

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Автоматизації проектування обчислювальної техніки
(повна назва)

АТЕСТАЦІЙНА РОБОТА Пояснювальна записка

рівень вищої освіти другий (магістерський)
(рівень вищої освіти)

Спеціалізовані комп'ютерні засоби для забезпечення
надійного функціонування розумного дому
(тема)

Виконав: студент 2 курсу, групи СКСм-19-1
Рижиков І.В.
(прізвище, ініціали)

Спеціальність 123 Комп'ютерна інженерія
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Спеціалізовані комп'ютерні системи
(повна назва освітньої програми)

Керівник проф. Кривуля Г. Ф.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____
(підпис)

Чумаченко С.В.
(прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет _____ Комп'ютерної інженерії та управління _____
Кафедра _____ Автоматизації проектування обчислювальної техніки _____
Рівень вищої освіти _____ другий (магістерський) _____
Спеціальність _____ 123 – Комп'ютерна інженерія _____
Тип програми _____ Освітньо-професійна _____
Освітня програма _____ Спеціалізовані комп'ютерні системи _____

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

« _____ » _____ 20 ____ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

Студентові Рижикову Ігорю Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема роботи _____ Спеціалізовані комп'ютерні засоби для забезпечення
надійного функціонування розумного дому _____

затверджена наказом по університету від "30" _____ 10 _____ 2020 р. № 1489СТ _____

2. Термін подання студентом роботи до екзаменаційної комісії _____ 18.12.2020 _____

3. Вихідні дані до роботи _____

Середовище розробки Arduino IDE

Мікроконтролер Arduino Uno R3

Мова програмування C/C++

Модульні датчики

GSM- модуль

4. Перелік питань, що потрібно опрацювати в роботі _____

Аналіз методів охорони

Огляд існуючих рішень

Вибір апаратного забезпечення

Середовище _____ розробки _____ програмного
забезпечення _____

_____ Розробка _____ схем _____ та _____ збирання
пристрою _____

Алгоритм роботи пристрою

Розробка програмного забезпечення

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) 15 слайдів

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

7. Дата видачі завдання 01 09 2020 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи (проекту)	Термін виконання етапів роботи	Примітка
1	Отримання завдання	01.09.2020 -10.09.2020	
2	Аналіз предметної області	10.09.2020 -30.09.2020	
3	Аналіз джерел з проблемної галузі	30.09.2020 -15.10.2020	
4	Постановка задачі	15.10.2020-15.11.2020	
5	Розробка системи	15.11.2020 -25.11.2020	
6	Створення функціонального пристрою	25.11.2020 -05.12.2020	
7	Проведення дослідження пристроєм	05.12.2020 -08.12.2020	
8	Оформлення пояснювальної записки	08.12.2020 -12.12.2020	
9	Оформлення графічного матеріалу	12.12.2020 -14.12.2020	
10	Перевірка виконаного проекту керівником	14.12.2020 -15.12.2020	
11	Захист проекту	16.12.2020 -23.12.2020	

Студент

(підпис)

Керівник роботи

(підпис)

проф. Кривуля Г. Ф.

(посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 74 с., 3 додатки, 41 рис., 6 табл., 33 джерела за переліком посилань.

СИСТЕМА, РОЗУМНИЙ ДІМ, ДОМАШНЯ БЕЗПЕКА, СИГНАЛІЗАЦІЯ, ІНТЕРНЕТ РЕЧЕЙ, ДАТЧИКИ, МІКРОКОНТРОЛЛЕР, GSM

Метою дослідницької роботи є дослідження яке спрямовано на підвищення безпеки і надійності розумного будинку за рахунок системи моніторингу з використанням GSM-модуля на пристроях за допомогою Інтернету речей. Система використовує модульні датчики: датчик руху, датчик відкриття дверей, датчик витоку газу і протікання води. При будь-якому виявленні модульними датчиками буде відправлятися повідомлення у вигляді SMS оповіщення з інформацією про можливі події в будинку.

В результаті реалізації забезпечена більш висока безпека будинку завдяки використанню функції, при технічній реалізації якої можна періодично відправляти повідомлення про стан будинку, щоб отримувати інформацію про можливі події в залежності від даних, отриманих за допомогою датчиків.

ABSTRACT

Explanatory note: 74 pages, 3 applications, 41 pictures, 6 tables, 33 source by reference list.

