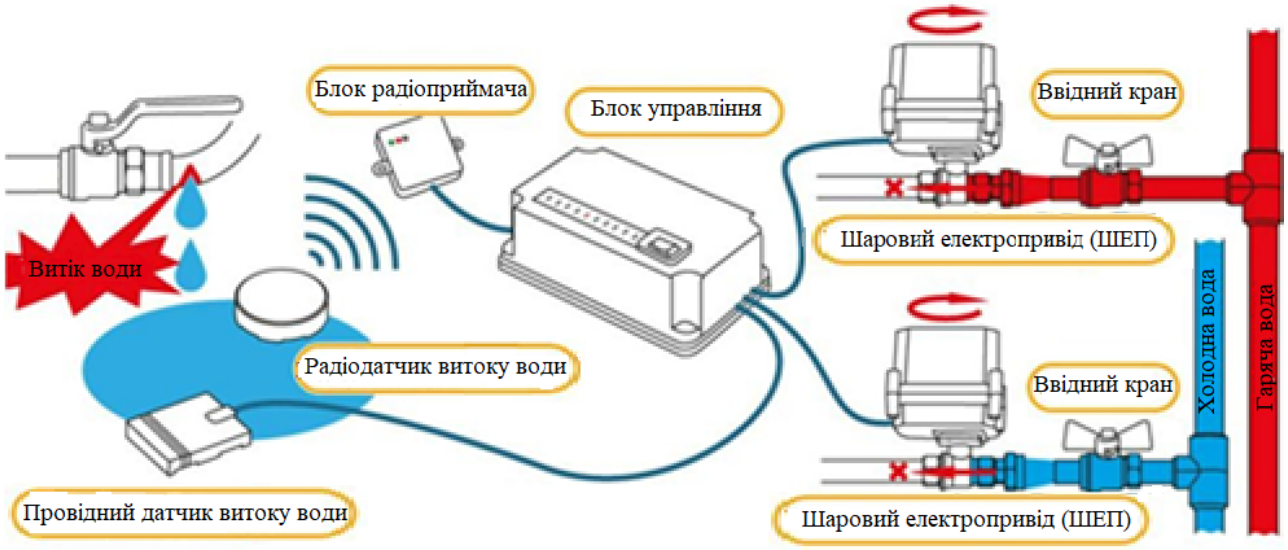


Рисунок 2.1 – Приклад побудови системи захисту від протікання води

Датчик протікання води розміщується в тих приміщеннях і місцях, в яких можливе протікання води: під ванною, поруч з пральною машиною і так далі. При попаданні води на контактну поверхню датчика сигнал від датчика надходить на блок управління, який задіє кульові клапани з електроприводом, встановлені на водопровідних трубах для холодної і гарячої води, тим самим перекриваючи подачу води до тих пір, поки домовласник самостійно не

перезавантажить систему або вручну не відкриє клапани. Деякі функції, які можуть мати системи захисту від протікання води: звукове і світлове оповіщення при виявленні протікання, дистанційне повідомлення користувача за допомогою SMS-повідомлень або через Інтернет, робота від вбудованих акумуляторів в разі відключення основного джерела електроенергії.

Система захисту від витоків газу працює за принципом, схожим з системою захисту від протікання води і встановлюється в приміщеннях з газовим обладнанням: котельні, кухонні кімнати. Газоаналізатор, тобто датчик газу, фіксує витік газу, якщо його концентрація в повітрі перевищує деяке порогове значення. Далі газоаналізатор подає відповідний сигнал на контролер, а той, в свою чергу, задіє електромагнітний клапан, що перекриває подачу газу (рисунок 2.2).

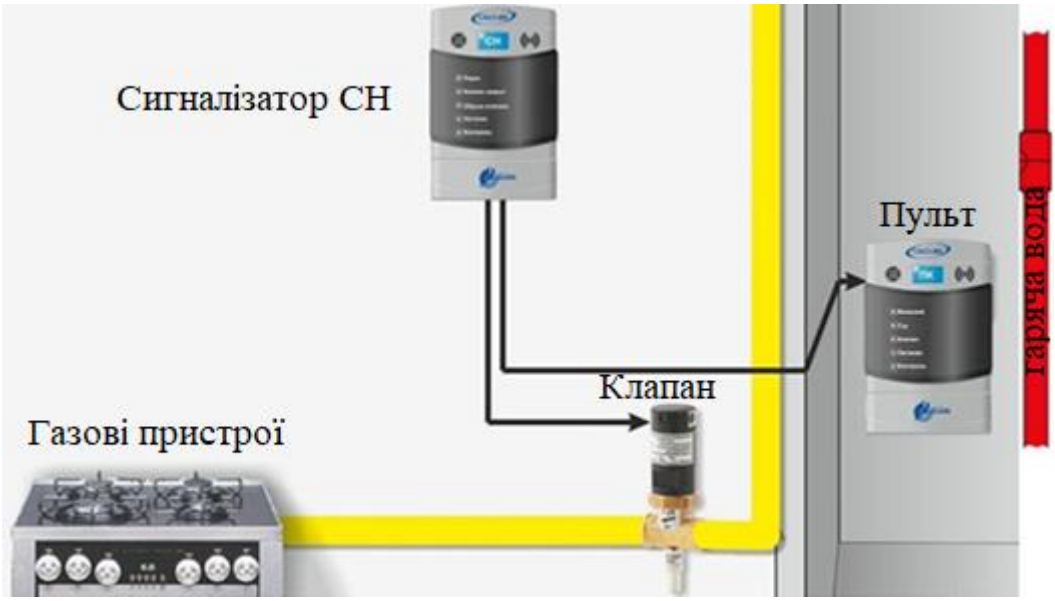


Рисунок 2.2 – Загальний пристрій системи захисту від витоку газу

Використання СКУД в «Розумних будинках» в більшості випадків зводиться до установки «розумних» дверних замків. Такі замки мають кілька способів для ідентифікації користувача: введення пароля на складальній панелі, використання технології RFID або NFC, за допомогою біометричних даних користувача, а також комбінацією цих способів.

Як приклад для розгляду вибрали модель дверного замка SHS-P718 від компанії Samsung (рисунок 2.3).

Рисунок 2.3 – «Розумний» дверний замок від Samsung

Завдяки вбудованому в корпус замку інфрачервоному датчику руху, замок активується, коли людина впритул підходить до дверей. Є можливість активації тривожного сигналу в разі, якщо хтось стоїть поруч з дверима протягом однієї хвилини без спроб відкрити замок. Можливі способи ідентифікації користувача: введення коду на складальній панелі, зчитування RFID-карти, зчитування відбитка пальця, а також комбіновані способи[24]. При спробі нанести замку механічні пошкодження активується звукова сигналізація. Від спроб злому програмного коду замок захищений спеціальними методами шифрування. Крім того, в замок вбудований датчик диму і при його спрацьовуванні також активується сигнал тривоги. Замок працює від батарейок і при низькому рівні їх заряду починає за допомогою спеціальних звукових сигналів повідомляти про це Користувача. Якщо батарейки все ж розрядилися, то в корпусі замка передбачена личинка для звичайного механічного ключа, а також роз'єм для підключення батарейки «Крона». «Розумні» замки від Samsung можуть бути об'єднані в єдину мережу з іншими «розумними» пристроями компанії: телевізорами, холодильниками, пральними машинами,

духовими шафами. Управління всіма пристроями здійснюється за допомогою мобільного телефону домовласника[25].

На ринку «розумних будинків» одним з лідерів є компанія Rubetek[26]. Вона пропонує як окремі "розумні" пристрої, так і готові комплекти, один з яких називається «управління та безпека». До його складу входять: модуль управління, датчик протікання, датчик відкриття, датчик диму. Однак користувач може зібрати свою власну систему з будь-яких вподобаних йому пристроїв від даного виробника: центр управління, поворотні Wi-Fi камери, датчик витоку газу, датчик відкриття, датчик протікання, датчик руху, датчик диму, а також «розумні» розетки і багатоканальні реле (рисунок 2.4).

Рисунок 2.4 – Система безпеки «розумного будинку» від Rubetek

Всі датчики працюють від батарейок і є бездротовими: обмін даними здійснюється на частоті 433 МГц по протоколу EV 1527. Користувач управляє системою і отримує від неї повідомлення через Інтернет за допомогою спеціального додатку для мобільного телефону. Приклад побудови системи "Розумного будинку" на основі пристроїв від даної компанії представлений на Рисунок 2.5

Рисунок 2.5 – Приклад розташування елементів «Розумного будинку» від компанії Rubetek

Широке визнання на ринку охоронних систем отримала «розумна» сигналізація Ajax українського виробництва. Дана охоронна система складається з керуючого пристрою і набору датчиків. Управління настройками системи здійснюється за допомогою програми для мобільного телефону. Для обміну даними між пристроями компанія розробила власний протокол передачі даних Jeweller, що використовує для роботи одну з декількох радіочастот: якщо зловмисник вирішить "заглушити" систему, то вона автоматично переключиться на іншу частоту і продовжить функціонувати. При спробі розтину корпусу будь-якого з пристроїв система активує сигналізацію, так як спрацюють вбудовані в корпуси пристроїв датчики розтину[27].

Перелік пропонованих виробником датчиків: датчик руху, датчик розбиття скла, датчик детектування диму, датчик виявлення затоплення, датчик відкриття дверей/вікна (рисунок 2.6).

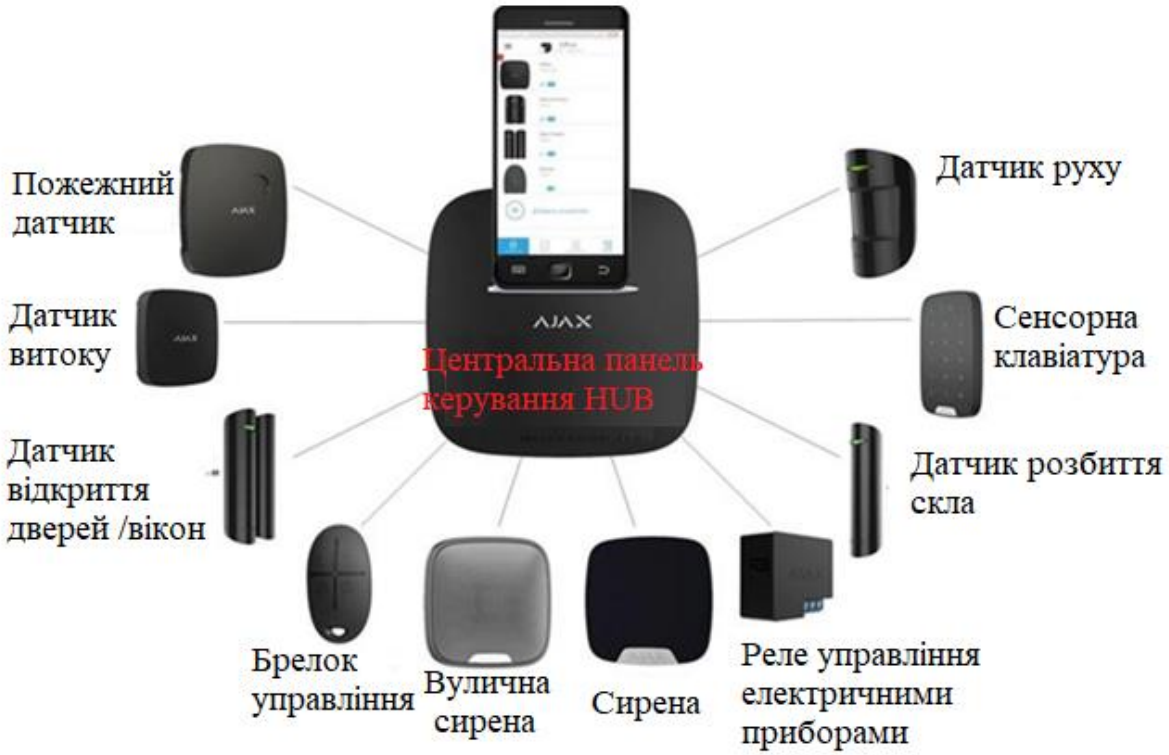


Рисунок 2.6 – «Розумна» охоронна система Ajax

Таким чином, більшість існуючих на сьогоднішній день систем безпеки, що застосовуються в «Розумних будинках», фіксують виникнення таких аварійних ситуацій: виникнення вогнища загоряння, витоку води, витік побутового газу, проникнення сторонніх осіб. Для цього вони мають у своєму складі: датчик вогню, датчик протікання води, датчик витоку газу, датчики проникнення (датчик відкриття дверей або вікна, датчик розбиття віконного скла, датчик руху). Для повідомлення Користувача використовується звукове або світлове оповіщення, а для дистанційного повідомлення і управління системою: GSM-зв'язок, Інтернет, Bluetooth.

На основі аналізу існуючих рішень визначили, які саме аварійні ситуації повинна фіксувати проектована система безпеки "Розумного будинку", а саме: протікання води, витік побутового газу, виникнення вогнища загоряння, проникнення сторонніх осіб. З даних аварійних ситуацій система повинна вміти запобігати протікання води і витік побутового газу. У разі виникнення будь-якої аварійної ситуації система повинна сповіщати користувача за допомогою

сигнального пристрою, а сам користувач повинен мати можливість дистанційно керувати системою. Повинна бути підсистема контролю і управління доступом.

Таким чином, проектована система повинна містити в собі кілька основних структурних блоків (рисунок 2.7)

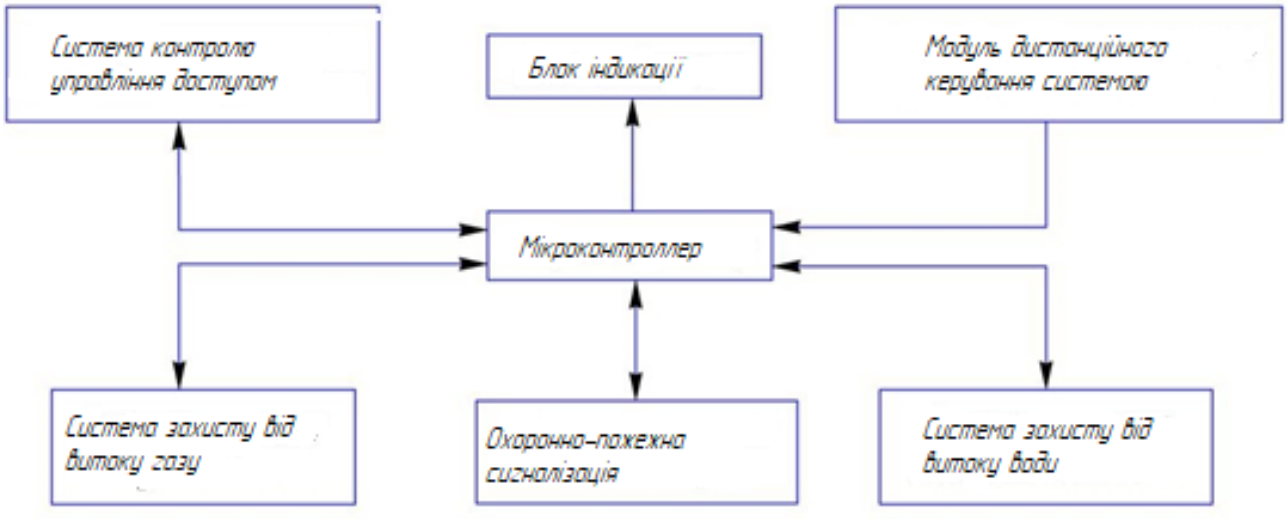


Рисунок 2.7 – Структурна схема проектованої системи безпеки "Розумного будинку" на основі мікроконтролера

Керуючим пристроєм проектованої системи є мікроконтролер. Його переваги в порівнянні з одноплатними комп'ютерами або промисловими контролерами полягають в низькій вартості, малому споживанні електроенергії, а також малих габаритах, при цьому мікроконтролери володіють достатніми можливостями для створення гнучких і функціональних систем.

Блок індикації містить в собі пристрої для оповіщення користувача в заздалегідь визначених випадках, а саме: дисплей для виведення інформації, а також сигнальний пристрій.

Охоронно-пожежна сигналізація виявляє проникнення сторонніх осіб, а також виникнення вогнища загоряння. У своєму складі вона має: датчик відкриття вхідних дверей і датчик вогню.

Система захисту від протікання води складається з відповідного датчика протікання води, а також виконавчого механізму, що перекриває подачу води.

Система захисту від витоків газу складається з відповідного датчика витоку газу, а також виконавчого механізму, що перекриває подачу газу.

Система контролю та управління доступом складається з пристрою для ідентифікації користувача, а також електромагнітного замка.

Можливість дистанційного керування системою здійснюється за допомогою відповідного модуля, що працює за однією з бездротових технологій.

Однак на ринку домашніх систем безпеки існує великий вибір не тільки різних датчиків, але і виконавчих механізмів: різні пристрої для перекриття подачі води; пристрої для перекриття подачі газу, а також примусової вентиляції приміщення в разі його витоку; електромагнітні замки в системах контролю і управління доступом. Вибір таких виконавчих механізмів залежить від безлічі різних факторів, наприклад: при виборі механізму для перекриття подачі води треба враховувати тиск у відповідному трубопроводі, при виборі механізму для примусової вентиляції повітря в приміщенні треба враховувати площу цього приміщення. Сигнальні звукові і світлові пристрої, що спрацьовують в разі виникнення будь-якої аварійної ситуації, також вимагають ретельного вибору. У зв'язку з цим в рамках даної роботи при проектуванні системи безпеки «Розумного будинку» не проводиться вибір безпосередньо виконавчих механізмів. Для розробки структурної схеми і наступних етапів проектування прийняли, що при виникненні аварійної ситуації мікроконтролер повинен задіяти тільки самі комутуючі пристрої, наприклад реле. За допомогою комутуючих пристроїв можна безпосередньо управляти роботою виконавчих механізмів, кінцевий вибір яких залишається за користувачем і ніяк не впливає на алгоритм роботи системи.

Таким чином, більш детальна структурна схема проектованої системи безпеки представлена на (рисунок 2.8).

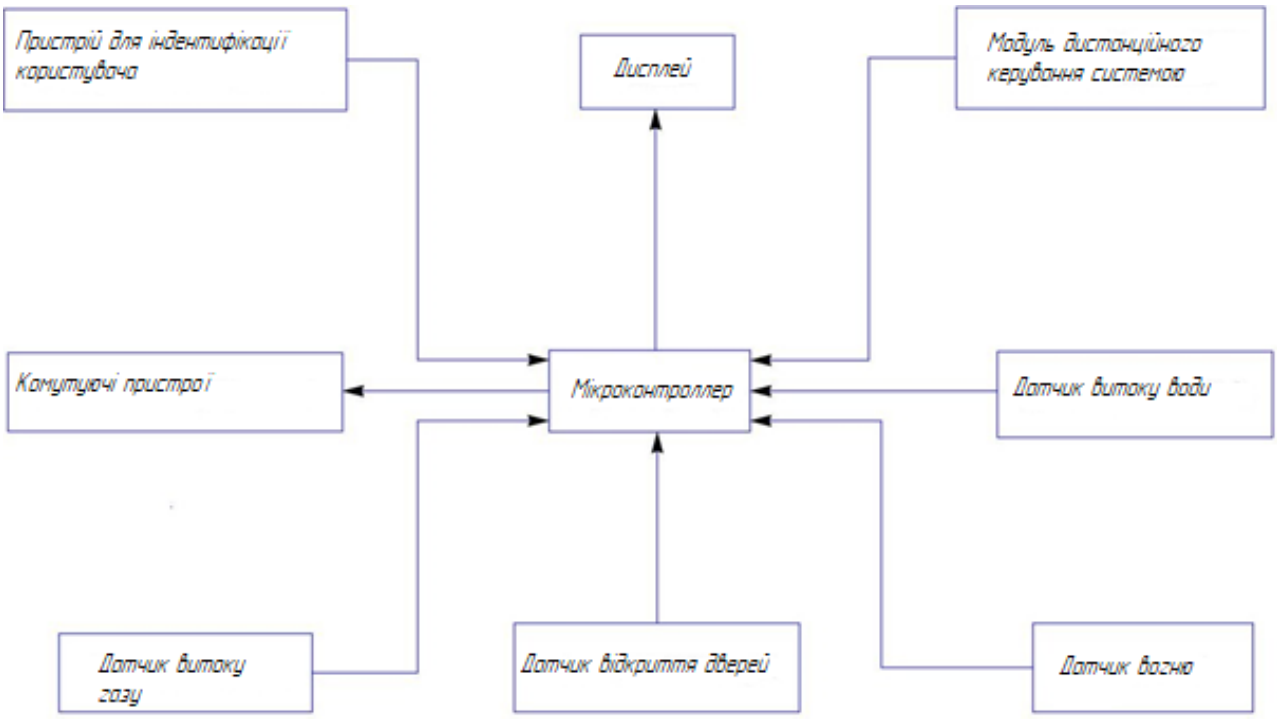


Рисунок 2.8 – Структурна схема проектованої системи безпеки «Розумного будинку»

2.2 Розробка алгоритму роботи

Проектована система безпеки «Розумного будинку» повинна мати два режими роботи: «Охорона відключена» і «Охорона включена».