SYSTEM, SMART HOME, HOME SECURITY, ALARM, INTERNET THINGS, SENSORS, MICROCONTROLLER, GSM

The purpose of the research is a study aimed at improving the safety and reliability of a smart home through a monitoring system using a GSM module on devices using the Internet of Things. The system uses modular sensors: motion sensor, door opening sensor, gas leak and water flow sensor. At any detection by modular sensors the message in the form of the SMS notification with the information on possible events in the house will be sent.

As a result of the implementation, a higher security of the house is provided due to the use of the function, during the technical implementation of which it is possible to periodically send messages about the state of the house to receive information about possible events depending on the data obtained by sensors.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ.....	8
ВСТУП.....	9
1 АНАЛІЗ МЕТОДІВ ОХОРОНИ ПРИМІЩЕНЬ ЗА ДОПОМОГОЮ ІНТЕРНЕТУ РЕЧЕЙ.....	10
1.1 Поняття «Інтернет речей».....	10
1.2 Управління розумним будинком.....	13
1.3 Безпека розумного будинку.....	13
1.3.1 Системи відеоспостереження.....	15
1.3.2 Системи контролю точок входу і виходу.....	18
1.3.3 Системи контролю витoku газу.....	21
1.3.4 Системи контролю протікання води.....	23
1.3.5 Системи контролю будинку детектором руху.....	25
1.4 Недоліки розумних будинків.....	28
1.5 Комерційні рішення і технології управління системою домашнього моніторингу.....	29
1.5.1 Комунікаційний протокол X10.....	30
1.5.2 Протокол бездротового зв'язку Z-Wave.....	30
1.5.3 Протокол передачі даних KNX.....	31
2 ЕТАПИ РОЗРОБКИ.....	33
2.1 Мета і технічна задача дослідження.....	33
2.2 Вибір комплектуючих.....	34
2.2.1 Мікроконтролер Arduino Uno.....	34
2.2.2 GSM-модуль Neoway M590.....	36
2.2.3 Пасивний інфрачервоний датчик руху HC-SR501.....	38
2.2.4 Датчик широкого спектра газів MQ-2.....	40
2.2.5 Датчик протікання води FC-37.....	41
2.2.6 Датчик відкриття дверей MC-38.....	42
2.2.7 Модуль активного зумера YL-44.....	43

2.2.8 Двоканальне реле постійного струму 5VDC-C.....	44
.....	45
3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ СИСТЕМИ.....	46
3.1 Структурна схема системи.....	46
3.2 Опис роботи системи.....	50
3.3 Середовище розробки програмного забезпечення Arduino.....	52
3.4 Програмна реалізація та опис.....	54
3.5 Опис алгоритму роботи пристрою.....	60
ВИСНОВКИ.....	71
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	73
ДОДАТОК А.....	77
Програмна реалізація пристрою.....	77
ДОДАТОК Б.....	84
Графічний матеріал атестаційної роботи.....	84
ДОДАТОК В.....	89
Наукова публікація.....	89

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ
І ТЕРМІНІВ

AT – Attention – Початок виклику строк команд модема;

CCTV – Closed Circuit Television – Система телебачення замкнутого контуру;

DC – Direct current – Постійний струм;

DIY – Do It Yourself –Зроби сам;

DVR – Digital Video Recorder –Цифровий відеореєстратор;

GND – Ground – Вузол в електроніці, потенціал якого умовно приймається за нуль;

GSM – Global System for Mobile Communications – Глобальний стандарт цифрового мобільного сотового зв'язку;

IoT – Internet of Things – Інтернет речей;

IP – Internet Protocol – Міжмережевий протокол;

LAN – Local Area Network – Локальна мережа;

MW sensor – Microwave sensor – Мікрохвильовий датчик;

NVR – Network Video Recorder – Мережевий відеореєстратор;

PIR sensor – Passive Infrared sensor – Інфрачервоний датчик;

RAM – Random Access Memory – Оперативна пам'ять;

RX – Receive – Канал отримання даних;

SIM – Subscriber identification module – Модуль ідентифікації абоненту;

SMS – Short Message – Технологія прийому та передачі коротких текстових повідомлень за допомогою сотового телефону;

SoC – System-on-a-Chip – Система на кристалі;

TX – Transceive – Канал відправлення даних;

VoIP – Voice over Internet Protocol – Телефонний зв'язок по протоколу IP;

VCR – Video Cassette Recording – Аналоговий відеореєстратор;

Wi-Fi – Wireless Fidelity – Стандарт бездротового зв'язку 802.11.