У режимі "Охорона відключена", який є вихідним і активується відразу після подачі живлення на систему, опитуються тільки датчики протікання води, витоку газу, вогню. Ці датчики відстежують виникнення найбільш небезпечних аварійних ситуацій і тому при наявності напруги живлення повинні працювати постійно з метою захисту від їх випадкового відключення. При спрацьовуванні будь-якого з даних датчиків задіюється блок індикації: спрацьовує сигнальний пристрій, виводиться відповідна інформація на дисплей. При виявленні протікання води повинен спрацьовувати виконавчий механізм, що перекриває її подачу до тих пір, поки користувач самостійно не відключить даний механізм (рисунок 2.9).

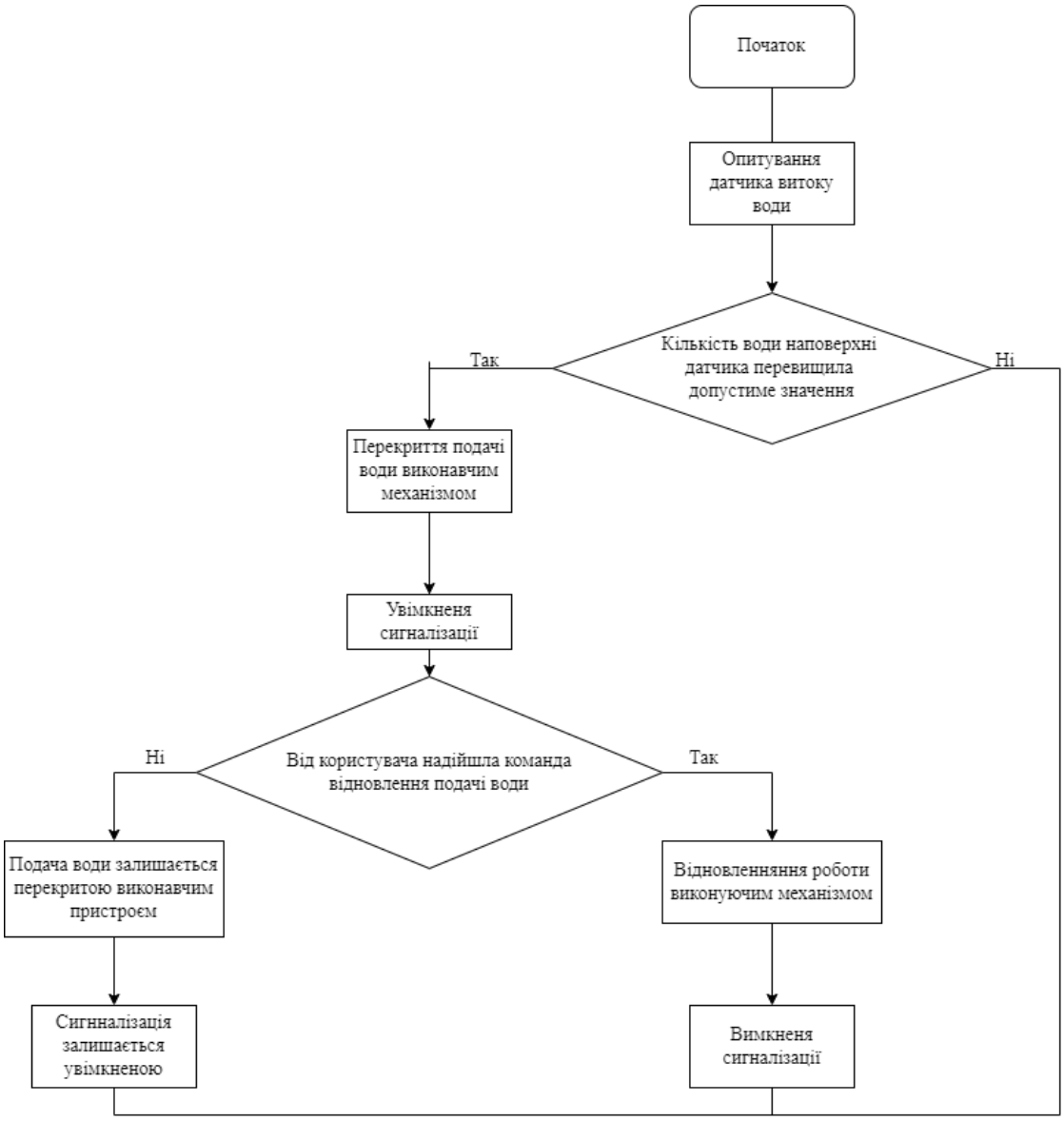


Рисунок 2.9 – Блок-схема алгоритму роботи системи захисту від протікання води

Аналогічно для системи захисту від витоків газу: при витоку газу виконавчий механізм перекриває його подачу до тих пір, поки користувач самостійно не відключить даний виконавчий механізм (рисунок 2.10).

Алгоритм роботи системи при виявленні загоряння: при виникненні вогнища загоряння відповідний датчик вогню фіксує дану аварійну ситуацію і включається сигналізація. Сигналізація залишається включеною, навіть якщо джерело полум'я погашене або не фіксується датчиком з якої-небудь іншої причини. Відключення сигналізації також проводиться користувачем в обох режимах роботи проектованої системи управління і контроль доступом

здійснюється за допомогою RFID-технології і виконавчого механізму, в якості якого виступає електромагнітний дверний замок.

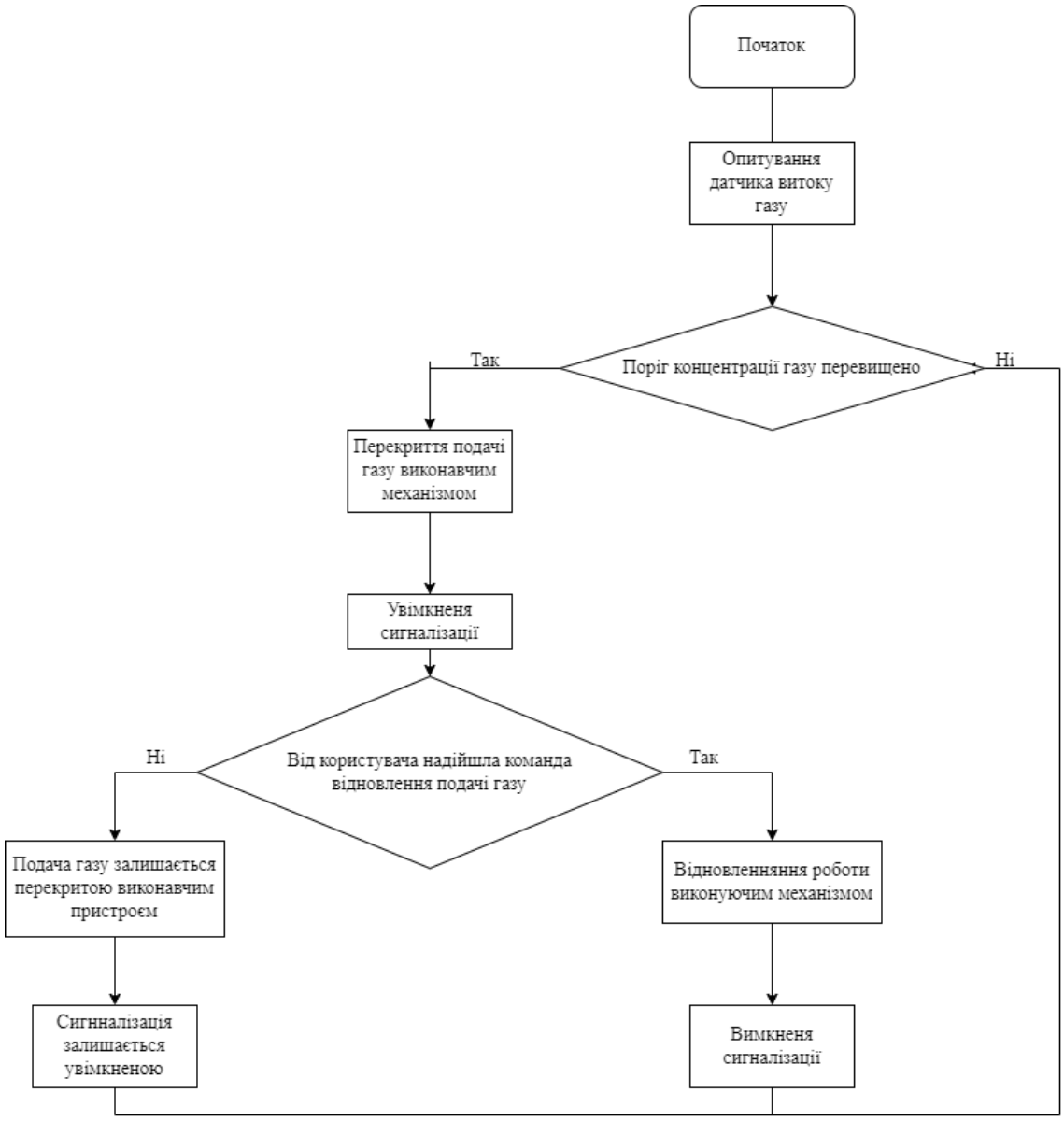


Рисунок 2.10 – Блок-схема алгоритму роботи системи захисту від витоків газу

У мікроконтролері зберігається унікальний ідентифікаційний номер RFID-мітки користувача і при піднесенні мітки до RFID-зчитувача останній здійснює читання номера мітки і на основі порівняння отриманого номера з номером, що зберігається в пам'яті мікроконтролера, дозволяє або забороняє доступ (рисунок 2.11). Відкриття і закриття дверного замка здійснюється за допомогою однієї мітки і одного зчитувача: спочатку користувач підносить

свою RFID-мітку, перебуваючи зовні вхідних дверей, а потім, увійшовши всередину свого будинку або квартири, він підносить мітку до зчитувача знову, щоб закрити за собою замок. Зчитувач повинен монтуватися в дверний замок таким чином, щоб була можливість зчитування мітки, коли користувач знаходиться з будь-якої зі сторін двері.

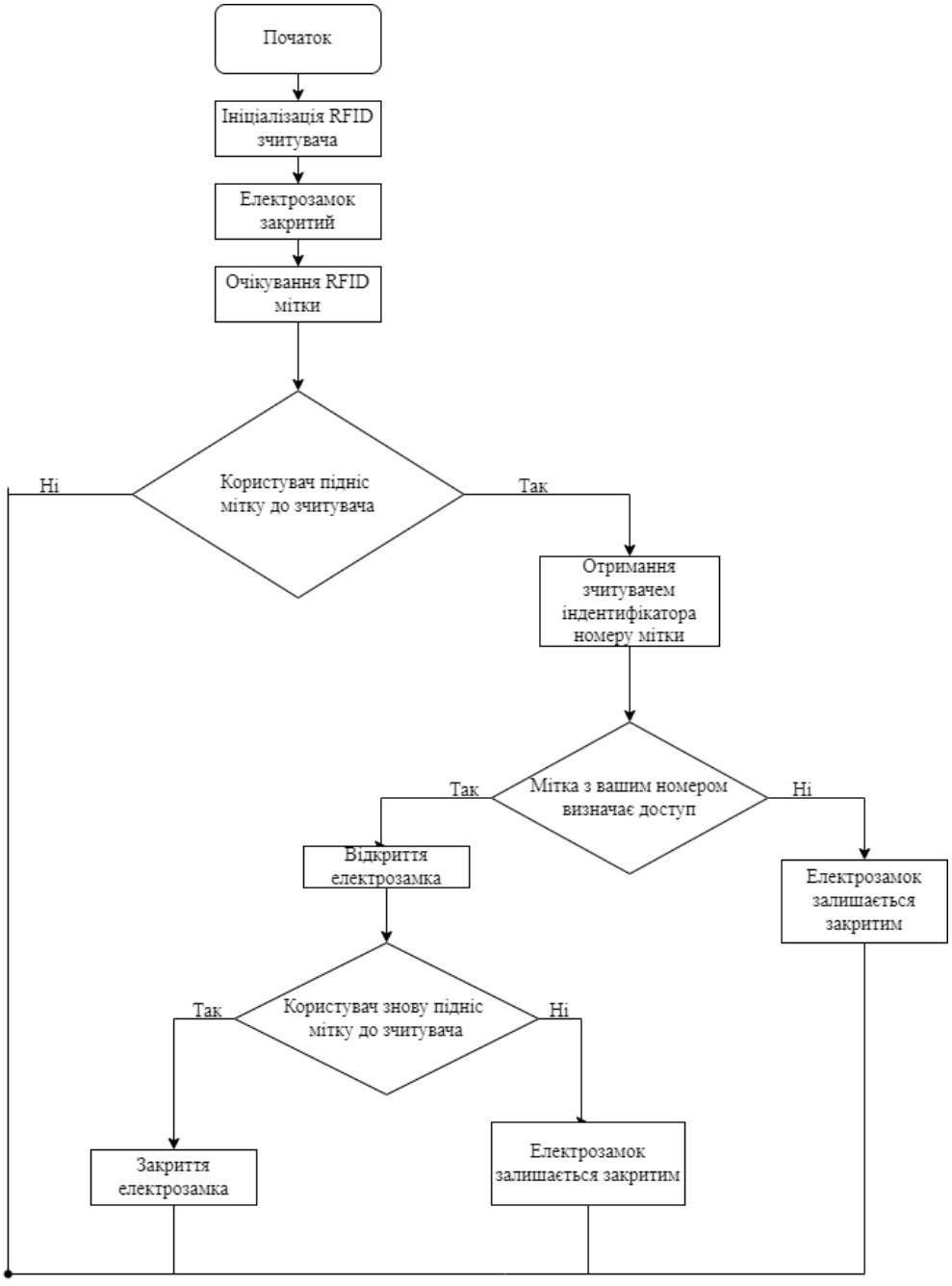


Рисунок 2.11 – Блок-схема алгоритму контролю доступу в проектованій системі безпеки «Розумного будинку»

У режимі "Охорона включена" опитуються не тільки датчики протікання води, витоку газу, вогню, а й датчик відкриття вхідних дверей. Режим "Охорона включена" активується Користувачем, коли він вже вийшов з будинку або квартири, тобто знаходиться за вхідними дверима. Зняття системи з режиму охорони також відбувається за межами будинку або квартири користувача. В іншому випадку, якщо користувач забув зняти систему з охорони і відкрив вхідні двері, активується Сигналізація — тоді користувачеві потрібно зняти систему з охорони і сигналізація автоматично відключиться (рисунок 2.12).

Відключення виконавчих пристроїв і сигналізації здійснюється без використання кнопок і інших фізичних перемикачів, але з використанням бездротової технології передачі даних, наприклад за допомогою мобільного телефону користувача і спеціальної встановленої на ньому програми.

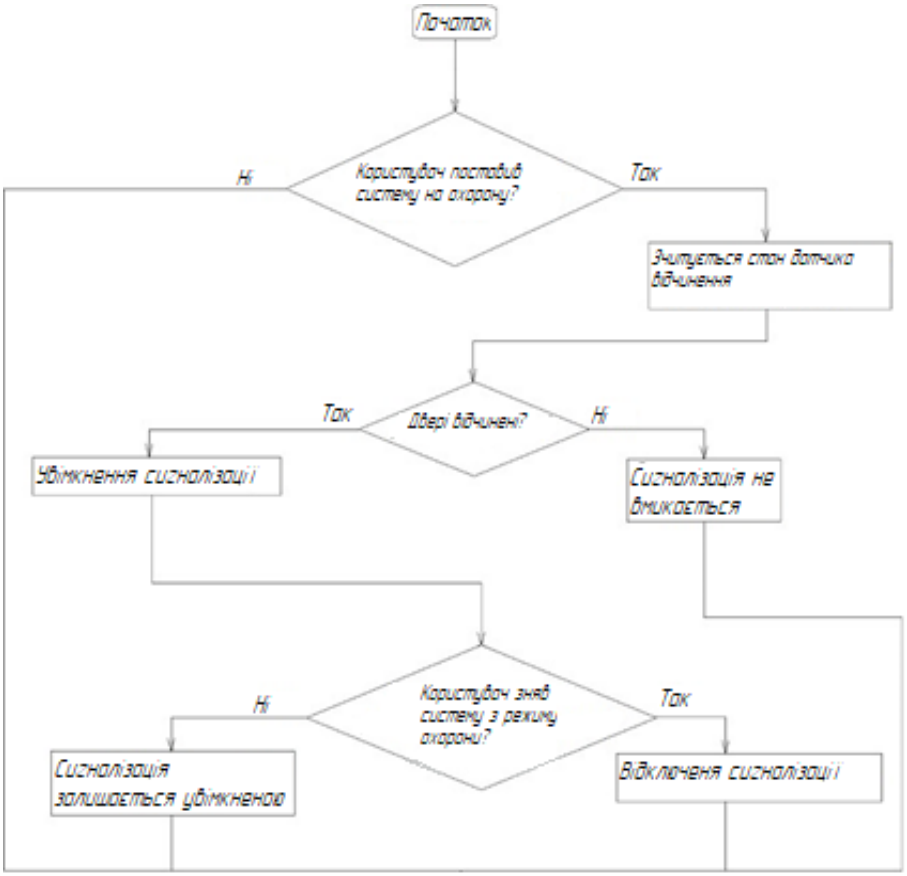


Рисунок 2.12 – Блок-схема алгоритму постановки системи в режим охорони і зняття системи з даного режиму за допомогою кнопки

2.3 Вибір необхідних компонентів

Проектована система безпеки "Розумного будинку" для роботи згідно з розробленим алгоритмом повинна мати в своєму складі ряд електронних елементів: мікроконтролер, датчики для фіксації аварійних подій, комутуючі пристрої для підключення виконавчих механізмів, дисплей для виведення різної інформації, модуль для дистанційного керування системою користувачем[28].

2.4 Програмна частина

В якості апаратно-програмної платформи проектованої системи була обрана Arduino. Дана платформа з відкритим вихідним кодом включає в себе серію плат на основі 8-бітних мікроконтролерів ATmega, сумісні з платами модулі для вирішення різних завдань (рисунок 2.13), а також середовище розробки і налагодження програм Arduino IDE (Integrated Development Environment).

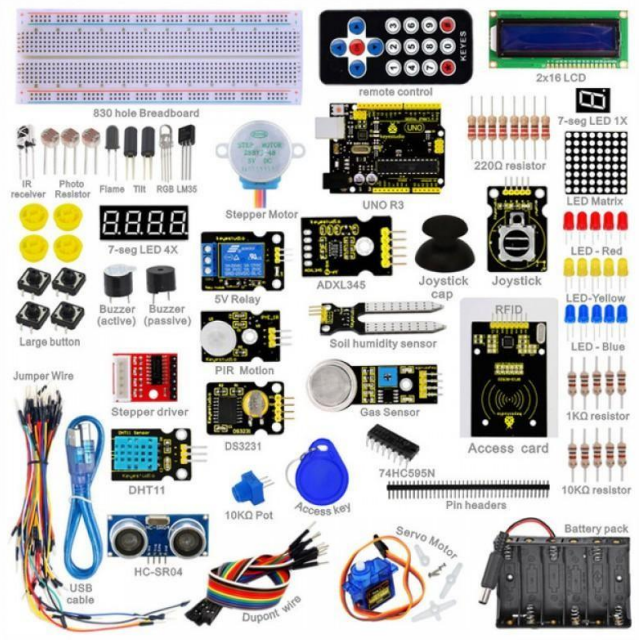


Рисунок 2.13. – Частина апаратного забезпечення платформи Arduino

Приклад деяких модулів, сумісних з платами Arduino: дисплеї, індикатори, крокові двигуни і сервоприводи, датчики, кнопки, реле, а крім того, є модулі і плати розширення, за допомогою яких платформа може працювати з сучасними технологіями Wi-Fi, Bluetooth, GSM, ZigBee, Ethernet, RFID, NFC[29].

Плати Arduino крім самого мікроконтролера містять у своїй конструкції різні компоненти: аналогові і цифрові порти введення-виведення інформації, роз'єми для живлення і підключення до комп'ютера, стабілізатор вхідної напруги, інтерфейс UART (Universal Asynchronous Receiver-Transmitter) і багато іншого (рисунок 2.14). З лінійки плат Arduino варто виділити дві плати, що найбільш часто зустрічаються в складних електронних проектах і забезпечують підключення відносно великого числа різних зовнішніх пристроїв, а саме: плата Arduino Uno і плата Arduino Mega 2560. На основі порівняльного аналізу цих двох плат в якості центрального керуючого пристрою проектованої системи була обрана плата Arduino Mega 2560[30].