ВСТУП

Існують різні форми і види кримінальних злочинів в сучасному суспільстві. Бути захищеним від різних інцидентів, таких як крадіжка, пожежа, витік газу і тому подібні аномалії, є постійною турботою власників будинків. Однією з основних завдань є прийняття запобіжних заходів з використанням різних систем сигналізації та інших датчиків для виявлення вторгнення в будинок.

Дослідницька робота присвячена розробці та впровадженню системи інтелектуального моніторингу розумного будинку з використанням GSM-модуля на пристроях за допомогою Інтернету речей. При цьому загальна безпека розумного будинку з використанням інтелектуального моніторингу системи домашньої безпеки може бути значно покращено.

Дослідження спрямовано на підвищення безпеки і надійності за рахунок системи інтелектуального моніторингу розумного будинку. Система використовує модульні датчики: датчик руху, датчик витіку газу і протікання води для запобігання можливих витоків, датчик відкриття дверей для виявлення руху злоумисників. У разі будь-якого виявлення модульними датчиками, власники будинку будуть попереджені через SMS-повідомлення з інформацією про можливі події в будинку.

Дослідження також підвищує безпеку завдяки новій функції, яка може відправляти SMS-повідомлення з інформацією про статус системи інтелектуального моніторингу та модульних датчиків, щоб бути в курсі можливих подій в залежності від даних, отриманих за допомогою датчиків.

1 АНАЛІЗ МЕТОДІВ ОХОРОНИ ПРИМІЩЕНЬ ЗА ДОПОМОГОЮ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Поняття «Інтернет речей»

Internet of Things (IoT) – система взаємопов'язаних обчислювальних пристроїв, механічних і цифрових машин, об'єктів, тварин або людей, яким надають унікальні ідентифікатори і можливість передати дані по мережі, не вимагаючи взаємодії від людини до людини або людини до комп'ютера.

В інтернеті речей «рiччю» може бути людина з імплантатом кардіомонітора, сiльськогосподарська тварина з транспондером біочипа, автомобіль, у якого є вбудовані датчики, щоб попереджати водія, коли тиск повітря в шині стає низьким, або будь-який інший природний або штучний об'єкт, якому може бути привласнена IP-адреса і надана можливість передати дані по мережі.

Більш широкодоступним стає широкосмуговий інтернет, вартість підключення зменшується, створюється все більше пристроїв з можливостями Wi-Fi і вбудованими в них датчиками, технологічні витрати знижуються, і впровадження смартфонів стає більш популярним і необхідним. Всі ці речі створюють прекрасні умови для IoT.

IoT описує світ, де практично все може бути пов'язано і взаємодіяти інтелектуальним способом (рис. 1.1). Іншими словами, з Інтернетом речей матеріальний світ стає однією великою інформаційною системою. Простіше кажучи, це концепт простого з'єднання будь-яких пристроїв з вкл/викл перемикачами до Інтернету. Це включатиме в себе все: мобільні телефони, кавоварки, пральні машини, навушники, лампи і майже все, про що можна подумати. Це також може бути застосовано до компонентів машин, наприклад до реактивного двигуну літака, або розгортці нафтової платформи.

Якщо пристрій має вкл/викл перемикач, тоді є велика ймовірність, що цей пристрій може бути частиною IoT.