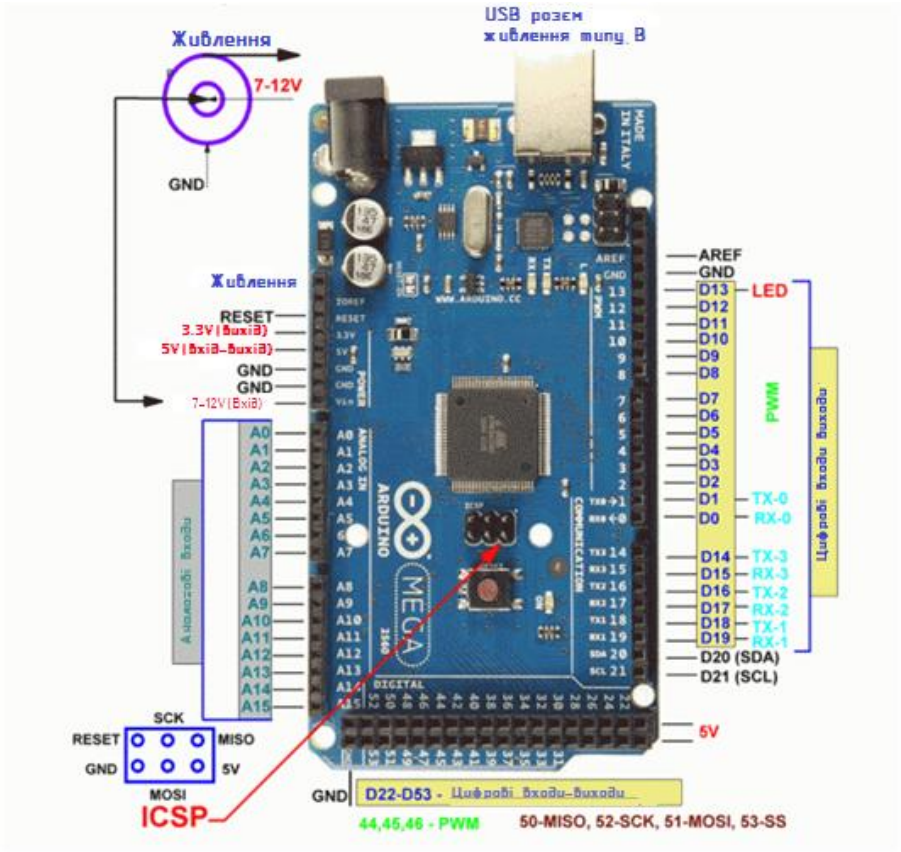


Рисунок 2.14 – Плата Arduino Mega 2560

Дана плата оснащена "потужним" мікроконтролером і має найбільше число портів введення-виведення інформації серед всіх плат Arduino, що забезпечує гнучкість проектованої системи в плані можливості її подальшого масштабування .

У проектованій для виведення різної корисної інформації необхідний дисплей. З його допомогою користувач може отримувати інформацію про фіксацію тієї чи іншої аварійної події, про режим роботи схеми, про факт зчитування незареєстрованої в пам'яті мікроконтролера RFID-мітки, про включення комутуючих пристроїв.

В якості дисплей вибрали дисплей LCD - 1602 HD44780 (рисунок 2.15).

Рисунок 2.15 – LCD-дисплей 16x2

Даний дисплей можна підключити до плати Arduino за допомогою інтерфейсу I2C (Inter-Integrated Circuit) з використанням всього чотирьох проводів: двох для живлення і двох для обміну інформацією [31].

Напруга живлення дисплея становить від 3,3 до 5 В, яскравість зображення регулюється потенціометром на I2C-модулів.

Для фіксації виникнення вогнища загоряння необхідний датчик вогню. Вибрали модель KY - 026 (Рисунок 2.16).

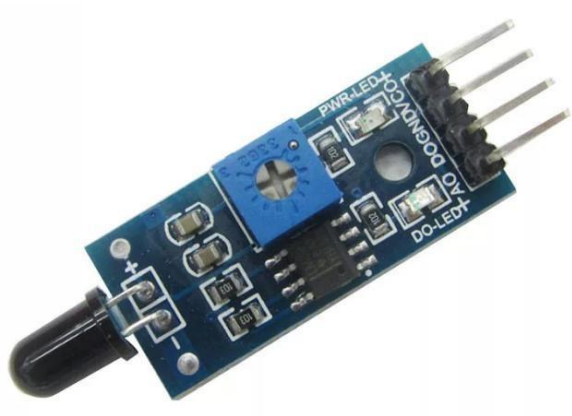


Рисунок 2.16 – Датчик вогню KY-026

Даний датчик реагує електромагнітні хвилі, що лежать в області інфрачервоного випромінювання, завдяки чому він може виявляти відкритий вогонь [32]. Однак при певних умовах він може спрацювати і на яскраве сонячне світло, виправити цей недолік можна регулюванням чутливості датчика. Робоча дистанція датчика становить до 4 м. Робоча напруга датчика знаходиться в межах від 3,3 до 5 В. Максимальний струм споживання становить 10 мА.

Для системи захисту від витоків газу вибрали модуль MQ-2 на основі напівпровідникового газоаналізатора MQ-2 (рисунок 2.17).

Рисунок 2.17 – Датчик газу MQ-2

Даний модуль здатний виявляти різні горючі і займисті гази, в тому числі природний газ (метан, бутан, пропан) [33].

У своїй конструкції газоаналізатор має трубку з кераміки, покриту чутливим шаром з діоксиду олова. Усередині трубки знаходиться спеціальний нагрівальний елемент, що забезпечує правильну роботу датчика: нагрітий чутливий шар починає реагувати на молекули газу, концентрацію якого необхідно відстежувати. Концентрацію відстежуваного газу можна контролювати за допомогою аналогового сигналу, що знімається з виходу датчика: чим вище концентрація цього газу, тим більше за величиною вихідна напруга, і навпаки. Робоча напруга датчика знаходиться в межах від 3,3 до 5 В. Струм споживання становить 160 мА. Датчик, при подачі на нього живлення, вимагає кілька хвилин на нагрів чутливого елемента, тому іноді можливі помилкові спрацьовування.

Для системи захисту від протікання води вибрали модуль FC-37 [34]. Контактна поверхня датчика складається з двох не пов'язаних один з одним струмопровідних доріжок: вода, при попаданні одночасно на обидві доріжки, замикає їх, тим самим викликаючи спрацьовування датчика (рисунок 2.18).

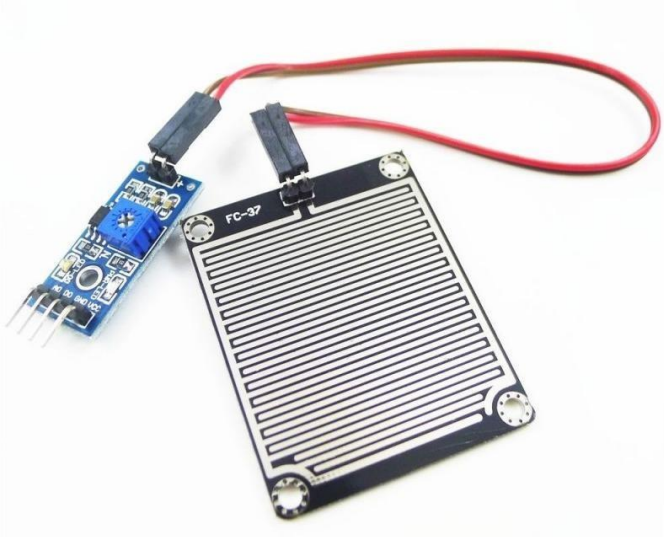


Рисунок 2.18 – Датчик протікання води FC-37

Для фіксації відкриття вхідних дверей вибрали датчик відкриття KY025. Даний модуль містить у своїй конструкції геркон (рисунок 2.19).

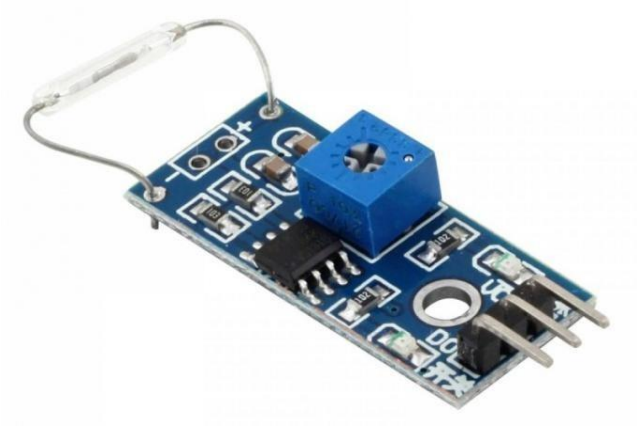


Рисунок 2.19 – Датчик відкриття дверей KY-025

При відсутності магнітного поля геркон нормально відкритий, а при його появі контакти геркона замикаються. Сам датчик повинен розташовуватися на нерухомій частині конструкції (дверній рамі), а магніт, що створює потрібне магнітне поле, повинен кріпитися до рухомої частини конструкції, тобто безпосередньо до самих дверей.

Даний модуль має робочу напругу від 3,3 до 5 В, здатний витримати протікання струму величиною до 1,2 А і має робочу відстань до 1,5 м [35].

Для контролю доступу вибрали модуль RC522 [36]. Для RFID-зчитувача потрібна RFID-мітка, наприклад RFID-карта (рисунок 2.20).

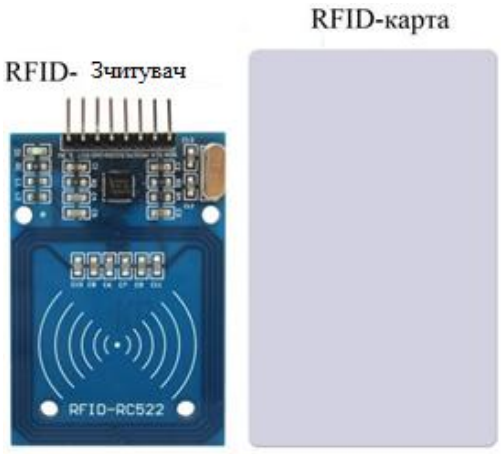


Рисунок 2.20 – RFID-система для платформи Arduino

Робоча напруга RFID-зчитувача RC522 становить 3,3 В, а максимальний робочий струм досягає 26 мА.

Технологія RFID (радіочастотна ідентифікація) є надійною і економічною технологією, створеною з метою автоматичного розпізнавання об'єктів з використанням електромагнітних полів (рисунок 2.21).

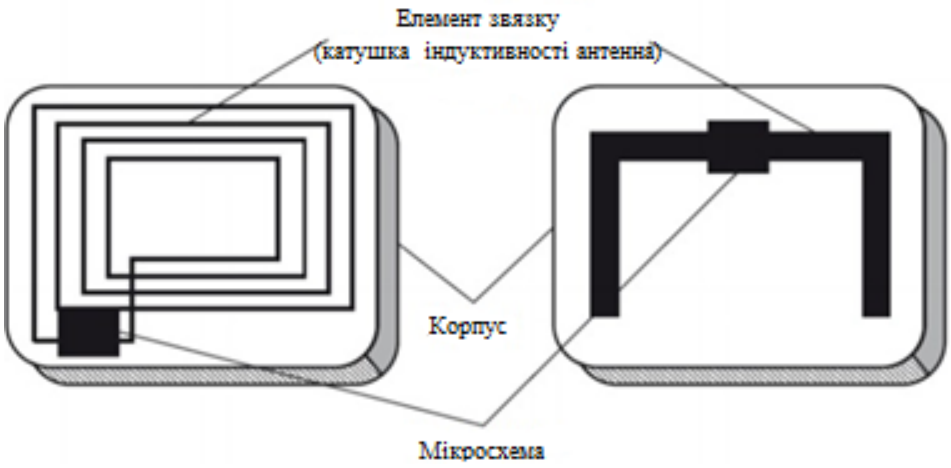


Рисунок 2.21 – Будова RFID-мітки

Система працює наступним чином. Усередині RFID-карти знаходиться чіп, що зберігає в собі унікальний ідентифікаційний номер у вигляді цифрового коду. Також в корпусі карти знаходиться спеціальна антена, яка приймає і випромінює радіохвилі. Зчитувач генерує радіохвилю - антена RFID-карти приймає її, отримуючи потрібну для своєї роботи енергію. RFID-карта за допомогою антени випромінює радіохвилю тієї ж частоти, що і хвиля, що прийшла від зчитувача, модулювавши її вмістом пам'яті чіпа. Нарешті, RFID-зчитувач отримує цю радіохвилю від карти і декодує її, отримуючи доступ до цифрового ідентифікаційного номера саме даної RFID-карти [37].

Для підключення до плати Arduino різних виконавчих механізмів необхідні комутуючі пристрої. Вибрали модуль чотириканального реле (рисунок 2.22).

Рисунок 2.22 – Модуль чотириканального реле для Arduino

Модуль працює від напруги 5 В. Струм споживання кожного з чотирьох реле становить 70 мА. В даному модулі є зворотні діоди, що захищають контакти реле, а також гальванічна розв'язка, що захищає висновки безпосередньо самого мікроконтролера [38].

Для можливості дистанційного керування платою Arduino Mega 2560 вибрали Bluetooth-модуль HC-05 [39]. Звичайно, технологія Bluetooth не може забезпечити передачу даних на великі відстані, на відміну від GSM-зв'язку або ж мережі Інтернет. Однак до важливих переваг протоколу Bluetooth слід віднести низьке енергоспоживання, хорошу захищеність переданих даних, локалізований радіус дії.

Обраний Bluetooth-модуль обмінюється даними з платою Arduino по інтерфейсу UART через висновки TX і RX (рисунок 2.23).

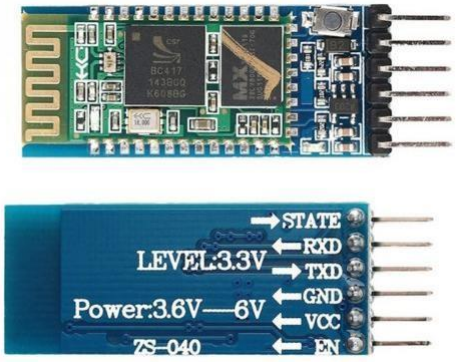


Рисунок 2.23 – Bluetooth модуль HC-05

Склали принципову електричну схему проектованої системи безпеки "Розумного будинку"[40] (рисунок 2.24).

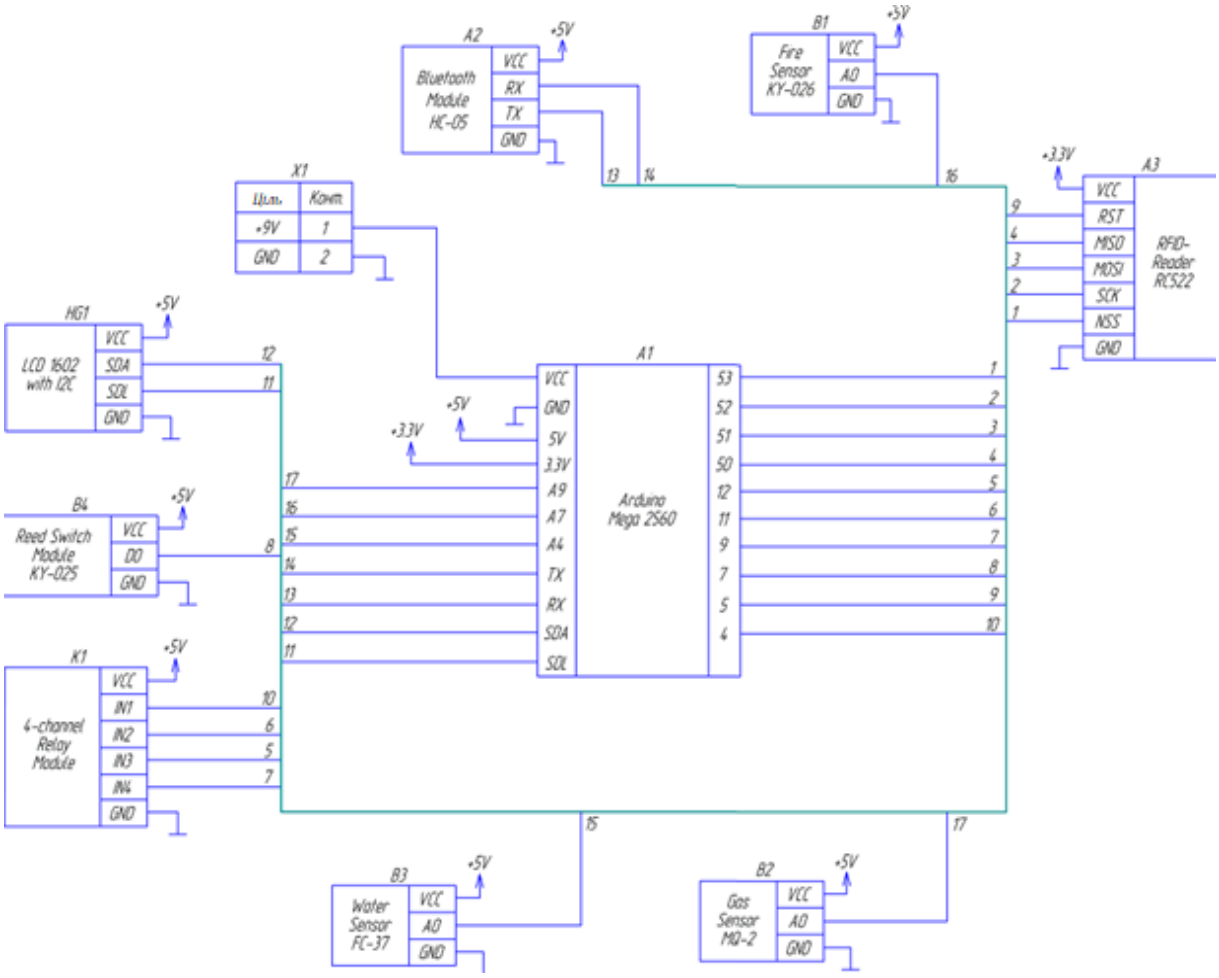


Рисунок 2.24 – Принципова схема проектованої системи

2.4 Висновки

У системах захисту від протікання води і витоків газу ключову роль відіграють виконавчі механізми, які відсікають подачу, відповідно, води або газу.

Датчик протікання води розміщується в тих приміщеннях і місцях, в яких можливе протікання води: під ванною, поруч з пральною машиною і так далі.

Система захисту від витоків газу працює за принципом, схожим з системою захисту від протікання води і встановлюється в приміщеннях з газовим обладнанням: котельні, кухонні кімнати. Газоаналізатор, тобто датчик

газу, фіксує витік газу, якщо його концентрація в повітрі перевищує деяке порогове значення.

Як приклад для розгляду вибрали модель дверного замка SHS-P718 від компанії Samsung.

На ринку «розумних будинків» одним з лідерів є компанія Rubetek. Вона пропонує як окремі "розумні" пристрої, так і готові комплекти, один з яких називається «управління та безпека». До його складу входять: модуль управління, датчик протікання, датчик відкриття, датчик диму. Однак користувач може зібрати свою власну систему з будь-яких вподобаних йому пристроїв.

Широке визнання на ринку охоронних систем отримала «розумна» сигналізація Ajax українського виробництва. Дана охоронна система складається з керуючого пристрою і набору датчиків.

Проектована система безпеки «Розумного будинку» повинна мати два режими роботи: «Охорона відключена» і «Охорона включена».

Проектована система безпеки "Розумного будинку" для роботи згідно з розробленим алгоритмом повинна мати в своєму складі ряд електронних елементів: мікроконтролер, датчики для фіксації аварійних подій, комутуючі пристрої для підключення виконавчих механізмів, дисплей для виведення різної інформації, модуль для дистанційного керування системою користувачем.

В якості апаратно-програмної платформи проектованої системи була обрана Arduino. Дана платформа з відкритим вихідним кодом включає в себе серію плат на основі 8-бітних мікроконтролерів ATmega, сумісні з платами модулі для вирішення різних завдань, а також середовище розробки і налагодження програм Arduino IDE (Integrated Development Environment).

3 АЛГОРИТМИ ТА ТЕХНОЛОГІЯ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ

3.1 Алгоритм вирішення задачі

У середовищі розробки Arduino IDE склали програмний код, що реалізує розроблений раніше алгоритм роботи проектованої системи (див. додаток А).

Для розробки системи використовувалися наступні технології та інструменти такі як C#, ASP .NET Core, ASP .NET SignalR, Enitity Framework Core, WPF.

C# - це мова програмування призначена для розробки найрізноманітніших додатків, призначених для виконання в среді .NET Framework. Мова C# проста, типобезпечна та об’єктно-орієнтовнаю Завдяки багатьох нововедень C# забезпечує можливість швидкої розробки додатків і при цьому зберігає елегантність C-подібних мов. З останніми тенденціями та нововведеннями такими як .NET Core та .NET Standard надає можливість кросплатформенної розробки як і при розробці під ОС Windows.

ASP .NET Core – це новий кросплатформений фреймворк з відкритим вихідними кодом («open-source») для розробки сучасних хмаро орієнтованих додатків, таких як веб-застосування, IoT (Internet of Things) додатків та серверних частин для мобільних додатків [41].

ASP .NET Core надає наступні основні можливості:

- розробка графічного веб інтерфейсу та Web Api як єдиного цілого;
- інтеграцію з сучасними клієнтськими фреймворками;
- систему конфігурацій, що забезпечує підтримку хмарних обчислень;
- вбудований IoC-контейнер;
- нову модульну обробку HTTP запитів;
- новий набір інструментів, що полегшують веб розробку;
- можливість запуску ASP .NET додатків на таких ОС як Windows, Mac, Linux.

ASP .NET SignalR – це бібліотека для ASP .NET, що надає можливість розробляти «real-time» веб додатки [42]. SignalR надає двонаправлену комунікацію між сервером та клієнтом. Сервер може безпосередньо відправляти контент до користувачів, що встановили з ним зв'язок. SignalR підтримує Web Sockets та має зворотню підтримку інших підходів таких як SSE та pooling. Даний фреймворк дозволить забезпечити відправку сповіщень користувачеві у нашій системі.