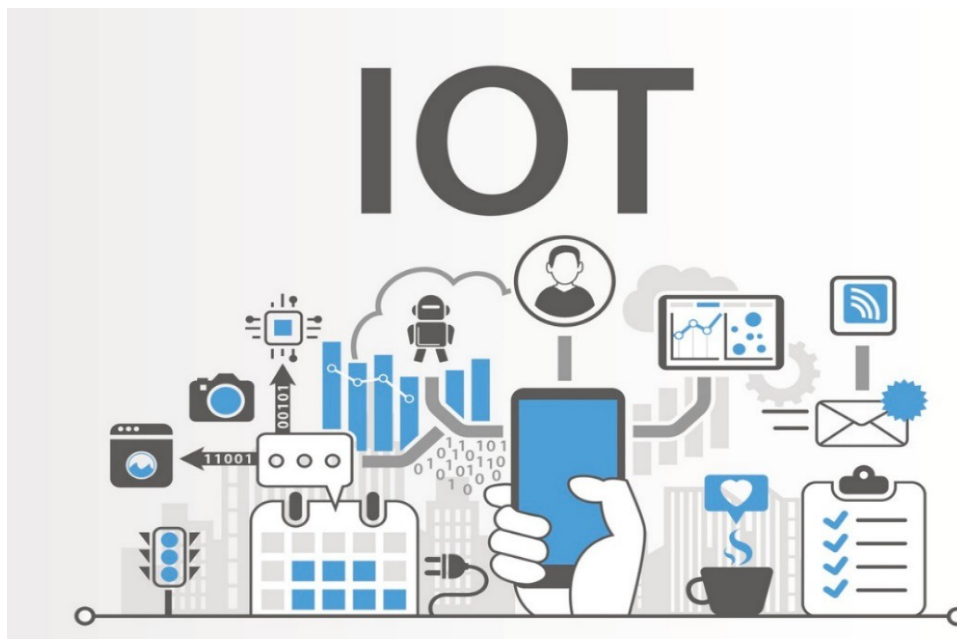


Рисунок 1.1 – Інтернет речей

Це також може бути застосовано до компонентів машин, наприклад до реактивного двигуну літака, або розгортці нафтової платформи. Якщо пристрій має вкл/викл перемикач, тоді є велика ймовірність, що цей пристрій може бути частиною IoT. Аналітична фірма Gartner заявляє, що до 2022 буде більш ніж 26 мільярдів з'єднаних пристроїв. Це величезна кількість з'єднань. В майбутньому будуть існувати відносини людей між собою, відносини між речами і людьми [15].

Новим правилом для майбутнього буде: «Все, що може бути пов'язано, буде з'єднано». Але з якого дива стільки підключених пристроїв, які говорять один з одним? Є безліч прикладів, на що це може бути схожим. Скажімо, наприклад, прямуючи на зустріч в дорозі, автомобіль міг би мати доступ до календаря водія і заздалегідь знати, який маршрут буде найбільш оптимальним. Якщо на дорозі щільний рух, автомобіль міг би відправити повідомлення з текстом іншому учаснику зустрічі, що ви не встигнете. Що

якщо будильник починає будити о 6:00 і потім повідомляє кавоварку, щоб та почала варити каву?

У більш широкому масштабі IoT може бути застосований до таких речей як транспортні мережі: «розумні міста», які можуть допомогти людям зменшувати відходи і підвищувати ефективність користування деякими речами, наприклад, використання енергії - це допоможе людям зрозуміти, як ми працюємо і живемо, допоможе поліпшити умови життя і зменшити витрати ресурсів (рис. 1.2).