Entity Framework (EF) Core – це легковісна та кросплатформена версія популярного EF, що надає доступ до даних [42]. Це об'єктно-реляційне відображення, що надається розробникам .NET для роботи з БД. Він відображує реляційні таблиці на об'єкти та зменшує обсяг коду для взаємодії з БД. Надає можливість вибірки та додавання/оновлення/видалення даних з БД.

Windows Presentation Foundation (WPF) – система для побудови клієнтських додатків Windows з візуальними можливостями комунікації з користувачем [23]. В основі WPF закладено векторну систему візуалізації, що не залежна від приладу виводу та створена з урахуванням можливостей сучасного графічного обладнання. WPF надає інструментарій для створення візуального інтерфейсу, що містить в основі мову XAML (eXtensible Application Markup Language) зокрема, елементи управління, прив'язку даних, макети, двомірну та трьохмірну графіку, анімацію, стилі, шаблони і т. д.

Ми обрали базу даних PostgreSQL, оскільки вона кросплатформена та має вбудовані інструменти для горизонтального масштабування такі як шардинг та «мультимастер». Діаграма бази даних представлена на кресленику ІА32.120БАК.005 Д3. При проектуванні таблиць використовувалася третя нормальна форма.

Нормальна форм – вимога, яка пред'явлена до структури таблиць в теорії реляційних баз даних для усунення з БД надлишкових функціональних залежностей між атрибутами (полями таблиць). Ціль нормалізації полягає у тому, щоб виключити дублювання даних, яке можне стати причиною

отримання неочікуваних результатів при редагування, додаванні чи видаленні. Часто застосовують перші три нормальні форми (НФ).

Відношення знаходиться у 1НФ, якщо його атрибути є простими та атомарними.

Відношення знаходиться у 2НФ, якщо воно знаходиться в 1НФ та кожен не ключовий атрибут залежить від первинного ключа (ПК).

Відношення знаходиться у 3НФ, якщо воно знаходиться в 2НФ та кожен не ключовий атрибут нетранзитивно залежить від ПК.

Розглянемо деякі ключові відношення. Маємо користувача (таблиця «User»), який може приймати участь у декількох проектах (таблиця «Project») з різними ролями (таблиця «Role»). Відповідно для розв'язки між ними створено таблицю «UserRoleProject» (рисунок 3.1), яка містить три зовнішні ключі – UserId, ProjectId, RoleId.

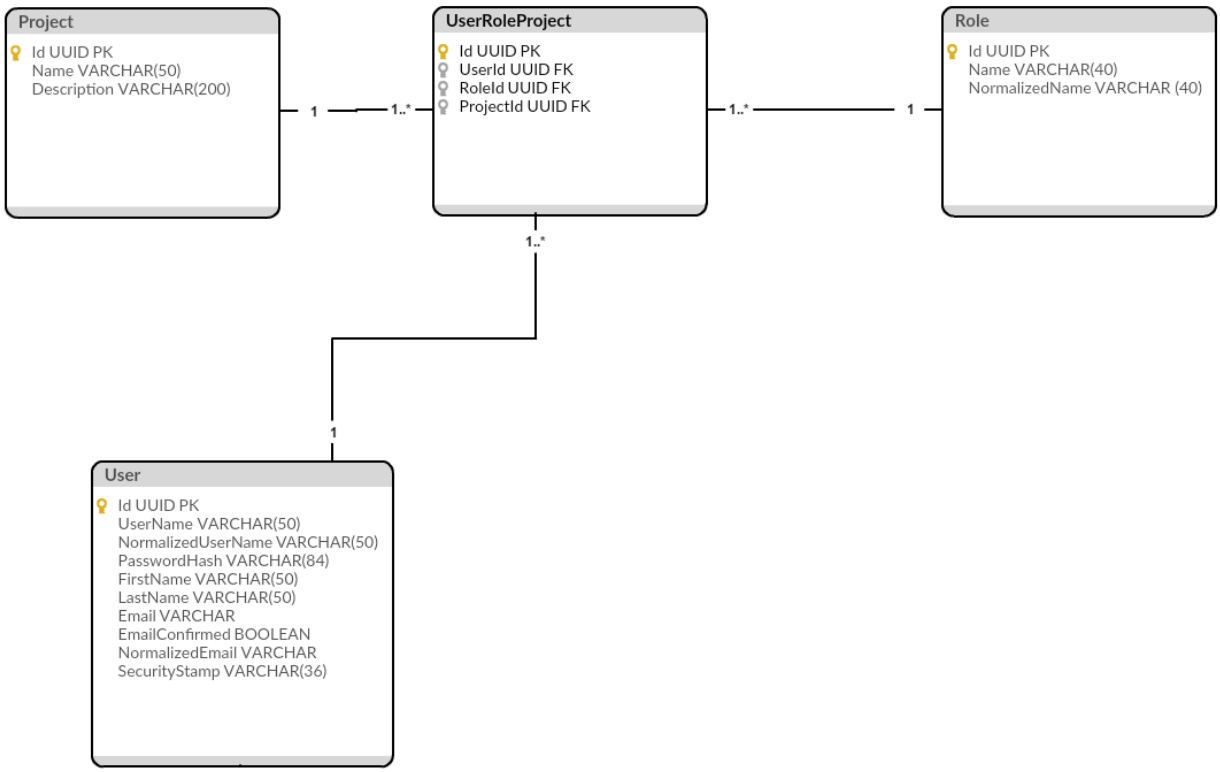


Рисунок 3.1 – Відношення між таблицями «User», «Project», «Role»

Надаємо можливість запрошувати інших користувачів до проекту для цього створено таблицю «Invite» (Рисунок 3.2). Вона має два зовнішні ключі на

таблиці «User» - це пов’язано з тим, що нам необхідно знати хто створив запрошення (CreatorId) та кого запрошують (InviteeId).

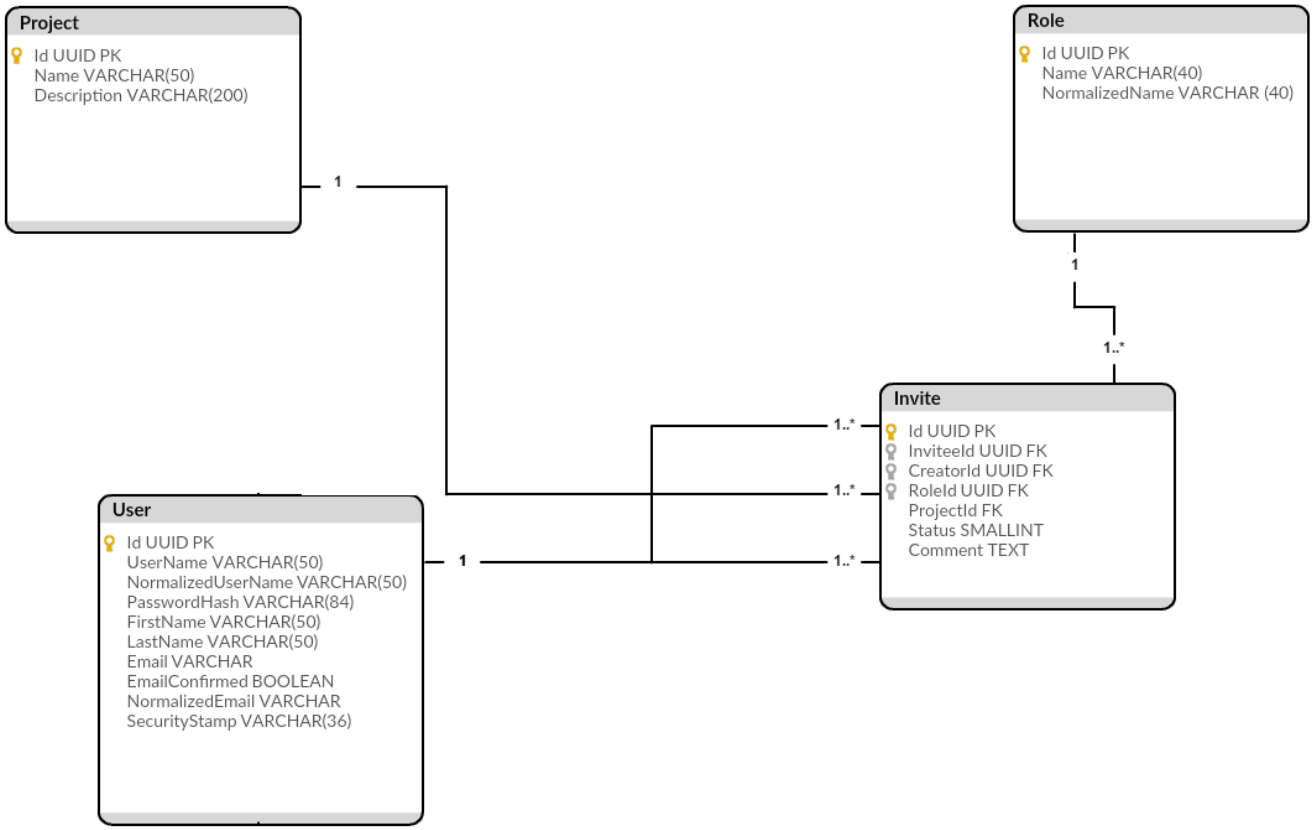


Рисунок 3.2 – Відношення таблиць «User», «Invite», «Role», «Project»

Для збереження бінарних даних створено таблицю «Attachment». Файли можуть бути прикріплені як до вимог так й до задач і для економії місця та скорочення часу очікування надається можливість обрати вже з завантажених файлів, отже, маємо відповідні розв’язочні таблиці зв’язку «багато до багатьох» «RequirementAttachment» та «TaskAttachment».

При написанні програми використовувалися спеціальні готові бібліотеки для Arduino IDE: бібліотека для роботи з RFID-зчитувачем, бібліотека для роботи з LCD - дисплеєм і бібліотека для роботи з I2C-інтерфейсом.

Для можливості управління платою Arduino за допомогою протоколу Bluetooth вибрали додаток Bluetooth Terminal для мобільної операційної платформи Android. За допомогою цієї програми користувач може як

відправляти команди на плату Arduino, так і приймати від неї дані. Основне вікно програми і приклад обміну даними представлені на рисунку 3.3.

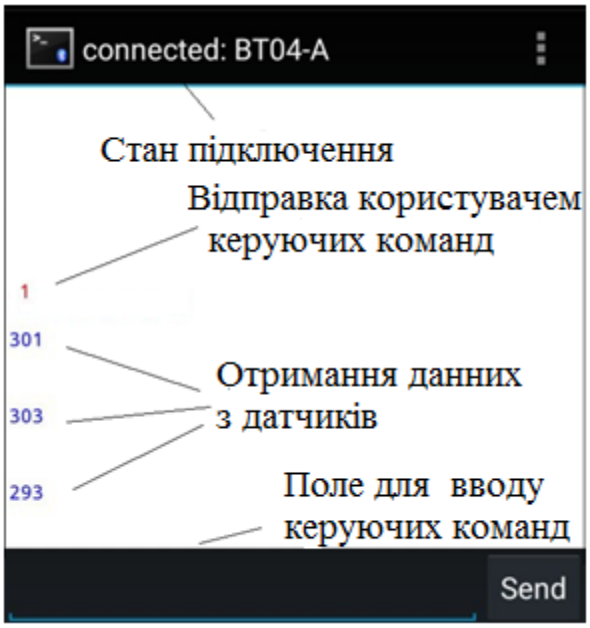


Рисунок 3.3. – Вікно програми Bluetooth Terminal для обміну даними між пристроєм користувача і модулем HC-05 по протоколу Bluetooth

За допомогою Bluetooth-модуля і цього додатка можливе підключення мобільного телефону користувача до послідовного порту Arduino, який ініціалізується функцією Serial.begin(). У дужках даної функції вказується швидкість обміну даними по порту, найчастіше це 9600 біт / С. Підключившись до послідовного порту, користувач може бачити дані, які Arduino виводить в послідовний порт, наприклад дані з датчиків. І у зворотний бік: користувач може сам відправити дані по послідовному порту, а Arduino їх вважає і, в залежності, від інформації, що надійшла, виконає ту чи іншу дію.

Реалізація управління платою Arduino по Bluetooth у функції Void loop () виглядає наступним чином:

if (Serial.available () > 0) / / якщо в послідовний порт щось прийшло

{

val = Serial.read (); / / зчитуємо дані, що прийшли в порт, і записуємо їх в змінну

```
if (val == '1') //якщо прийшла цифра 1
{
digitalWrite (Relay, LOW); / / спрацьовує реле
}
```

Варто відзначити, що відправка керуючих команд здійснюється шляхом відправки однієї з цифр від 0 до 10. Для проектованої системи встановили наступні співвідношення: «1» - задіяти реле 1 (відключити подачу газу); «2» - задіяти реле 1,4 (відновити подачу газу, відключити сигналізацію); "3"- задіяти реле 3 (відключити подачу води); "4" - задіяти реле 3,4 (відновити подачу води, відключити сигналізацію); «5» — задіяти реле 4 (відключити сигналізацію при виявленні загоряння); «6» — поставити систему на охорону (включити сигналізацію шляхом задіяння реле 4 в разі спрацьовування датчика відкриття); «7» - зняти систему з охорони і/або відключити сигналізацію шляхом задіяння реле 4.

Номери реле збігаються з відповідними висновками IN1, IN2, IN3, IN4 на обраному модулі чотириканального реле.

3.2 Розроблення вимог до програмного забезпечення для вирішення задачі

Серверна частина виконана у трьохшаровій архітектурі. Розберемо реалізацію кожного шару.

Шар доступу до даних виконано з використанням таких шаблонів як UnitOfWork та Repository [43] . Шаблон Repository забезпечує роботу з даними БД, наприклад, вибріка, додавання, оновлення, видалення. Під кожну сутність створюється свій репозиторій. Для перетворення реляційних даних (дані із БД) у об’єкти використовується Entity Framework Core. Він надає можливість перетворення C# лямбда-виражень у SQL запити, що полегшує процес розробки.

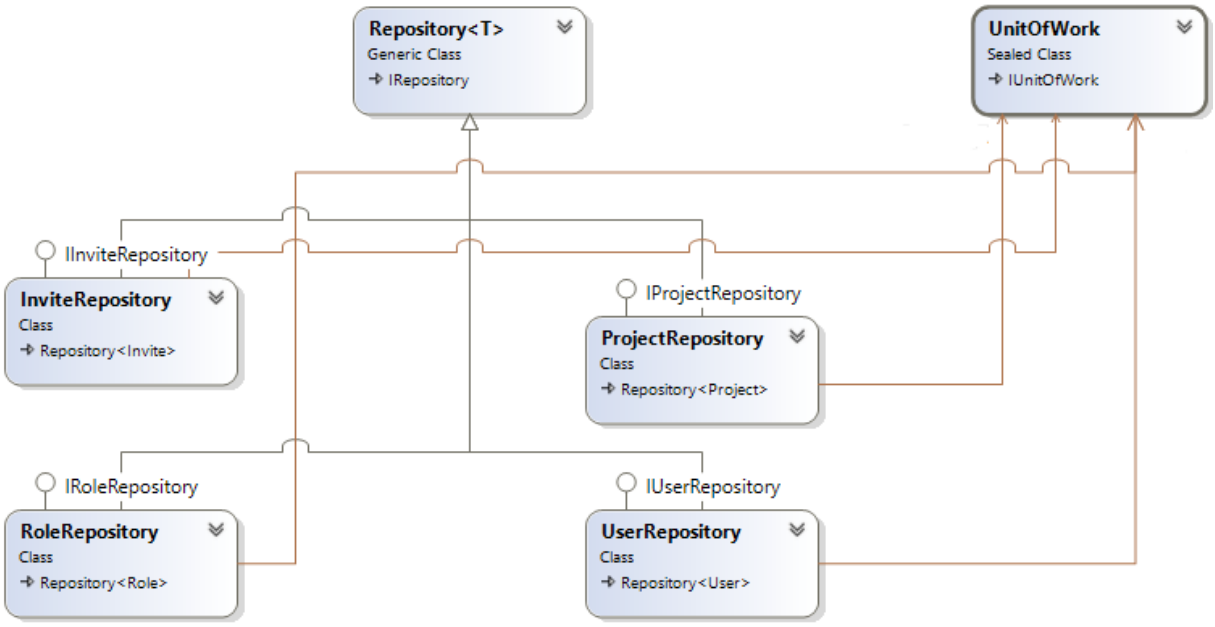


Рисунок 3.4 – Діаграма класів UnitOfWork та Repository

Шаблон UnitOfWork виконує роль контексту взаємодії з БД. В нашій серверній частині, під контекстом слід розуміти проміжок часу від часу надходження запиту до його обробки (час відправлення відповіді). Тобто, контекст існує в цьому часовому проміжку часу та є індивідуальним для кожної сесії запит-відповідь. Він агрегує в собі усі репозиторії, тобто, надає можливість виконати операції виборки, створення, редагування та видалення даних для будь-якої сутності, а потім після виклику методу SaveChanges, що також є членом даного класу, при необхідності одним чи декількома запитами зафіксувати зміни.

Варто відзначити, що метод SaveChanges підтримує асинхронну модель взаємодії з використанням CancellationToken, призначений для відміни дії, якщо це можливо, користувача в контексті виконання.

Шар бізнес-логіки відповідає за такі основні операції як перевірка прав доступу, перевірку надісланих даних у відповідності з бізнес-правил та взаємодії між шарами презентації та доступу до даних.

Під перевіркою прав слід розуміти процес, який визначає чи може користувач здійснювати ті чи інші дії. Наприклад, користувач маю типову роль

«Замовник», якщо він здійснить редагування задачі, то отримає помилку, оскільки він не має на це прав[44].

Під перевіркою даних у відповідності з бізнес-правилами слід розуміти процес, який визначає чи не порушують отримані дані із шару презентації бізнес-правилам. Наприклад, користувач хочу зареєструватися в системі, у поле «Username» ввів більше 20-ти символів, то він отримає помилку, про те що допускається до 20 символів для даного поля.

Кожен клас, який призначен для комунікації з шаром презентації має закінчення «Manager». Дані сутності інкапсулюють роботу з шаром доступу до даних, та виконують вищезгадані операції. Також, за необхідністю, виконує конвертацію сутностей. Наприклад, є сутність «User», що має поле «PasswordHash», користувач не повинен його отримати, тому для цього вводиться сутність «UserInfo», що не містить дане поле, а Manager конвертує із «User» у «UserInfo» та віддає його шару презентації.

Шар презентації виконано за допомогою ASP .NET Core MVC з використанням Web Api. Раніше Microsoft диференціювало Web Api та MVC на два фреймворки: ASP .NET WebApi та ASP .NET MVC, відповідно, зараз же, маємо один фреймворк ASP .NET Core MVC, який поєднав два попередні фреймворки.

Для побудови Web Api використовувалася REST архітектура. Використовуємо чотири головні операції (ще їх називають «action verbs» або «HTTP verbs») GET, POST, PUT, DELETE. Розглянемо їх призначення:

- GET – використовується для операцій отримання даних;
- POST – використовується для операцій створення даних;
- PUT – використовується для операцій зміни даних;
- DELETE – використовується для операцій видалення даних.

За замовчуванням, URL складається із IP, далі номер порту, що відокремлен двокрапкою, потім сегмент з назвою «api», далі ім’я контролера, для визначення який метод викликати використовуються «action verbs», за необхідності створюється ще один сегмент після назви контроллера. Пізніше,

після випуску першої версії системи буде куплено DNS ім’я, що замінить IP адресу та номер порту.

Усі контроллери, що створюються наслідуються від BaseController, який в свою чергу наслідується від Controller, який поставляється у фреймворці ASP .NET Core MVC. Створили базовий контролер, щоб винести туди всю загальну логіку для всіх дочірніх контролерів.

За замовчуванням, усі користувачі повинні бути автентифікованими у системі – для цього використовується атрибут «AuthorizeAttribute», який застосовано до базового контролера, для доступу до деяких методів не автентифікованим користувачам використовується атрибут «AllowAnonymousAttribute».

До базового контроллеру застосовано ще два основних атрибути «RouteAttribute» та «HandleExceptionFilterAttribute». Перший використовується для задання шаблону маршруту, в нашому випадку, за замовчуванням, це «api/[controller]». Другий використовується для обробки усіх помилок, що можуть статися при обробці запиту. Якщо не використовувати його і виникла помилка при запиті, буде повернено 500 Internal Server Error, що не є достатньо інформативним для користувача, тому завдяки цьому атрибуту, повертаємо 400 Bad Request, що містить у тілі відповіді («Response Body») опис помилки.

Для автентифікації використовуються токени. Даний тип автентифікації реалізовано за допомогою JSON Web Token[45].

JSON Web Token (JWT) – це безпечний URL-засіб репрезентації інформації користувача («claims»), яку необхідно передати між двома сторонами [26]. Інформація в JWT кодується як JSON об’єкт, який є являє собою JSON Web Signature (JWS) структуру чи як відкритий текст («plaintext») з шифруванням JSON Web Encryption (JWE) структури, що здійснює цифровий підпис інформації користувача.