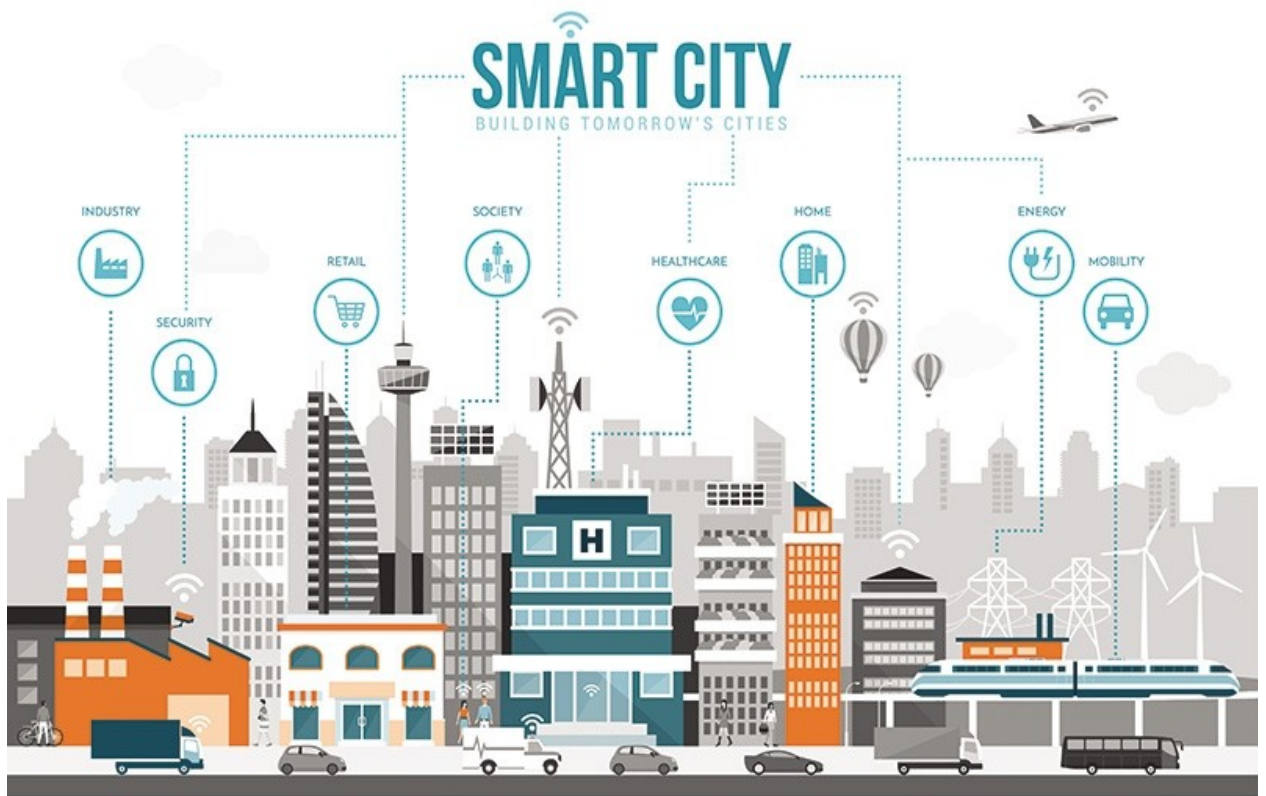


Рисунок 1.2 – Потенційне розумне місто

Розмови про IoT ведуться в усьому світі, оскільки ми прагнемо зрозуміти, як це вплине на наше життя. Люди також намагаються збагнути, як багато можливостей і перешкод перед нами виникне, коли все більше пристроїв почне приєднуватися до IoT [30].

1.2 Управління розумним будинком

Однією з головних переваг системи автоматизації будинку - це зручність і легкість управління системою і різноманітним обладнанням, об'єднаним в єдине ціле.

Для моніторингу за системою і управління нею, може використовуватися центральний головний пристрій, який знаходиться безпосередньо в будинку, або ж портативний пристрій з виходом в інтернет, за допомогою якого можна віддалено контролювати роботу «Розумного будинку».

Панель контролю (локальна або дистанційна), керуюча системою будинку, має широкі можливості управління, так як в одну систему автоматизації зв'язуються різні прилади, такі як системи освітлення, електрична мережа, кліматичні та обігрівальні установки, системи охорони, це дозволяє контролювати і змінювати умови комплексно. Налаштування системи визначаються користувачем, виходячи з можливих життєвих ситуацій, і можуть бути налаштовані в будь-який момент.

Для підвищення зручності використання автоматизації будинку, системи можуть включати в себе набір сценаріїв автоматизованої роботи з встановленими фіксованими налаштуваннями.

1.3 Безпека розумного будинку

Безпека розумного будинку – це єдина система управління контролюю комфорт і безпекою будинку. Система контролює не тільки цілісність інженерних систем, але і захистить будинок від непроханих гостей. Системи безпеки включають: системи відеоспостереження, системи контролю точок входу і виходу, охоронно-пожежну сигналізацію, інфрачервоні датчики руху, датчики витoku газу та датчики протікання води.

Система безпеки розумного будинку спрямована на забезпечення інженерної та особистої безпеки. Інженерна безпека система «Розумний будинок» забезпечує:

- захист від протікання води;
- захист від замикання в електромережі;
- захист від загоряння;
- систему автоматичного пожежогасіння;
- аварійну сигналізацію для оповіщення сервісних служб.

Розумні системи безпеки призначені для забезпечення безпеки будинку, захисту від будь-яких надзвичайних ситуацій. Надзвичайні ситуації такі як: захист запобігання вторгнення за рахунок камер відеоспостереження, автоматизація всіх дверей, охоронної сигналізації, запобігання будь-яких аварійних ситуацій. Система «Розумний будинок» забезпечує:

- контроль цілісності дверей та вікон;
- імітація присутності господарів;
- контроль входу в приміщення;
- відеоспостереження за територією(прилеглою);
- автоматичне освітлення території при виявленні;
- управління захисними жалюзями;
- захист від пожежі, витоків газу.