Для роботи з JWT токенами використовується бібліотека Microsoft.AspNetCore.Authentication.JwtBearer, яка надає можливість створення токенів з вибором шифрування, назначення видавника тощо[46].

При створенні веб-форми для горизонтального масштабування постає питання синхронізації сесій. Одна з головних переваг використання токенів це те, що вони не зберігають стан (stateless). Цим самим токени полегшують процес горизонтального масштабування.

Для впровадження таких функцій як реєстрація, додавання до ролі та інше використовується бібліотека ASP .NET Core Identity, що має реалізацію цих та інших функцій. ASP .NET Core Identity надає вбудовану в ASP .NET систему автентифікації та авторизації. Дана система надає можливість користувачам створювати облікові записи, аутентифікуватися, керувати обліковими записами або використовувати для входу у систему облікові записи зовнішніх провайдерів таких як Facebook, Google, Microsoft, Twitter та інших. Дана бібліотека пропонує рішення, яке надає роботу з БД через EF Core, але воно не достатньо підходило нам по архітектурі, тому перевизначаємо необхідні інтерфейси з використанням нашої реалізації UnitOfWork.

ASP .NET Core має вбудований IoC-контейнер, що надає можливість ставити у відповідність абстракцію та реалізацію з вибором стратегії життєвого циклу об’єкта. Виділяють три основні стратегії[47].:

- transient – на кожен запит до контейнеру створюється об’єкту;
- scoped – на кожен запит до контейнеру в рамках однієї сесії створюється один об’єкт;
- singleton – об’єкт створюється лише один раз.

В нашому випадку зазвичай користоємося стратегію «scoped». Наші менеджери, контексти до БД існують в рамках запит-відповідь. Тобто на кожен запит, що надходить створюються за необхідністю менеджери та контекст до БД.

Веб-додатки ASP .NET розгорталися на веб-серверах IIS. Але, оскільки, ASP .NET Core має кросплатформену природу, виникла необхідність відв’язати ASP .NET Core від IIS та від Windows в цілому. На даний момент ASP .NET Core підтримує розгортання додатку на стандартних веб-серверах IIS та IIS Express, також надає можливість запускати додатки без IIS в рамках власного

процесу за допомогою двох додаткових HTTP-серверів, котрі йдуть в комплекті з ASP .NET Core:

– Microsoft.AspNetCore.Server.WebListener (чи просто WebListener);

– Microsoft.AspNetCore.Server.Kestrel (чи просто Kestrel).

WebListener працює лише на платформі Windows, а Kestrel є кросплатформеним.

Ми робимо акцент на кросплатформеності, оскільки, це надає широкий вибір ОС під якими можна розгорнути сервер та за статистикою на 2017 рік 66.7% серверів розгорнені на Unix-подібних системах [48].

Рекомендованими характеристиками комплексу програмно-технічного забезпечення:

А) Для серверу

- процесор Intel Core i5 з тактовою частотою не менше 2.5 ГГц;
- об’єм оперативної пам’ять від 16 ГБ;
- наявність 1 ГБ вільного місця на жорсткому диску;
- наявність відеокарти;
- операційна система Windows Server 2012R2 та старше;
- встановлений .NET Core 1.1.0;
- встановлений PostgreSQL починаючи з версії 9.6.

Б) Для шини повідомлень

- процесор Intel Core i5 з тактовою частотою не менше 2.5 ГГц;
- об’єм оперативної пам’ять від 16 ГБ;
- наявність 4 ГБ вільного місця на жорсткому диску;
- наявність відеокарти;
- операційна система Windows Server 2012R2 та старше;
- встановлений RabbitMQ починаючи з версії 3.6.2.

В) Для настільного клієнта

- процесор Intel Core i3 з тактовою частотою не менше 1.8 ГГц;
- об’єм оперативної пам’ять від 4 ГБ;
- наявність 256 МБ вільного місця на жорсткому диску;

- наявність відеокарти;
- операційна система Windows 7 та старше;
- встановлений .NET Framework 4.6.2.

Г) Для мобільного клієнта

- об’єм оперативної пам’яті від 2 ГБ;
- наявність 128 МБ фізичного вільного місця;
- операційна система iOS 10 чи Android 7 та старше;

Д) Для веб клієнту

- процесор Intel Core i3 з тактовою частотою не менше 1.8 ГГц;
- об’єм оперативної пам’яті від 2 ГБ;
- наявність відеокарти;
- наявність браузера з підтримкою WebSocket та ECMAScript 6.

3.3 Проектування програмного забезпечення для вирішення задачі

Використовуючи раніше вибране апаратне забезпечення, зібрали модель спроектованої системи безпеки "Розумного будинку" (рисунок 3.5).

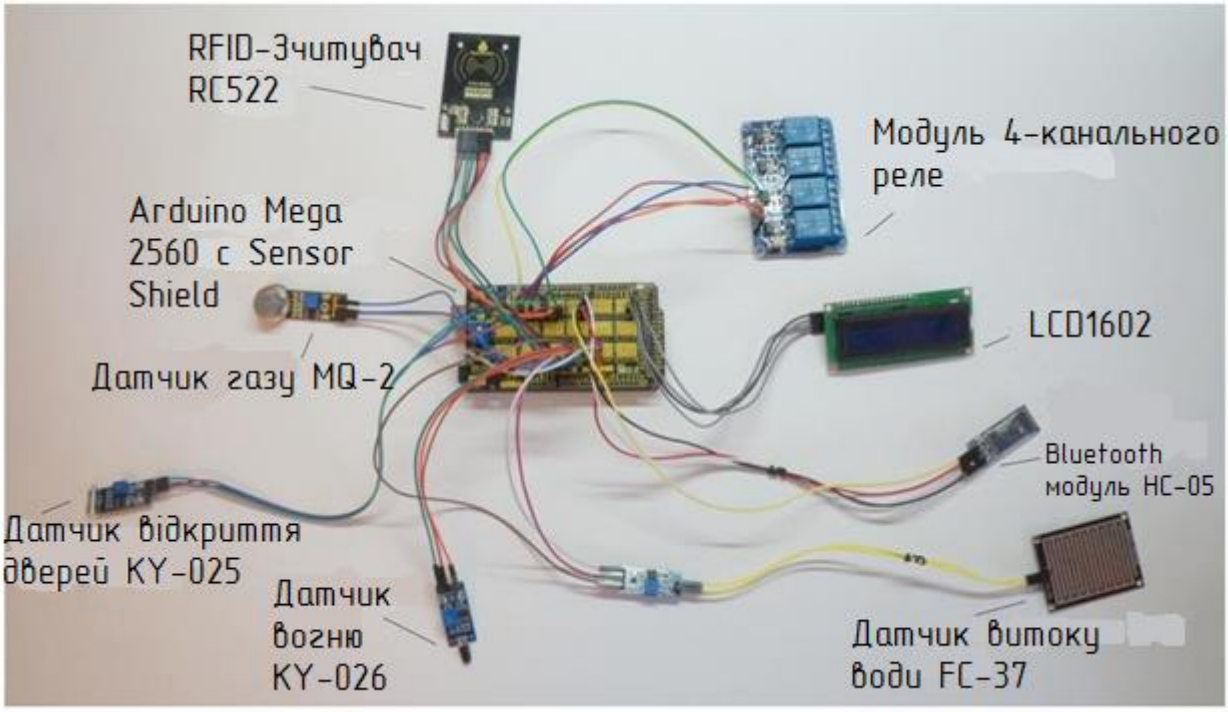


Рисунок 3.5. – Зібрана модель проектованої системи

Для зручності збірки використовували розширення для плати Arduino Mega 2560, так зване Sensor Shield[49]. Дане розширення дозволяє спростити процес підключення до плати великої кількість датчиків та інших електронних модулів, не використовуючи макетну плату (рисунок 3.6).

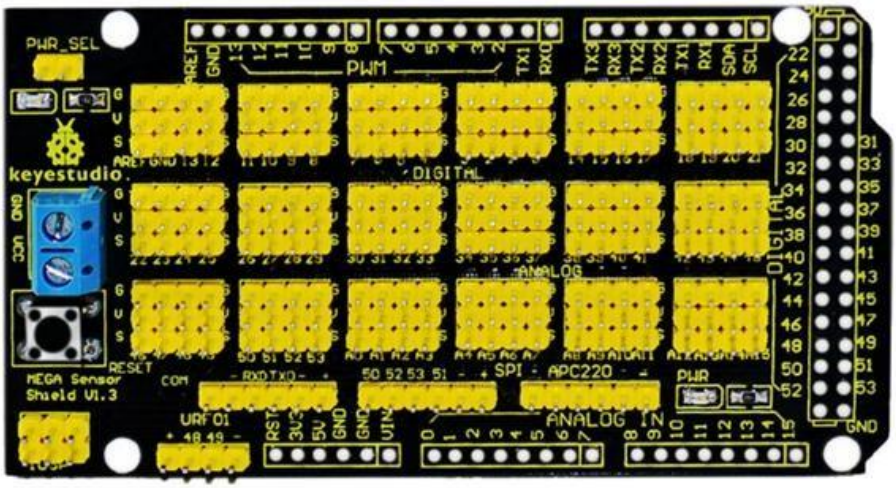


Рисунок 3.6 – Розширення Sensor Shield для плати Arduino

В якості виконавчих механізмів для демонстрації роботи спроектованої системи були обрані наступні пристрої (рисунок 3.7): електромагнітний замок для системи контролю та управління доступом, електромагнітний клапан для системи захисту від протікання води.

Для демонстрації системи захисту від витоків газу вибрали вентилятор з системного блоку комп'ютера, щоб показати інший можливий варіант роботи системи: включення витяжної вентиляції при скупченні небезпечного обсягу газу в приміщенні. Всі вибрані виконавчі пристрої працюють від напруги від 9 до 12 В, а їх робота управляється блоком 4-х канального реле.

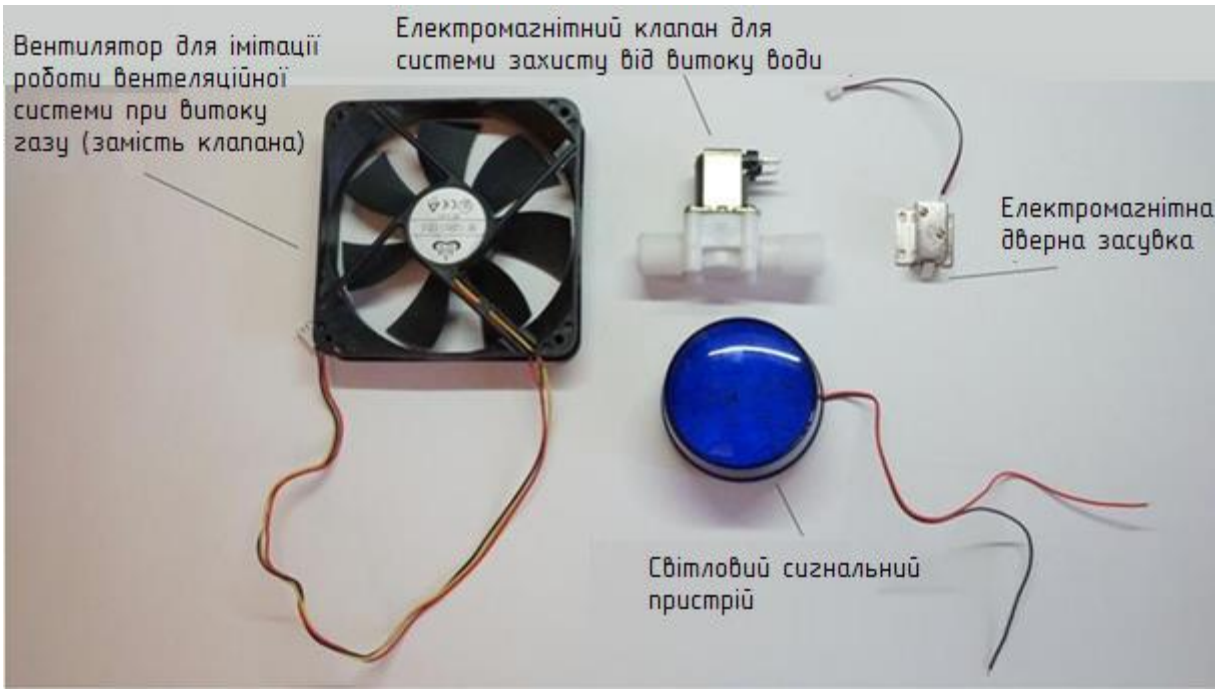


Рисунок 3.7. – Виконавчі механізми для демонстрації працездатності спроектованої системи

На Рисунок 3.8 представлена реалізація виведення інформаційних повідомлень при будь-якій події в системі, а саме: при фіксації будь-якої аварійної події, при зчитуванні незареєстрованої RFID-мітки, при включенні користувачем будь-якого реле, при активації режиму охорони, при відкритті вхідних дверей в режимі охорони.

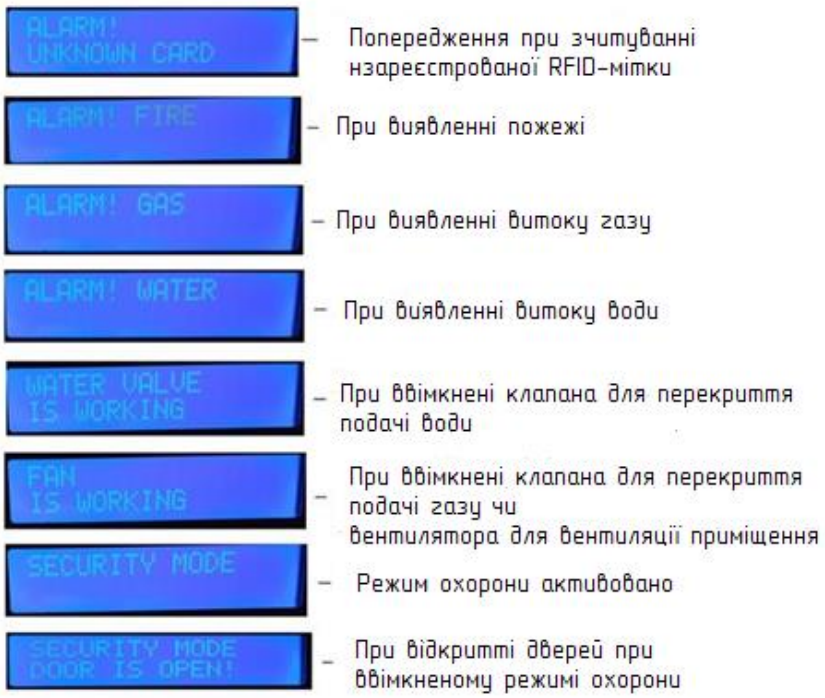


Рисунок 3.8 – Виведення інформаційних повідомлень на LCD-дисплей

3.4 Висновки

У середовищі розробки Arduino IDE склали програмний код, що реалізує розроблений раніше алгоритм роботи проектованої системи

Програма складена на мові C / C++. При написанні програми використовувалися спеціальні готові бібліотеки для Arduino IDE: бібліотека для роботи з RFID-зчитувачем, бібліотека для роботи з LCD - дисплеєм і бібліотека для роботи з I2C-інтерфейсом.

Використовуючи раніше вибране апаратне забезпечення, зібрали модель спроектованої системи безпеки "Розумного будинку".

Для зручності збірки використовували розширення для плати Arduino Mega 2560, зване Sensor Shield. Дане розширення дозволяє спростити процес підключення до плати великої кількість датчиків та інших електронних модулів, не використовуючи макетну плату.

4 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ

4.1 Програмна (апаратно-програмна) реалізація

При розробці системи використовувалися такі підходи та принципи: ООП, SOLID, DRY, KISS, YAGNI та coding guidelines, які рекомендує Microsoft [30].

ООП (об’єктно-орінтоване програмування) – методологія програмування, що заснована на представленні програми у вигляді сукупності об’єктів, кожен з яких являє собою екземпляр деякого класу, а класи утворюють ієрархії наслідування. Можна виділити три основних парадигми ООП:

- інкапсуляція – властивість системи, яка надає можливість об’єднувати дані та методи, що працюють з ними, в класі та приховати деталі реалізації від користувача;
- наслідування – властивість системи, яка надає можливість описати новий клас, що базується на існуючому з частковою або повною функціональністю. Клас, від якого наслідуються, називається базовим, батьківським чи суперкласом. Новий клас – нащадком, спадкоємцем, дочірнім чи похідним;
- поліморфізм – властивість системи, яка надає можливість використовувати об’єкти з однаковими інтерфейсами без інформації про тип та внутрішню структуру об’єкта.

SOLID – являє собою акронім для набору практик проектування програмного коду, побудові гнучкої та адаптивної програми. Сам акронім складається з перших літер назв SOLID-принципів:

- Single Resposibility Principle (Принцим єдиного обов’язку);
- Open/Closed Principle (Принцип відкритості/закритості);
- Liskov Substitution Principle (Принцип підстановки Лісков);
- Interface Segregation Principle (Принцип поділу інтерфейсів);
- Dependency Inversion Principle (Принцип інверсій залежностей).

Принцип єдиного обов’язку – у кожного класу повинна бути тільки одна причина для зміни. Під обов’язком тут слід розуміти набір функцій, які виконують єдину задачу. Суть цього принципу полягає в тому, що клас повинен виконувати одну єдину задачу. Весь функціонал класу повинен бути цілісним та мати високу зв’язність (high cohension).

Принцип відкритості/закритості – сутності програми повинні бути відкритими для розширення, але закритими для зміни. Суть цього принципу полягає в тому, за всі її наступні зміни повинні бути реалізовані за допомогою додавання нового коду, а не зміною вже існуючого.

Принцип підстановки Лісков – повинна бути можливість замість базового типу підставити будь-який його підтип. Наприклад, клас S може вважатися підкласом T, якщо заміна T на об’єкти S не призведе до зміни роботи програми.

Принцип поділу інтерфейсів – клієнти не повинні примусово залежати від методів, якими не користуються. При порушенні цього принципу клієнт, який використовує деякий інтерфейс з усіма його методами, залежить від методів, якими не користується, тому він буде сприйнятливим до змін в цих методах.

Принцип інверсій залежностей – модулі верхнього рівня не повинні залежити від модулей нижнього рівня. Обидва повинні залежити від абстракцій.

DRY (не повторюйся, Don’t Repeat Yourself) – цей принцип полягає в тому, что потрібно уникати повторень одного й тож самого коду.

KISS (не ускладнюй, Keep It Simple, Stupid) – цей принцип полягає в тому, що потрібно робити максимально просту та зрозумілу архітектуру, застосовувати шаблони проектування та не винаходити велосипед.

YAGNI (це вам не знадобиться, You Ain’t Gonna Need It) – цей принцип полягає в тому, що необхідно реалізовувати тільки поставлені задачі та відмовитися від надлишкового функціоналу.

При розробці використовувалися code guidelines, які рекомендує Microsoft. Наприклад, використовувався camelCase, усі інтерфейси починаються з префіксу «I», назви властивостей класу є іменниками[50].

4.2 Результати експериментів (тестування) та їх аналіз

Під час мануального тестування було перевірено основні функції системи. Нижче наведено перелік випробувань та отриманий результат.

Таблиця 4.1 – Тестовий сценарій «Автентифікація у системі»

Назва	Тест для перевірки RFID автентифікації у системі	
Use case	Автентифікація користувача у системі.	
Дія	Очікуваний результат.	Результат тесту
Передумова		
Увімкнути живлення Arduino Mega 2560	Діод, автентифікації RFID увімкнутий	Пройдений
Кроки тесту		
Підносим мітку до рідера з ключем 16909060	Сигналізація не спрацювала,	Пройдений
Відчиняємо двері	Виведено надпис ("DOOR IS OPEN!");	Пройдений

Таблиця 4.2 – Тестовий сценарій «Спроба зчитування хибної мітки користувача у системі»

Назва	Тест для перевірки автентифікації у системі	
Use case	Спроба автентифікації користувача з хибною міткою.	
Дія	Очікуваний результат	Результат тесту
Передумова		
Живлення увімкнуте	Діод, автентифікації RFID увімкнутий	Пройдений
Підносим мітку до рідера з ключем 18009060	Виводиться напис «ALARM! UNKNOWN CARD».	Пройдений
«ALARM! UNKNOWN CARD».	Спрацювала сигналізація	Пройдений

Кінець Таблиці 4.2 – Тестовий сценарій «Спроба зчитування хибної мітки користувача у системі»

Спробуєм відкрити замок	Замок зачинено	Пройдений

Таблиця 4.3 – Тестовий сценарій «Відімкненя дверей без мітки RFID »

Назва	Тест для перевірки автентифікації у системі.	
Use case	Відімкненя дверей без мітки RFID.	
Дія	Очікуваний результат	Результат тесту
Передумова		
Живлення увімкнуте	Діод, автентифікації RFID увімкнутий	Пройдений
Відчиняємо двері ключем	("DOOR IS OPEN!")	Пройдений
Заходим у будинок	Спрацювала сигналізація	Пройдений
Потрапляння води на датчик	«ALARM! WATER».	Пройдений
«ALARM! WATER».	«WATER VALVE IS WORKING».	Пройдений

Таблиця 4.4 – Тестовий сценарій «Витоку газу»

Назва	Тест для перевірки витоку газу	
Use case	Моделювання ситуації витоку газу	
Дія	Очікуваний результат	Результат тесту
Передумова		
Перевищена концентрація газу у повітрі	«ALARM! GAS».	Пройдений
«ALARM! GAS».	«FAN IS WORKING».	Пройдений
«FAN IS WORKING».	Спрацювала сигналізація	Пройдений
Повторна перевіка витоку газу	Сигналізація вимкнулась, клапан закритий	Пройдений

Таблиця 4.5 – Тестовий сценарій «Взяття квартири під охорону»

Назва	Тест взяття квартири під охорону	
Use case	Моделювання ситуаці взяття квартири під охорону	
Дія	Очікуваний результат	Результат тесту
Передумова		
За допомогою телефону підєднуємось до bluetooth модуля вводим пароль (ErhfYf6tM5)	Аутентифікацію пройдено	Пройдений
Заходим у додаток bluetooth terminal hc-05 І вводимо змінну 6	("SECURITY MODE")	Пройдений
За допомогою телефону підєднуємось до bluetooth модуля вводим пароль (ErhfYf6tM5)	Аутентифікацію пройдено	Пройдений
Заходим у додаток bluetooth terminal hc-05 І вводимо змінну 7	Квартиру знято з охорони	Пройдений

Таблиця 4.6 – Тестовий сценарій «Займання»

Назва	Тест для перевірки датчика вогню	
Use case	Моделювання ситуації займання	
Дія	Очікуваний результат	Результат тесту
Передумова		
Підносим вогонь до датчика	"ALARM! FIRE"	Пройдений
"ALARM! FIRE"	Спрацювала сигналізвція	Пройдений

4.3 Оцінка ефективності моделі та методів для вирішення задачі

Модульні тести (Unit-тести) надають можливість швидко та автоматично протестувати окремі ділянки коду незалежно від іншої частини програми. При

правильному написанні модульних тестів вони в повній мірі можуть покрити більшу частину коду додатку. Більшість юніт-тестів мають наступний ряд ознак: тестування невеликих ділянок коду («юнітів»), тестування в ізоляції від іншого коду, тестування лише загальнодоступних кінцевих точок, автоматизація тестування. Розглянемо кожну більш детально.