Поточний стан охоронюваних зон контролює стан дротових і бездротових датчиків (датчики вікон, дверей, руху, задимленості, газу та води). Залежно від типу сигналу датчики викликають певну реакцію керуючої системи. Якщо датчик фіксує небезпеку виникнення пожежі, автоматично буде увімкнена система протипожежної безпеки, припинено доступ свіжого повітря, що сприяє розгоранню полум'я, перекритий газ, вимкнено електрику, сигналізація сповістить присутніх в приміщенні про пожежу, відправить на мобільний телефон господаря SMS-повідомлення.

Все це перешкоджає поширенню вогню і зменшує ймовірність його збільшення, знижуючи ризик нанесення серйозних збитків.

Протікання води може створити проблеми як самим господарям квартири, так і їхнім сусідам. Для запобігання наслідків виходу з ладу елементів водоподачі створені системи які контролюють протікання. Датчики протікання води встановлюються в місцях з'єднання побутової техніки або сантехніки з водопровідними трубами, а між ручними вентилями і фільтрами водоочистки ставляться магнітні клапани. Якщо трапилося пошкодження гнучкого проводу і потрапила волога на підлогу, датчик фіксує її наявності і подає сигнал на клапан, який перекриває подачу воду, запобігаючи затоплення приміщення [13].

1.3.1 Системи відеоспостереження

Системи відеоспостереження вважаються одним з найбільш надійних методів захисту певної території. Такі системи безперервно розвиваються щодо використовуваного обладнання і щодо його функціональності.

Найбільш популярні додатки були засновані на DVR. Незважаючи на їх популярність, у них є певні недоліки, в першу чергу необхідність забезпечення окремого кабелю для кожної камери, по-друге, обмежене число каналів (для наступних каналів буде потрібно інший DVR), а також, один центр спостереження (з DVR всередині). На рисунку 1.3 показана система моніторингу на основі DVR.

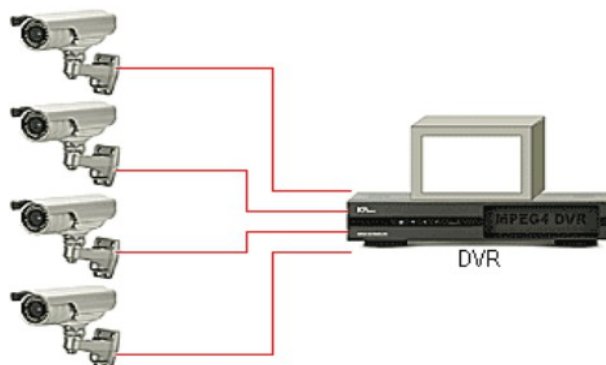


Рисунок 1.3 – Система моніторингу на основі DVR

NVR і DVR – використовується щоб керувати переглядами і зберегти відеозапис спостереження. Існує NVR і DVR, які спрощують процес збереження і перегляду відео. В якому з цих форматів зберігати відео, залежить від наявності CCTV або камер спостереження IP. Приклад системи моніторингу на основі NVR можна побачити на рисунку 1.4.