При створенні модульних тестів обираються невеликі частни коду, які необхідно протестувати. Як правило, ділянка коду, яка перевіряється повинна бути менше класу, а у більшості випадків тестується окремий метод класу. Завдяки цьому написання модульних тестів займає небагато часу.

При тестуванні важливо ізолювати перевіряємий код від іншої програми з якою він взаємодіє, щоб потім чітко визначити можливість помилок саме в цій ділянці ізолюваного коду. Це полегшує та підвищує контроль над окремими компонентами програми.

Невеликі зміни в класу можуть призвести до провалу багатьох модульних тестів, оскільки реалізація класу змінилася. Щоб уникнути цього, при написанні юніт-тестів обмежуються тільки загальнодоступними кінцевими точками, що дозволяє ізолювати модульні тести від багатьох деталей внутрішньої реалізації.

Написання модульних тестів для невеликих ділянок коду призводить до того, шо кількість цих юніт-тестів досягає великої кількості. Якщо процес отримання результату та виконання тестів не автоматизован, це може призвести до зниження продуктивності під час розробки. Тому дуже важливо, щоб модульні тести являли собою просте рішення, що надає інформацію чи пройден тест чи ні. Для автоматизації процесу розробники зазвичай використовують готові фреймворки.

Розробка через тестування (Test-Driven Development, TDD) – це підхід, який застосовують при розробці. Його головна ідея полягає в тому, що спочатку пишуть модульні тести, а потім вже програмний код, якого достатнь для виконання цих тестів.

Використання TDD дозволяє знизити кількість потенціних помилок у програмі. Створюючи модульні тести до початку написання коду, тим самим

описуємо спосіб поведінки майбутніх компонентів, не зв’язуючи себе при цьому з конкретною реалізацією цих перевіряємих компонентів. Таким чином, тести допомагають оформити та описати API майбутніх компонентів.

Моделі тестів Arrange-Act-Assert являє собою не лише особливість тестування в Visual Studio, а й цілу парадигму тестування:

- arrange – підготовка середовища, в якому виконується код;
- act – тестування коду
- assert – переконуємося, що результат тесту саме той, який очікували.

Під час тестування досить часто використовуються фіктивні об’єкти (mock-об’єкти). Mock-об’єкт – це тип об’єктів, які реалізують задані аспекти програмного середовища, яке моделюється. Фіктивний об’єкт являє собою лише конкретну фіктивну реалізацію інтерфейсу, призначену виключно лише для тестування взаємодії та щодо якого висловлюється твердження.

Для написання модульних тестів обрали фреймворк NUnit. Для позначення класу, який призначено для юніт-тестів використовують атрибут TestFixtureAttribute. Метод, який являє собою виконання самого тесту декорують атрибутом TestAttribute. Також є можливість позначити метод, задача якого виконати базові налаштування середовище, для цього метод позначають атрибутом SetupAttribute й зазвичай називають Setup. На рисунку 4.1 наведено результат виконання тестів для RequirmentController.

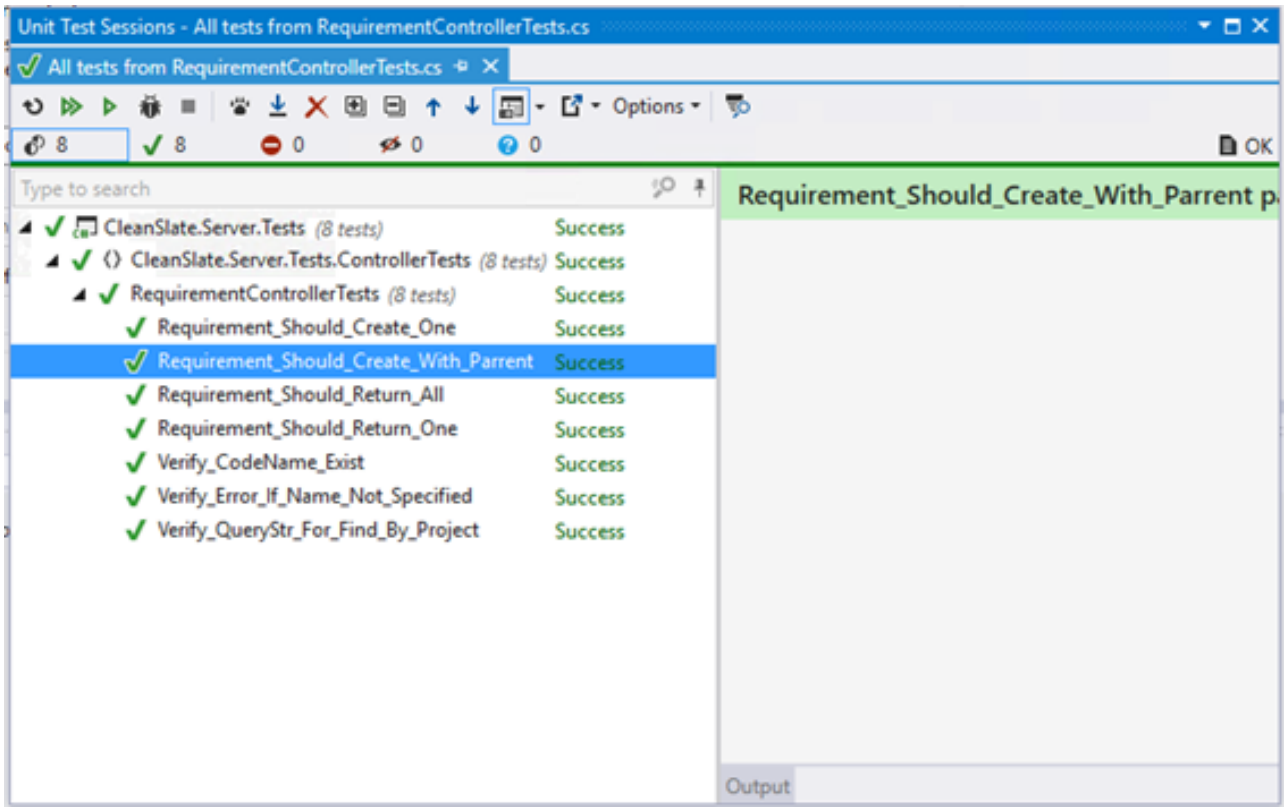


Рисунок 4.1 – Результат виконання модульних тестів

4.4 Висновки

При розробці системи використовувалися такі підходи та принципи: ООП, SOLID, DRY, KISS, YAGNI та coding guidelines, які рекомендує Microsoft.

ООП (об’єктно-орінтоване програмування) – методологія програмування, що заснована на представленні програми у вигляді сукупності об’єктів, кожен з яких являє собою екземпляр деякого класу, а класи утворюють ієрархії наслідування.

При розробці використовувалися code guidelines, які рекомендує Microsoft. Наприклад, використовувався camelCase, усі інтерфейси починаються з префіксу «I», назви властивостей класу є іменниками тощо.

Під час мануального тестування було перевірено основні функції системи.

Модульні тести (Unit-тести) надають можливість швидко та автоматично протестувати окремі ділянки коду незалежно від іншої частини програми. При

правильному написанні модульних тестів вони в повній мірі можуть покрити більшу частину коду додатку.

Для написання модульних тестів обрали фреймворк NUnit. Для позначення класу, який призначено для юніт-тестів використовують атрибут TestFixtureAttribute. Метод, який являє собою виконання самого тесту декорують

ВИСНОВКИ

Провівши дослідження, можемо зробити наступні висновки:

"Розумний будинок" являє собою житлове або нежитлове (не використовується для проживання) приміщення, оснащене засобами обчислювальної техніки та управління, що підтримують інформаційні технології, які здатні діяти про-активно з метою задоволення потреби людини в комфортному і безпечному проживанні.

Застосування комплексу засобів автоматизації та інформаційних технологій «Розумного будинку» дозволяє забезпечити безпечну і ефективну експлуатацію, запобігти ризику нанесення шкоди, що приводить до відмови або аварії обладнання інженерних комунікацій, систем енергозабезпечення, газопостачання, вентиляції, опалення, холодного і гарячого водопостачання, водовідведення, систем зв'язку, охоронних та інших систем будівель, і споруд.

До основних підсистем «Розумного будинку» відносяться системи: освітлення, клімат-контролю, безпеки та моніторингу, комунікаційних мереж і мультимедіа.

Ефективна і багатофункціональна система "Розумного будинку" включає в себе різноманітні датчики, що реєструють і передають параметри середовища, і іншу важливу інформацію. Датчики автоматизації являють собою конструктивно автономний самостійний пристрій, що змінює свій сигнал відповідно відстежуваному параметру.

Виконавчі пристрої призначені для перетворення керуючих (командних) сигналів в регулюючі впливи на об'єкт управління. Сигнальна сирена, сервоприводи, що перекривають подачу води або газу, відкривають вентиляційні вікна, різні силові реле і таймери - відносяться до виконавчих пристроїв.

Центральний пристрій "Розумного будинку" координує всі його функції і управляє всіма його компонентами.

Нами розглянуто основні фактори, що впливають на безпеку інформації «Розумного будинку», побудованого на основі готових систем.

Таким чином розроблена система суб'єктивних і об'єктивних факторів, що впливають на систему «Розумного будинку». Надалі ця система буде використана для аналізу загроз «розумного будинку».

У системах захисту від протікання води і витоків газу ключову роль відіграють виконавчі механізми, які відсікають подачу, відповідно, води або газу.

Датчик протікання води розміщується в тих приміщеннях і місцях, в яких можливе протікання води: під ванною, поруч з пральною машиною і так далі.

Система захисту від витоків газу працює за принципом, схожим з системою захисту від протікання води і встановлюється в приміщеннях з газовим обладнанням: котельні, кухонні кімнати. Газоаналізатор, тобто датчик газу, фіксує витік газу, якщо його концентрація в повітрі перевищує деяке порогове значення

Як приклад для розгляду вибрали модель дверного замка SHS-P718 від компанії Samsung.

На ринку «розумних будинків» одним з лідерів є компанія Rubetek. Вона пропонує як окремі "розумні" пристрої, так і готові комплекти, один з яких називається «управління та безпека». До його складу входять: модуль управління, датчик протікання, датчик відкриття, датчик диму. Однак користувач може зібрати свою власну систему з будь-яких вподобаних йому пристроїв.

Широке визнання на ринку охоронних систем отримала «розумна» сигналізація Ajax українського виробництва. Дана охоронна система складається з керуючого пристрою і набору датчиків.

Проектована система безпеки «Розумного будинку» повинна мати два режими роботи: «Охорона відключена» і «Охорона включена».

Проектована система безпеки "Розумного будинку" для роботи згідно з розробленим алгоритмом повинна мати в своєму складі ряд електронних

елементів: мікроконтролер, датчики для фіксації аварійних подій, комутуючі пристрої для підключення виконавчих механізмів, дисплей для виведення різної інформації, модуль для дистанційного керування системою користувачем.

В якості апаратно-програмної платформи проектованої системи була обрана Arduino. Дана платформа з відкритим вихідним кодом включає в себе серію плат на основі 8-бітних мікроконтролерів ATmega, сумісні з платами модулі для вирішення різних завдань, а також середовище розробки і налагодження програм Arduino IDE (Integrated Development Environment).

У середовищі розробки Arduino IDE склали програмний код, що реалізує розроблений раніше алгоритм роботи проектованої системи

Програма складена на мові C / C++. При написанні програми використовувалися спеціальні готові бібліотеки для Arduino IDE: бібліотека для роботи з RFID-зчитувачем, бібліотека для роботи з LCD - дисплеєм і бібліотека для роботи з I2C-інтерфейсом.

Використовуючи раніше вибране апаратне забезпечення, зібрали модель спроектованої системи безпеки "Розумного будинку".

Для зручності збірки використовували розширення для плати Arduino Mega 2560, зване Sensor Shield. Дане розширення дозволяє спростити процес підключення до плати великої кількість датчиків та інших електронних модулів, не використовуючи макетну плату.

При розробці системи використовувалися такі підходи та принципи: ООП, SOLID, DRY, KISS, YAGNI та coding guidelines, які рекомендує Microsoft.

ООП (об’єктно-орінтоване програмування) – методологія програмування, що заснована на представленні програми у вигляді сукупності об’єктів, кожен з яких являє собою екземпляр деякого класу, а класи утворюють ієрархії наслідування.

При розробці використовувалися code guidelines, які рекомендує Microsoft. Наприклад, використовувався camelCase, усі інтерфейси починаються з префіксу «I», назви властивостей класу є іменниками тощо.

Під час мануального тестування було перевірено основні функції системи.

Модульні тести (Unit-тести) надають можливість швидко та автоматично протестувати окремі ділянки коду незалежно від іншої частини програми. При правильному написанні модульних тестів вони в повній мірі можуть покрити більшу частину коду додатку.

Для написання модульних тестів обрали фреймворк NUnit. Для позначення класу, який призначен для юніт-тестів використовують атрибут TestFixtureAttribute. Метод, який являє собою виконання самого тесту декорують

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЬ

1. Grinter R. E., Edwards W. K. At Home with ubiquitous computing: Seven challenges. *Computer Science Laboratory Xerox Palo Alto Research Center:* Proceedings of Ubicomp., California, 22-24 apr. 2018. California, 2018. P.256-272.

2. Davidoff S., Lee M. K., Zimmerman J., Dey A. K. *Sociallyaware requirements for a smart home*: Proceedings of the International Symposium on Intelligent Environments., Pittsburgh, PA, 24 jan. 2019. Pittsburgh, PA, 2019. P. 41-44.

3. Cook, D. J., Youngblood M., Heierman E., Gopalratnam K., Rao S., Litvin, A., Khawaja, F.: *An agent-based smart home*: Proceedings of PerCom. Department of Computer Technology., Texas,12 feb. 2018. Texas, 2018 P. 521-524.

4. Проєктування систем автоматизації. URL: https://alterair.ua/avtomatizaciya/proyektyrovaniye-systemy. (дата звернення: 27.04.2022).

5. Crabtree, A., Rodden T., Hemmings T., Benford, S.: *Finding a place for ubicomp in the home*: in Proceedings of Ubicomp. School of Computer Science and IT, University of Nottingham., UK, 21 oct.2018. UK, 2018 P. 208-226.

6. Harper R. Inside the smart home., *Ideas, possibilities and methods:* Richard Harper Inside the smart home., New York,15 jan.2021. New York,2021 P.1-14.

7. F. Liu., H. Zhao.The Design of WIFI-Based Smart Home Communication Hardware Adapter: *Fifth International Conference Instrumentation Measurement, Computer, Communication and Control (IMCCC)*.Qinhuangdao, 5 oct 2017. Qinhuangdao, 2017 pp. 1193-1197.

8. Як розробити Розумний Дім самому?. URL: https://bron.ua/article/yak-zrobiti-rozumnij-dm-samomu/2. (дата звернення: 20.11.2021).

9. Maneesh R. Internet of Things with Raspberry Pi: Packt Publishing 30.04.2018. 248 с.

10. Budijono S., Andrianto J., Axis N.M. *Design and implementation of modular home security system with short messaging system: EPJ Web of Conferences*. 2019. Vol. 68, No 9. doi: 10.1051/epjconf/20146800025.

11. Технологія розумного будинку: як AI створює простір, комфортний для життя.URL: https://www.everest.ua/tehnologiya-rozumnogo-budynku-yak-ai-stvoryuye-prostirkomfortnyj-dlya-zhyttya/.(дата звернення: 13.03.2022).

12. Котунова., Д. Г. Огляд DIY елементів для систем «Smart Home» / Д. Г. Котунова, О. М. Павловський // XIII Науково-практична конференція студентів, аспірантів та молодих вчених «Погляд у майбутнє приладобудування», 13-14 травня 2020 р., м. Київ, Україна : збірник праць конференції. – Київ : КПІ ім. Ігоря Сікорського, 2020. – С. 35–38.

13. Bangali J., Shaligram A. Design and Implementation of Security Systems for Smart Home Based on GSM Technology: *International Journal of Smart Home*.2018 Vol.7, No.6. P.201-208.

14. Chitnis S., Deshpande N., Shaligram A. An Investigative Study for Smart Home Security: Issues, Challenges and Countermeasures. *Wireless Sensor Network*. 2020. Vol. 68, No 7. doi: 10.4236/wsn.2020.84006.

15. Choudhary V., Parab A., Bhapkar S., Jha N., Kulkarni Ms. Medha. Design and Implementation of Wi-Fi based Smart Home System, *International Journal Of Engineering And Computer Science*. 2016. Vol.5, No 6. PP.15852-15855.

16. Krishna M., V. Narasimaha N., K. Ravi Kishore Reddy., B. Rakesh., “Bluetooth Base Wireless Home Automation System Using FPGA”, *Journal of Theoretical and Applied Information Technology*. 2019. Vol.77, No 3. PP. 1992-8645.

17. Kumar A., Tiwari N. “Energy Efficient Smart Home Automation System”, *International Journal of Scientific Engineering and Research (IJSER). 2021*. Vol. 3, No 1. PP. 2347-3878.

18. Shirisha Tadoju., J. Mahesh. “Bluetooth Remote Home Automation System using Android Application”, *International Journal Of Advanced Technology and Innovative Research*. 2019. Vol.07, No 10. PP.1815-1818.

19. Table Of Contents -X10 MT10 Owner's Manual. URL: https://www.manualslib.com /manual/720184/X10-Mt10.html?page=2#manual.(дата звернення: 21.12.2021).

20. Протокол X10.URL: http::www.iq-home.ru/tech/x10.html.(дата звернення: 3.02.2022).

21. Honeywell Ademco TUXWIFIW Tuxedo .URL: https://www.jmac.com/Honeywell_Ademco_TUXWIFIW_p/honeywell-ademco-tuxwifiw.htm.(дата звернення: 21.12.2021).

22. H. Jiang, B. Liu and C. W. Chen, "Performance analysis for ZigBee under WiFi interference in smart home,"2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-6.

23. Adams C. E. Home area network technologies. *BT Technology Journal*.20.02.2020.N12. P.53–72.

24. Система контролю та управління доступом. URL**:** https://valtek .com.ua/ua/ system-integration/security-control-system/access-control/access-control-review.(дата звернення: 11.12.2021).

25. Розумні дверні замки: що це таке та як вибрати .URL:https://blog.allo.ua/ua/rozumni-dverni-zamki-shho-tse-take-ta-yak-vibrati_2021-10-40.(дата звернення: 14.12.2021).

26. Rubetek . URL: https://rubetek.by/.(дата звернення: 19.12.2021).

27. Ajax Security System.URL: https://ajax.systems/ua.(дата звернення: 21.12.2021).

28. Valtchev, D., & Frankov, I., & ProSyst Software AG. (2002). Service Gateway Architecture for a Smart Home. IEEE Communications Magazine, 126–132.

29. Сервіс-ороріентована архітектура IC.URL: https://studopedia.su/10_104529_servisorientirovannaya-arhitektura-is.html. .(дата звернення: 19.12.2021).

30. Arduino Mega 2560 Datasheet. URL: https://www.robotshop.com/media/files/pdf/arduinomega2560datasheet.pdf.

(дата звернення: 11.01.2022).