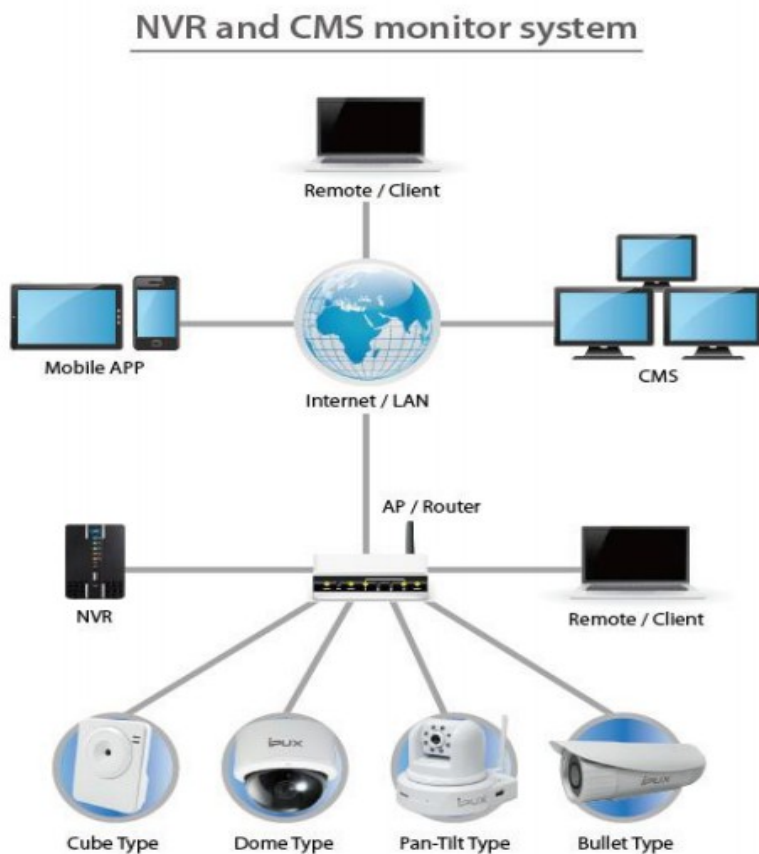


Рисунок 1.4 – Система моніторингу на основі NVR

NVR і DVR виконують спільне завдання запису і зберігання відео, NVR і DVR розроблені таким чином, що можуть взаємодіяти з різними типами камер. І NVR, і DVR спроектовані за єдиним стандартом в плані габаритів. DVR використовуються в CCTV або аналогових системах спостереження. Більш старі системи записали б відео безпосередньо на касетну стрічку, використовуючи VCR, але учасні системи використовують DVR, щоб перетворювати відеофайли в цифрові формати, дозволяючи зберегти більше відео. DVR також надають зручність віддаленого доступу.

Ці реєструючі пристрої, що використовують локальну мережу, щоб відправляти і отримувати дані, вони ідеальні для віддаленого контролю системи спостереження з комп'ютера, смартфона або планшета. Оскільки IP-камери - це передовий рубіж технологій спостереження, використання NVR дозволить додавати нові камери з великою кількістю розширених функцій. Якщо в системі спостереження використовується суміш CCTV і IP-камер, можна використовувати спеціалізовані відеокодери, які дозволять камерам CCTV з'єднуватися з NVR.

NVR і DVR ідеальні для управління безліччю камер з одного центру управління. NVR і DVR можуть поліпшити систему спостереження: зберігання більшої кількості відеофайлів, камера може зберігати на локальну MicroSD карту, можливість зберігання відео протягом більш тривалих проміжків часу, запис відео високої якості у великих обсягах. Установка попереджень і вікон виявлення руху, якщо ці функції вже не встановлені в камерах. Перегляд і аналіз всіх відеозаписів на єдиному інтерфейсі, замість того, щоб отримувати доступ до відео кожної камери індивідуально.

NVR і DVR доступні для придбання, у багатьох головних брендів систем спостереження включаючи Milestone, Smartvue і QNAP.

Камери спостереження доступні в різних конфігураціях, камери спостереження можуть використовуватися кількома різними способами в якості частини цільної системи безпеки.

Типове використання камер відеоспостереження включає в себе контроль за:

- 1) важкодоступними для очей або віддаленими областями;
- 2) віддаленими будівлями, такими як гаражі, сараї, ангари, склади;
- 3) точками входу, внутрішніми і зовнішніми.

До камер спостереження можна отримати доступ віддалено з комп'ютерів, смартфонів і планшетів. Камери часто використовуються, коли власники поза містом, щоб спостерігати за всім, що відбувається біля будинку. Камери можуть також використовуватися, щоб зробити запис будь-

яких порушень правил безпеки, за допомогою чого можна добре розглянути грабіжників і навіть транспортний засіб, на якому вони прибули [8].

1.3.2 Системи контролю точок входу і виходу

Всі домашні системи безпеки працюють над основним принципом захисту точок входу, таких як двері і вікна. Незалежно від розміру будинку або кількості дверей і вікон власник хоче захистити своє майно, єдина суттєва різниця полягає в кількості компонентів безпеки, розгорнутих по всьому будинку і контрольованих панеллю керування.

В даному випадку ми говоримо про домашню систему безпеки, які є мережами інтегрованих електронних пристроїв, які з'єднано з центральною панеллю керування, щоб захистити майно від грабіжників і інших зловмисників. Типова домашня система безпеки включає:

- панель управління, яка є основним контролером системи безпеки будинку;
- датчики на дверях і вікнах;
- гучна сирена або сигналізація;
- значки, стікери, наклейки охоронної компанії.

Домашня система безпеки працює над простим поняттям, охорони точок входу в будинок датчиками, які зв'язуються з панеллю керування або центром управління, встановленим в зручному місці будинку. Датчики як правило встановлюють на дверях, які ведуть в будинок, а також на вікнах, особливо тих, які відкриваються.