31. Specification for LCD Module 1602A-1 (V1.2). URL: https://www.openhacks.com/uploadsproductos/eone-1602a1.pdf. (дата звернення: 13.03.2022).

32. KY-026 Модуль датчика полум'я.URL: https://datasheetspdf.com/pdf/1402037/Joy-IT/KY-026/1. (дата звернення: 19.04.2022).

33. Датчик газу. URL: https://www.pololu.com/file/0J309/MQ2.pdf. (дата звернення: 23.04.2022).

34. Датчик витоку води FC37. URL:https://randomnerdtutorials.com/guide-for-rain-sensor-fc-37-or-yl-83-with-arduino/.(дата звернення: 25.04.2022).

35. Specification for MRFC522. URL: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf. (дата звернення: 13.03.2022).

36. DataSheet. URL: https://pdf1.alldatasheet.com/datasheet-pdf/view/112132/DALLAS/DS3231.html. (дата звернення: 14.03.2022).

37. Channel 5V Optical Isolated Relay Module. URL: http://www.handsontec.com/dataspecs/4Ch-relay.pdf. (дата звернення: 13.03.2022).

38. Channel 5V Optical Isolated Relay Module. URL: http://www.handsontec.com/dataspecs/4Ch-relay.pdf. (дата звернення: 13.03.2022).

39. HC-05-Bluetooth to Serial Port Module. URL: http://www.electronicaestudio.com/docs/istd016A.pdf. (дата звернення: 15.03.2022).

40. Котунова., Д. Г. Огляд DIY елементів для систем «Smart Home» / Д. Г. Котунова, О. М. Павловський // XIII Науково-практична конференція

студентів, аспірантів та молодих вчених «Погляд у майбутнє приладобудування», 13-14 травня 2020 р., м. Київ, Україна : збірник праць конференції. – Київ : КПІ ім. Ігоря Сікорського, 2020. – С. 35–38.

41. Протокол ZigBee: беспроводные технологии на службе «умного» URL: https://www.ferra.ru/review/smarthome/SmartHome-ZigBee.htm

42. Протокол X10: http::www.iq-home.ru/tech/x10.html

43. Adams C. E. Home area network technologies:*BT Technology Journal*.2017.17 jan. N 20(2), 53–72.

44. Tompros S.; Mouratidis N.; Draaijer M.; Foglar, A.; Hrasnica, H. *Enabling applicability of energy saving applications on the appliances of the home environment*. Qinhuangdao, 5 oct 2017. Qinhuangdao, 2017 pp. 1193-1197.

46. Dickson B. How to prevent your IoT devices from being forced into botnet bondage.URL:https://techcrunch.com/2016/08/16/how-to-prevent-your-iot-devices-from-beingforced-into-botnet-slavery/..(дата звернення: 19.12.2021).

47. Технологія «Розумний Дім»: майбутнє вже поруч.URL:http://elar.nung.edu.ua/bitstream/123456789/6141/1/6718p.pdf.(дата звернення: 19.12.2021).

48. ESP8266.URL:https://espressif.com/sites/default/files/documentation/ 0a-esp8266ex_datasheet_en.pdf. (дата звернення: 14.03.2022).

49. Ks0006 MEGA Sensor Shield .URL:https://wiki.keyestudio.com/Ks0006_MEGA_Sensor_Shield_V1.c. (дата звернення: 18.03.2021).

50. Is IoT Security a Ticking Time Bomb.URL:https://securityintelligence.com/is-iot-security-a-tickingbomb/..(дата звернення: 19.12.2021).

ДОДАТОК А

(обов’язковий)
Лістинг програмного забеспеченння

```
/Підключення LCD-дисплея #include <Wire.h>

#include <LiquidCrystal_I2C.h> LiquidCrystal_I2C lcd(0x27,16,2);


//Підключення RFID-СКУД #include <SPI.h>

#include <MFRC522.h> #define SS_PIN 53

#define RST_PIN 5

MFRC522 mfrc522(SS_PIN, RST_PIN);

unsigned long uidDec, uidDecTemp; //Для зберігання номера мітки в
десятковому форматі

int countRFID = 0; //Лічильник числа зчитувань RFID-карти

int relayDoor = 11; //Реле для керування ел.засувкою (далі - замком) bool
d = false; //Для реалізації зміни стану замку

int countUNKNOWN; //Лічильник числа зчитувань незареєстрованої RFID-карти


//Для сигналізації

int relayAlarm = 9; //Реле для підключення сирени


//Для управління з Bluetooth

int val = 0; //Змінна для запису даних із порту


//Для системи захисту від витоків газу int gasPin = A9; //Пін для датчика
газу

int gasValue = 0; //Змінна для зберігання даних із датчика газу

int relayGas = 4; //Реле для підключення вентилятора або ел.клапану (в
даному випадку - вентилятора)

bool a = true; //Включити сигналізацію навіть при одному спрацьовуванні
датчика газу

int countGas = 0; //Кількість спрацьовувань датчика газу


//Для системи захисту від протікання води int waterPin = A4; //Пін для
датчика води

int waterValue = 0; //Змінна для зберігання даних з датчика води int
relayWater = 12; //Реле для підключення ел.клапана
```

```
bool b = true; //Включити сигналізацію навіть при одному спрацьовуванні датчика води

int countWater = 0; //Кількість спрацьовувань датчика води


//Для датчика вогню

int firePin = A7; //Пін для датчика вогню

int fireValue = 0; //Змінна для зберігання даних із датчика вогню

bool c = true; //Включити сигналізацію навіть при одному спрацьовуванні датчика вогню

int countFire = 0; //Кількість спрацьовувань датчика вогню


//Для охорони вхідних дверей

int gerkon = 7; //Пін датчика відкриття

int gerkonState = 0; //Змінна для зберігання даних із датчика відкриття
int countDoor = 0; //Змінна для встановлення системи на охорону


void setup()

{

//Примітка: будь-яке реле відключено за рівня сигналу HIGH
Serial.begin(9600); / / Швидкість обміну даними по com-порту pinMode (relayAlarm, OUTPUT); //Підключення сирени digitalWrite(relayAlarm, HIGH); // Спочатку сирена відключена pinMode (gerkon, INPUT); //Підключення датчика відкриття


//Підключення дисплея lcd.begin(); //Ініціалізація

lcd.noBacklight(); //Вимкнути підсвічування


//Підключення системи захисту від витоків газу pinMode(relayGas, OUTPUT); digitalWrite(relayGas, HIGH);


//Підключення системи захисту від протікання води pinMode(relayWater, OUTPUT); digitalWrite(relayWater, HIGH);


//Підключення СКУД SPI.begin(); //Ініціалізація mfrc522.PCD_Init(); pinMode(relayDoor, OUTPUT);

digitalWrite(relayDoor, HIGH); //Спочатку замок закритий

}
```

```
void loop()

{

//УПРАВЛІННЯ ПО BLUETOOTH

if (Serial.available() > 0) //Якщо в com-порт щось прийшло

{

val = Serial.read(); //Записуємо в змінну val, рахувавши дані з порту


//Для системи захисту від витоків газу if (val == '1') //Якщо прийшла “1”

{

lcd.clear(); //Виведення напису на дисплей lcd.backlight();

lcd.setCursor(0,0); lcd.print("FAN"); lcd.setCursor(0,1); lcd.print("IS
WORKING");

digitalWrite(relayGas, LOW); //Включити вентиляцію

}

if(val == '2') //Якщо прийшла “2”

{

digitalWrite(relayGas, HIGH); //Вимкнути вентиляцію
digitalWrite(relayAlarm, HIGH); //Вимкнути сигналізацію lcd.clear();

lcd.noBacklight(); countGas = 0;

}


//Для системи захисту від протікання води if (val == '3') //Якщо прийшла
“3”

{

lcd.clear(); //Виведення напису на дисплей lcd.backlight();

lcd.setCursor(0,0); lcd.print("WATER VALVE"); lcd.setCursor(0,1);
lcd.print("IS WORKING");

digitalWrite(relayWater, LOW); //Включити ел.клапан

}

if(val == '4')

{

digitalWrite(relayWater, HIGH); //Вимкнути ел.клапан
digitalWrite(relayAlarm, HIGH); //Вимкнути сигналізацію lcd.clear();

lcd.noBacklight(); countWater = 0;

}
```

```
//Для датчика вогню if (val == '5')
{
digitalWrite(relayAlarm, HIGH); //Вимкнути сигналізацію lcd.clear();

lcd.noBacklight(); countFire = 0;
}

//Для постановки на охорону (контроль вхідних дверей) if (val == '6')
{
lcd.clear(); //Виведення напису lcd.backlight(); lcd.setCursor(0,0);
lcd.print("SECURITY MODE");
countDoor++; //Змінна для встановлення системи на охорону
}

//Для зняття з охорони if (val == '7')
{
countDoor = 0; //Обнулення змінної
lcd.clear(); //Вимкнення сигналізації, якщо включена lcd.noBacklight();
digitalWrite(relayAlarm, HIGH);
}
}

if (countDoor > 0 && a == true) // Якщо система в режимі охорони
{
a = false;
gerkonState = digitalRead(gerkon); //Зчитуємо дані з датчика відкриття
if(gerkonState == HIGH) // Якщо двері відчинені
{
lcd.clear(); //Виведення напису lcd.backlight(); lcd.setCursor(0,0);
lcd.print("SECURITY MODE"); lcd.setCursor(0,1); lcd.print("DOOR IS
OPEN!");
digitalWrite(relayAlarm, LOW); //Включення сигналізації
}
}
```

```
//СИСТЕМА ЗАХИСТУ ВІД ПРОТЕЧОК ВОДИ
waterValue = analogRead(waterPin); //Зчитуємо дані з датчика води if
(waterValue <= 500 && b == true) //Якщо виявлено протікання
{
b = false;

countWater = 1; //Збільшуємо лічильник спрацьовування датчика
}
if (waterValue > 500 && b == false) //Якщо не спрацював
{
countWater = 0; // Обнулюємо b = true;
}
if (countWater == 1) //При спрацьовуванні датчика робиться:
{
lcd.backlight(); //Виведення напису lcd.clear();
lcd.setCursor(0,0); lcd.print("ALARM! WATER"); lcd.setCursor(0,1);
lcd.print(" ");
digitalWrite(relayWater, LOW); //Включення ел.клапана
digitalWrite(relayAlarm, LOW); //Включення сигналізації
}

//СИСТЕМА ЗАХИСТУ ВІД Витоків ГАЗУ
gasValue = analogRead(gasPin); //Зчитуємо дані з датчика газу if
(gasValue > 400 && a == true) //Якщо виявлено витік
{
a = false;
countGas = 1; //Збільшуємо лічильник спрацьовування датчика
}
if (gasValue < 400 && a == false) //Якщо не спрацював
{
countGas = 0; // Обнулюємо a = true;
}
if (countGas == 1) //При спрацьовуванні датчика робиться:
{
lcd.backlight(); //Виведення напису lcd.clear();
```

```
lcd.setCursor(0,0); lcd.print("ALARM! GAS"); lcd.setCursor(0,1);
lcd.print(" ");

digitalWrite(relayGas, LOW); //Включення ел.клапана
digitalWrite(relayAlarm, LOW); //Включення сигналізації

}


//ДАТЧИК ВОГНЮ

fireValue = analogRead(firePin); //Зчитуємо дані з датчика вогню


if (fireValue < 30 && c == true) //Якщо виявлено вогонь

{

c = false; //Збільшуємо лічильник спрацьовування датчика countFire = 1;

}

if (fireValue > 100 && c == false) //Якщо не спрацював

{

countFire = 0; // Обнулюємо c = true;

}

if (countFire == 1) //При спрацьовуванні датчика робиться:

{

lcd.backlight(); //Виведення напису lcd.clear();

lcd.setCursor(0,0); lcd.print("ALARM! FIRE"); lcd.setCursor(0,1);
lcd.print(" ");

digitalWrite(relayAlarm, LOW); //Включення сигналізації

}


//СКУД

if (!mfrc522.PICC_IsNewCardPresent()) { //Пошук нової мітки return;

}

if (!mfrc522.PICC_ReadCardSerial()) { //Вибір мітки return;

}

uidDec = 0;

for (byte i = 0; i < mfrc522.uid.size; i++) { //Видача серійного номера
мітки uidDecTemp = mfrc522.uid.uidByte[i]; //У десятковому форматі

uidDec = uidDec * 256 + uidDecTemp;

}
```

```
if (uidDec == 16909060) { //Порівняння номера мітки із заданим, якщо номери рівні, то

d =! d; //Міняємо стан замку delay(1000);

}

if (d) {digitalWrite(relayDoor, LOW); //"двері відкриті"}

else

{digitalWrite(relayDoor, HIGH); //"двері зачинені"}


if (uidDec! = 16909060) { // Якщо номери не рівні delay (1000);

countUNKNOWN++;

if(countUNKNOWN = 1) { // Кількість зчитувань незареєстрованої карти
lcd.clear(); //Виведення напису

lcd.backlight(); lcd.setCursor(0,0); lcd.print("ALARM!");
lcd.setCursor(0,1); lcd.print("UNKNOWN CARD");

digitalWrite(relayAlarm, LOW); //Включення сигналізації

}

}

}
```

ДОДАТОК Б
(обов’язковий)

Копія тез доповіді на Всеукраїнській науково-практичній конференції Актуальні Проблеми Комп’ютерних Наук (АПКН-2021)

1) Рей К., Ковтонюк І., Грищук І. Дослідження методів керування ресурсами кіберфізичної системи «Розумний будинок» // Збірник наукових праць за матеріалами Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук» АПКН–2021 (Хмельницький, 15-16 жовтня 2021). С. 191-193.

УДК 004.031.42: 004.896

Рей К. С., Ковтонюк І. П., Грищук І. І.

Хмельницький національний університет

ДОСЛІДЖЕННЯ МЕТОДІВ КЕРУВАННЯ РЕСУРСАМИ КІБЕРФІЗИЧНОЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

Кіберфізична система «Розумний будинок» має забезпечувати комфорт, безпеку та ресурсозбереження, а також розпізнавати конкретні події та реагувати на них. В роботі проведено дослідження відомих методів керування ресурсами (зокрема, освітленням та контролем витоку води і газу) кіберфізичної системи «Розумний будинок».

The cyberphysical system "Smart Home" must provide comfort, security and resource conservation, as well as recognise and respond to specific events. The study of known methods of resource management (in particular, lighting and control of water and gas leakage) of the cyberphysical system "Smart Home" was conducted.

Кіберфізична система «Розумний будинок» дозволяє звільнити користувачів від левової частки побутових проблем. Це ціла інфраструктура, що перетворює середньостатистичну житлову площу в автономну екосистему.

Кіберфізична система «Розумний будинок» здатна: регулювати опалення та водопостачання; керувати освітленням житлової площі; забезпечувати охорону і відоспостереження; контролювати витік води і газу; підтримувати необхідний рівень вологості та температури в приміщеннях; керувати побутовою технікою [1-3].

Метою роботи є дослідження відомих методів керування ресурсами (зокрема, освітленням та контролем витоку води і газу) кіберфізичної системи «Розумний будинок».

В загальному вигляді структуру підсистеми освітлення кіберфізичної системи «Розумний будинок» зображено на рисунку 1 [4]. Така підсистема складається з модуля керування освітленням, модуля виявлення присутності, модуля контролю освітленням та модуля керування розетками, які об'єднані між собою за допомогою комутаційного середовища.

Модуль керування освітленням забезпечує ручне та автоматичне локальне керування освітленням. Модуль виявлення присутності визначає присутність людини в приміщенні та ввімкнення освітлення лише в тих приміщеннях, де помічена присутність. Модуль контролю освітленості вимірює природнє освітлення і вмикає освітлення лише в тих місцях, де є брак природного освітлення. Модуль управління розетками забезпечує можливість керування електроприладами з використанням безпровідної технології. Описана підсистема освітлення

кіберфізичної системи «Розумний будинок» керується з мобільного телефону за допомогою спеціального мобільного додатку.

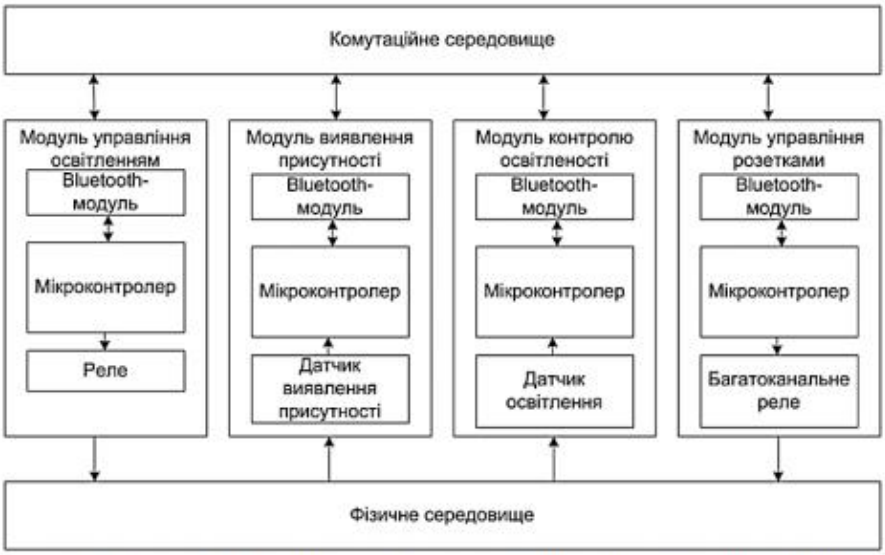


Рисунок 1 – Загальна структура підсистеми освітлення кіберфізичної системи «Розумний будинок» [4]

Рисунок 2 – Схема використання датчиків протікання води у підсистемі контролю витоку води і газу в кіберфізичній системі «Розумний будинок» [5]

Підсистема контролю витоку води і газу в кіберфізичній системі «Розумний будинок» забезпечує можливість закривати/відкривати клапани водо- і газопостачання при виявленні протікань в процесі контролю якості повітря, тобто автоматично блокувати подачу води та/або газу. Крім цього, така підсистема забезпечує правильну вентиляцію приміщень, дозволяє ввімкнення системи світло- та звукооповіщення, передачу сигналу на пульт оперативного чергового, а також передавати сигнал про аварію власнику житлового приміщення на мобільний телефон.

Схема використання датчиків протікання води у підсистемі контролю витоку води і газу в кіберфізичній системі «Розумний будинок» представлена на рисунку 2.

Отже, система «Розумний будинок» має забезпечувати комфорт, безпеку та ресурсозбереження, а також розпізнавати конкретні події та реагувати на них. В роботі проведено дослідження відомих методів керування ресурсами (зокрема, освітленням та контролем витоку води і газу) кіберфізичної системи «Розумний будинок».

Перелік посилань

1. Мельник А. О. Кіберфізичні системи: проблеми створення та напрями розвитку. Вісник Нац. ун-ту «Львівська політехніка». 2014. № 806. С. 154–161.
2. Ерфан П.. Микитин Г. Кіберфізичні системи в проектуванні розумних будинків. Студентська науково-технічна конференція : збірник тез доповідей, м. Львів, жовтень 2019 р. Львів, 2019. С. 176–178.
3. Lea P. Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security. Birmingham: Packt Publishing, 2018. 524p.
4. Франков Д.А. Кіберфізична система освітлення «Розумного будинку». Зв'язок. 2019. №5. С. 55-59.
5. Калінін Д. В. Електронні системи розумного будинку з підвищеною ефективністю: дипломна робота на здобуття ступеня бакалавра: 171 / Київ, 2021. 67 с.

ДОДАТОК В
(обов'язковий)

Презентація доповіді

Дипломна робота
на тему Метод та програмно-технічні засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок»

Судента II курсу групи КІ2м-20-1
Ковтонюка Івана Петровича
Науковий керівник: доктор технічні наук, професор
Говрущенко Тетяна Олександрівна

Хмельницький 2022

1

Мета і задачі дослідження

- ***Метою кваліфікаційної роботи*** є підвищення ефективності контролю витоку води і газу в кіберфізичній системі «Розумний будинок».
- ***Об'єктом дослідження*** є процес контролю витоку води і газу в кіберфізичній системі «Розумний будинок».
- ***Предметом дослідження*** є метод та засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

2

Мета і задачі дослідження

Для досягнення мети необхідно вирішити наступні *завдання дослідження:*

- 1) вивчити основні характеристики і виявити основні уразливості ключових систем «Розумного будинку»;
- 2) провести оцінку ризиків інформаційної безпеки «Розумного будинку» і виробити заходи захисту для їх зниження;
- 3) розробити і виконати прототип фрагмента системи «Розумний будинок»;
- 4) оцінити вразливість і захищеність системи «Розумного будинку» за допомогою експериментального дослідження функціонування розробленого прототипу фрагмента системи «розумний будинок».

.

Наукова новизна отриманих результатів:

- Вперше розроблено метод контролю витоку води і газу в кіберфізичній системі «Розумний будинок» для підвищення захищеності ІТ-систем «Розумного будинку» із застосуванням натурного моделювання для перевірки працездатності пропонованих рішень щодо захисту «Розумного будинку».

Практична значущість отриманих результатів полягає у:

- полягає у розробленні програмно-технічного засобу контролю витоку води і газу в кіберфізичній системі «Розумний будинок» з використанням Arduino в якості апаратно-програмної платформи проектованої системи.

5

Актуальність досліджень

- Обумовлена повсюдним розвитком інформаційно-технологічної (IT) інфраструктури та її застосуванням для забезпечення комфортного проживання громадян у помешканнях багатоквартирного чи індивідуального типу.
- Використання IT-технологій дозволяє створити т.зв. «Розумний будинок», тобто сукупність програмно–апаратних систем, безпосередньо керуючих інженерно–технічними, енергетичними, комунікаційними та іншими підсистемами житлового приміщення. Однак використання IT-інфраструктури, зокрема інформаційних систем управління нерозривно пов'язане з вирішенням питань забезпечення безпеки такої інфраструктури.

6

Аналіз та характеристики кіберфізичної системи Розумний Будинок

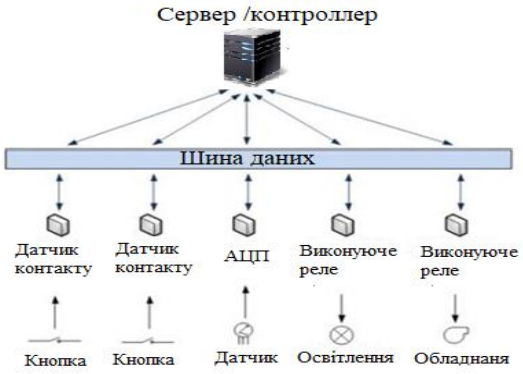
«Розумний будинок» це система що повинна вміти розпізнавати конкретні ситуації, що відбуваються в будівлі, і відповідним чином на них реагувати. Одна з систем може управляти поведінкою інших по заздалегідь виробленим алгоритмам. Основною особливістю інтелектуальної будівлі є об'єднання окремих підсистем в єдиний керований комплекс Важливою особливістю і властивістю «розумного будинку», яка відрізняє його від інших способів організації життєвого простору, є те, що це найбільш прогресивна концепція взаємодії людини з житловим простором, коли людина однією командою задає бажану обстановку, а вже автоматика відстежує режими роботи всіх інженерних систем і електроприладів

- Однією з найважливіших систе для комфортного проживання в будинку є: система витоку води та газу– це, головним чином, датчики води і газу. При витоку відповідний датчик в мить повідомить про це на центральний контролер, а той, у свою чергу, перекриває електроклапаном газ в будинку або воду в місце протікання.

7

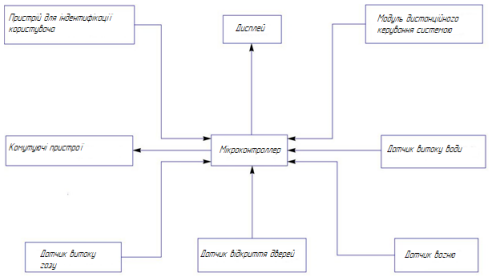
Аналіз існуючих рішень

- Після аналізу декількох пристроїв,з різними типами управління, було прийнято рішення обрати саме централізовану систему керування.
- Оскільки данна система є зручнішо і простішо в налаштуванні:



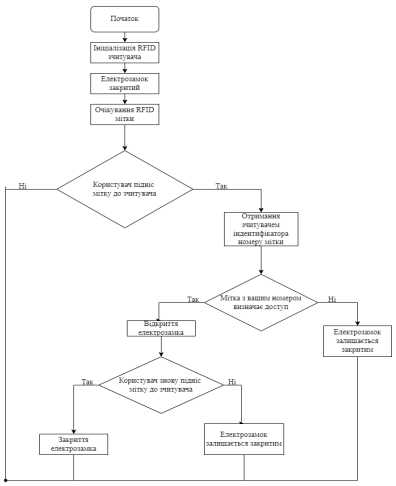
8

Для розробки структурної схеми і наступних етапів проектування було прийнято, рішення що при виникненні аварійної ситуації мікроконтролер повинен задіяти тільки самі комутуючі пристрої, наприклад реле. За допомогою комутуючих пристроїв можна безпосередньо керуватити роботою виконавчих механізмів, кінцевий вибір яких залишається за користувачем і ніяк не впливає на алгоритм роботи системи.



9

Алгоритму роботи зчитувача RFID



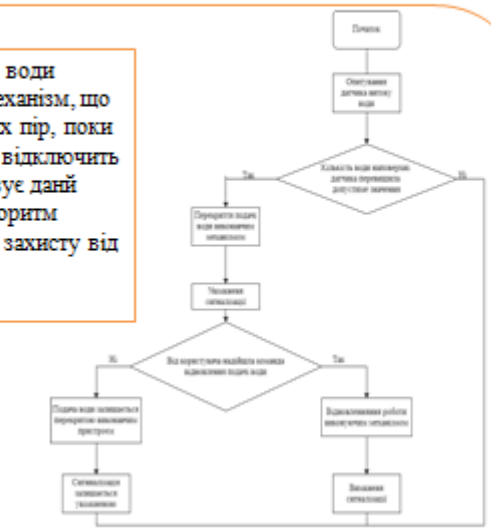
Відкриття і закриття дверного замка здійснюється за допомогою однієї мітки і одного зчитувача: спочатку користувач підносить свою RFID-мітку, перебуваючи зовні вхідних дверей, а потім, увійшовши всередину свого будинку або квартири, він підносить мітку до зчитувача знову, щоб закрити за собою замок.

Зчитувач повинен монтуватися в дверний замок таким чином, щоб була можливість зчитування мітки, коли користувач знаходиться з будь-якої

10

Алгоритму роботи датчика води

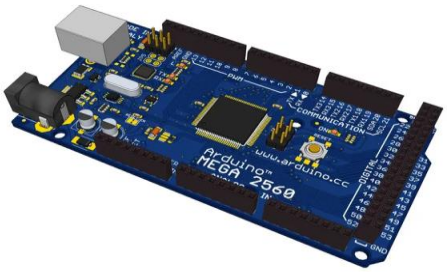
При виявленні протікання води спрацьовує виконавчий механізм, що перекриває її подачу до тих пір, поки користувач самостійно не відключить даний механізм що і показує даний алгоритм. Аналогічни алгоритм розроблений для системи захисту від витоку газу.



11

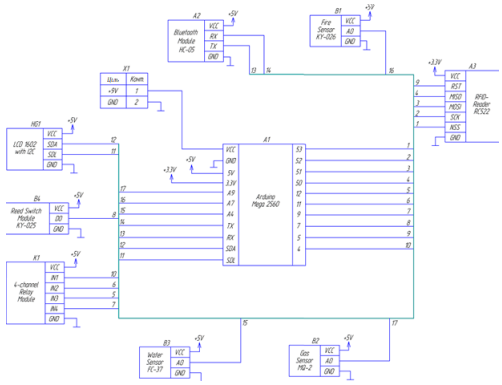
Апаратно-програмної платформи проектованої системи

В якості апаратно-програмної платформи проектованої системи була обрана Arduino. Дана платформа з відкритим вихідним кодом включає в себе серію плат на основі 8-бітних мікроконтролерів ATmega, сумісні з платами модулів для вирішення різних завдань, а також середовище розробки і налагодження програм Arduino IDE (Integrated Development Environment).



12

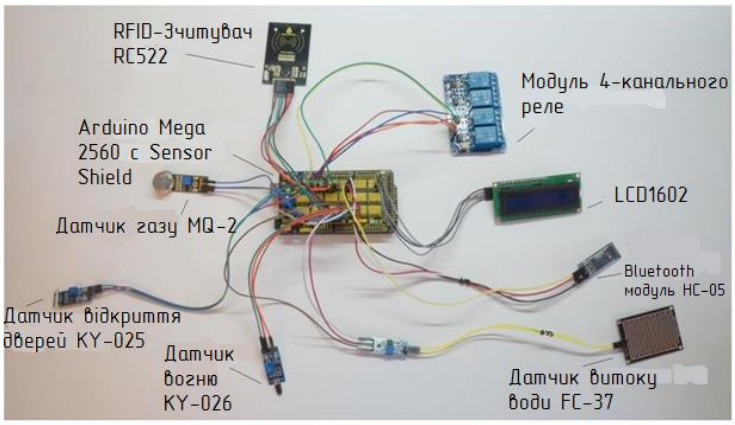
Складено принципову електричну схему проектованої системи "Розумного будинку"



13

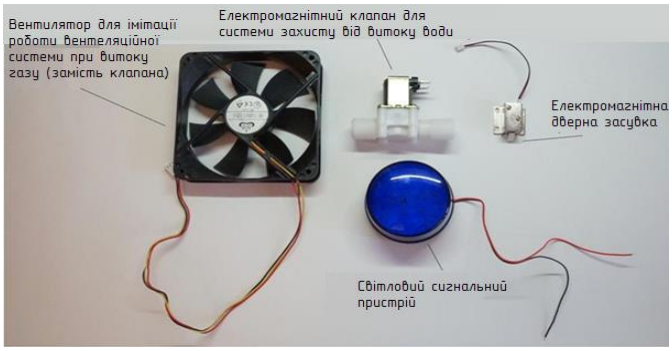
Збираємо модель спроектованої системи безпеки витоку води та газу

- Використовуючи раніше вибране апаратне забезпечення, зібрали модель спроектованої системи безпеки "Розумного будинку"



14

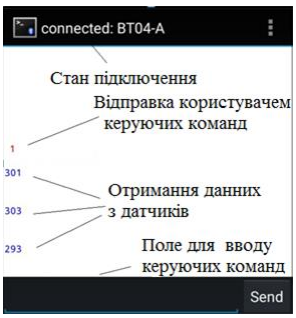
- В якості виконавчих механізмів для демонстрації роботи спроектованої системи були обрані наступні пристрої (рисунок 3.7): електромагнітний замок для системи контролю та управління доступом, електромагнітний клапан для системи захисту від протікання води.
- Для демонстрації системи захисту від витоків газу вибрали вентилятор з системного блоку комп'ютера, щоб показати інший можливий варіант роботи системи: включення витяжної вентиляції при скупченні небезпечного обсягу газу в приміщенні. Всі вибрані виконавчі пристрої працюють від напруги від 9 до 12 В, а їх робота управляється блоком 4-х канального реле.



15

Управління платою Arduino

- Для можливості управління платою Arduino за допомогою протоколу Bluetooth вибрали додаток Bluetooth Terminal для мобільної операційної платформи Android. За допомогою цієї програми користувач може як відправляти команди на плату Arduino, так і приймати від неї дані. Основне вікно програми і приклад обміну даними представлені на рисунку



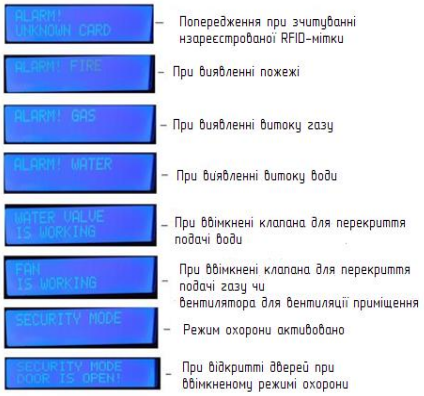
16

Управління платою Arduino

- Варто відзначити, що відправка керуючих команд здійснюється шляхом відправки однієї з цифр від 0 до 10. Для проектованої системи встановили наступні співвідношення: «1» - задіяти реле 1 (відключити подачу газу); «2» - задіяти реле 1,4 (відновити подачу газу, відключити сигналізацію); "3"- задіяти реле 3 (відключити подачу води); "4" - задіяти реле 3,4 (відновити подачу води, відключити сигналізацію); «5» — задіяти реле 4 (відключити сигналізацію при виявленні загоряння); «6» — поставити систему на охорону (включити сигналізацію шляхом задіяння реле 4 в разі спрацьовування датчика відкриття); «7» - зняти систему з охорони і/або відключити сигналізацію шляхом задіяння реле 4.
- Номери реле збігаються з відповідними висновками IN1, IN2, IN3, IN4 на обраному модулі чотириканального реле.

17

- Нижче представлена реалізація виведення інформаційних повідомлень при будь-якій події в системі, а саме: при фіксації будь-якої аварійної події, при зчитуванні незареєстрованої RFID-мітки, при включенні користувачем будь-якого реле, при активації режиму охорони, при відкритті вхідних дверей в режимі охорони.



18

Тестування

Моделювання ситуації аутентифікації користувача в системі

Назва	Тест для перевірки RFID автентифікації у системі	
Use case	Автентифікація користувача у системі.	
Дія	Очікуваний результат.	Результат тесту
Передумова		
Увімкнути живлення Arduino Mega 2560	Діод, аутентифікації RFID увімкнутий	Пройдений
Кроки тесту		
Підносим мітку до рідера з ключем 16909060	Сигналізація не спрацювала,	Пройдений
Відчиняємо двері	Виведено надпис ("DOOR IS OPEN!");	Пройдений

19

Публікація за матеріалами дипломної роботи

- 1) Рей К., Ковтонюк І., Грищук І. Дослідження методів керування ресурсами кіберфізичної системи «Розумний будинок» // Збірник наукових праць за матеріалами Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук» АПКН–2021 (Хмельницький, 15-16 жовтня 2021). С. 191-193.

20

Висновки

- "У даном розділі проведено аналіз та дослідження технології " Розумний будинок" що являє собою житлове або нежитлове (не використовується для проживання) приміщення, оснащене засобами обчислювальної техніки та управління, що підтримують інформаційні технології, які здатні діяти проактивно з метою задоволення потреби людини в комфортному і безпечному проживанні.
- Застосування комплексу засобів автоматизації та інформаційних технологій «Розумного будинку» дозволяє забезпечити безпечну і ефективну експлуатацію, запобігти ризику нанесення шкоди, що приводить до відмови або аварії обладнання інженерних комунікацій, систем енергозабезпечення, газопостачання, вентиляції, опалення, холодного і гарячого водопостачання, водовідведення, систем зв'язку, охоронних та інших систем будівель, і споруд.
- В роділі було досліджено найпопулярніші рішення щодо проектування та оптимізація взаємодії компонентів, розглянуто технології такі як Z-Wave та X10 основні фактори, що впливають на безпеку інформації «Розумного будинку», побудованого на основі готових систем, було виявлено переваги та недоліки.
- Розглянуто також основні фактори, що впливають на безпеку інформації «Розумного будинку», побудованого на основі готових систем.
- Таким чином розроблена система суб'єктивних і об'єктивних факторів, що впливають на систему «Розумного будинку». Надалі ця система буде використана для аналізу загроз «розумного будинку».

Висновок

- У системах захисту від протікання води і витоків газу ключову роль відіграють виконавчі механізми, які відсікають подачу, відповідно, води або газу.
- Датчик протікання води розміщується в тих приміщеннях і місцях, в яких можливе протікання води: під ванною, поруч з пральною машиною і так далі.
- Система захисту від витоків газу працює за принципом, схожим з системою захисту від протікання води і встановлюється в приміщеннях з газовим обладнанням: котельні, кухонні кімнати. Газоаналізатор, тобто датчик газу, фіксує витік газу, якщо його концентрація в повітрі перевищує деяке порогове значення.
- Як приклад для розгляду вибрали модель дверного замка SHS-P718 від компанії Samsung.
- На ринку «розумних будинків» одним з лідерів є компанія Rubetek. Вона пропонує як окремі "розумні" пристрої, так і готові комплекти, один з яких називається «управління та безпека». До його складу входять: модуль управління, датчик протікання, датчик відкриття, датчик диму. Однак користувач може зібрати свою власну систему з будь-яких вподобаних йому пристроїв.
- Широке визнання на ринку охоронних систем отримала «розумна» сигналізація Ajax українського виробництва. Дана охоронна система складається з керуючого пристрою і набору датчиків.
- Проектована система безпеки «Розумного будинку» повинна мати два режими роботи: «Охорона відключена» і «Охорона включена».
- Проектована система безпеки "Розумного будинку" для роботи згідно з розробленим алгоритмом повинна мати в своєму складі ряд електронних елементів: мікроконтролер, датчики для фіксації аварійних подій, комутуючі пристрої для підключення виконавчих механізмів, дисплей для виведення різної інформації, модуль для дистанційного керування системою користувачем.
- В якості апаратно-програмної платформи проектованої системи була обрана Arduino. Дана платформа з відкритим вихідним кодом включає в себе серію плат на основі 8-бітних мікроконтролерів ATmega, сумісні з платами модулі для вирішення різних завдань, а також середовище розробки і налагодження програм Arduino IDE (Integrated Development Environment).

Висновок

- У середовищі розробки Arduino IDE склали програмний код, що реалізує розроблений раніше алгоритм роботи проектованої системи
- Програма складена на мові C / C++. При написанні програми використовувалися спеціальні готові бібліотеки для Arduino IDE: бібліотека для роботи з RFID-зчитувачем, бібліотека для роботи з LCD - дисплеєм і бібліотека для роботи з I2C-інтерфейсом.
- Використовуючи раніше вибране апаратне забезпечення, зібрали модель спроектованої системи безпеки "Розумного будинку".
- Для зручності збірки використовували розширення для плати Arduino Mega 2560, зване Sensor Shield. Дане розширення дозволяє спростити процес підключення до плати великої кількість датчиків та інших електронних модулів, не використовуючи макетну плату.

23

Висновок

- При розробці системи використовувалися такі підходи та принципи: ООП, SOLID, DRY, KISS, YAGNI та coding guidelines, які рекомендує Microsoft. Під час мануального тестування було перевірено основні функції системи. Оцінено вразливість і захищеність системи «Розумного будинку» за допомогою експериментального дослідження функціонування розробленого прототипу фрагмента системи «розумний будинок».
-

24

UNICHECK

Ім'я користувача:
Кафедра КІ

ID перевірки:
1011113584

Дата перевірки:
09.05.2022 16:39:57 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
09.05.2022 18:03:16 EEST

ID користувача:
100005591

Назва документа: **Ковтонюк_Метод та програмно-технічні засоби контролю витоку води і газу в кіберфізичн...**

Кількість сторінок: **83** Кількість слів: **13626** Кількість символів: **105648** Розмір файлу: **4.08 MB** ID файлу: **1011012342**

2.24%
Схожість

Найбільша схожість: **0.57%** з джерелом з Бібліотеки (ID файлу: **1010865495**)

1.44% Джерела з Інтернету	36	Сторінка 85
0.92% Джерела з Бібліотеки	70	Сторінка 85

0.28% Цитат

Цитати	2	Сторінка 86

Не знайдено жодних посилань

0%
Вилучень

Немає вилучених джерел

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 10%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 103344 Название: Метод та програмно-технічні засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок» Добавлено в БД: 2022-05-09 Авторы: І.П Ковтонюк Руководители: Т.О.Говорущенко Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	98737	701	1657 (2%)	21 (3%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Ковтонюк Іван Петрович

Тема: Метод та програмно-технічні засоби контролю витоку води і газу в кіберфізичній системі «Розумний будинок»

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг дипломної роботи:

Кількість сторінок записки 120 с.

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є підвищення ефективності контролю витоку води і газу в кіберфізичній системі «Розумний будинок».

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі проведено аналіз відомих моделей, методів та засобів контролю витоку води і газу і кіберфізичній системі «Розумний будинок». В другому розділі проведено моделювання та вибір необхідної елементної бази для контролю витоку води і газу і кіберфізичній системі «Розумний будинок». В третьому розділі розроблено алгоритми та метод контролю витоку води і газу і кіберфізичній системі «Розумний будинок». Вперше розроблено метод контролю витоку води і газу в кіберфізичній системі «Розумний будинок» для підвищення захищеності ІТ-систем «Розумного будинку» із застосуванням натурного моделювання для перевірки працездатності пропонованих рішень щодо захисту «Розумного будинку». В четвертому розділі реалізовано програмно-технічний засіб контролю витоку води і газу і кіберфізичній системі «Розумний будинок».

4. Позитивні сторони роботи: ретельний підбір елементної бази.

5. Негативні сторони роботи: розроблений метод не має математичного

ФОРМА ЗАТВЕРДЖЕНА ПРОТОКОЛОМ

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на середньому науково-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: добре/С.

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Бурлак Леонід Петрович, д. ф.-м. н., проф., зав. каф. УПЗ

"12" 05 2022 р. _____ (підпис)

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Ковтонюк Іван Петрович
ПІБ здобувача вищої освіти

ФПКТС, 2 курсу, групи КІ2м-20-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в ельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020). но з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної оти до захисту та застосування заходів дисциплінарної та академічної повідальності, ознайомлений (а). Про використання програмно-технічних засобів для ревірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та даю свою згоду на обробку та збереження університетом моєї роботи в інституційному позитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та ереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та користання роботи для виявлення плагіату в інших роботах, які перевіряються ограмно-технічними засобами та користувачами, що мають доступ до цих програмно-хнічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному ріанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

9.05.2022

дата

підпис

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОМАЦІЙНИХ СИСТЕМ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, енерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод та програмно-технічні засоби контролю витоку води і газу в кіберфізичній истемі «Розумний будинок»

Автор: Ковтонюк Іван Петрович

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Говорущенко Тетяна Олександрівна, д.т.н, професор

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) найбільшу схожість встановлено з одним документом і становить вона 0.57% в частині загальноприйнятої термінології.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 2.24% і адресується до 22 першоджерел, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи Т. О. Говорущенко

Гарант ОНП О. С. Савенко

Завідувач кафедри КІІС Т. О. Говорущенко