Панель управління – це комп'ютер, який вмикає і вимикає систему безпеки, зв'язується з кожним встановленим компонентом, піднімає тривогу, коли зона безпеки порушена і зв'язується з компанією з контролю аварійного сигналу. Панель управління зазвичай з сенсорною панеллю для простого програмування і взаємодії, можуть працювати з мовними командами і можуть бути запрограмовані, щоб працювати з бездротовим пультом дистанційного керування.

Датчики на дверях і вікнах складаються з двох частин, встановлених поруч один з одним. Одна частина пристрою встановлюється на вікнах або дверях, а інша на підвіконні або дверній рамі. Коли двері або вікно закриті, дві частини датчика об'єднуються, створивши схему захисту (рис. 1.5).

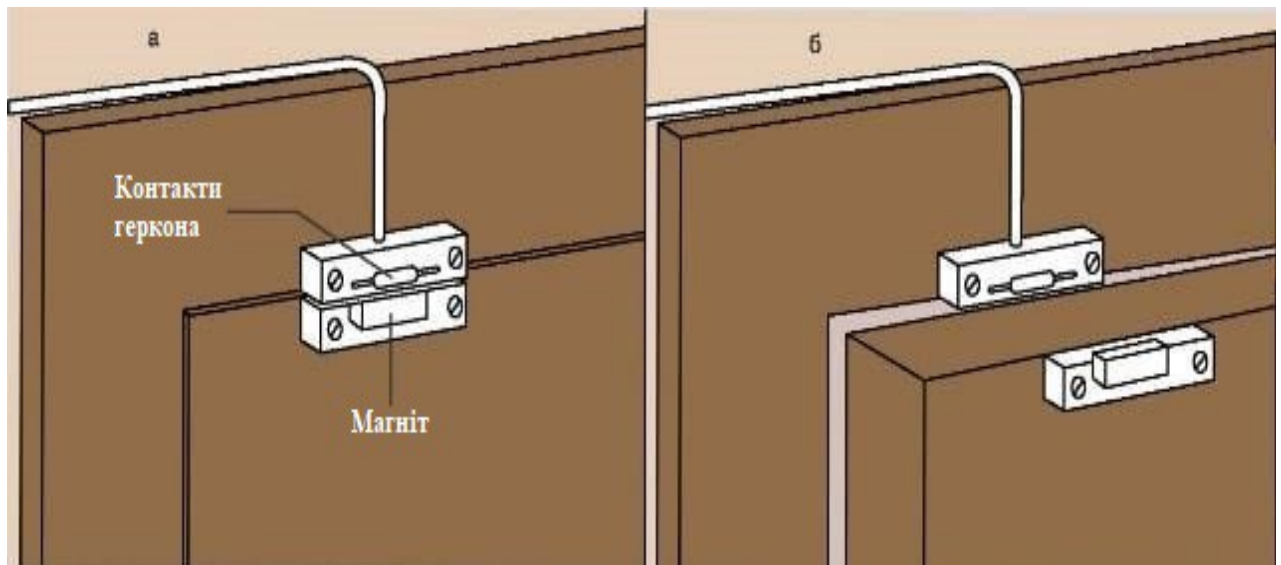


Рисунок 1.5 – Датчик відкриття дверей

Коли система безпеки увімкнена на панелі управління, ці датчики зв'язуються з нею, повідомляючи, що точка входу безпечна. Якщо контрольовані двері або вікно раптово відкривається, схема захисту виявляє пошкодження, і панель управління інтерпретує це як порушення охоронної зони. Піднімається тривога, і в більшості випадків автоматично оповіщається компанія з контролю аварійним сигналом [7].

Сигналізація досить гучна для того, щоб сусіди могли її почути, домашні сигналізації служать для різних цілей. По-перше, сигналізація попереджає людей в будинку, що трапилося порушення безпеки. Сигналізація також досить пронизлива, щоб прогнати грабіжника. Пульта управління домашньою сигналізацією рисунок 1.6.



Рисунок 1.6 – Пульт управління домашньою сигналізацією

Маркетингові інструменти для охоронних компаній, наклейки охоронної компанії грають важливу роль в домашній безпеці. Коли людина наклеює етикетку компанії по забезпеченню безпеки (рис 1.7) на вікно або двері, вона показує грабіжникам що територія професійно захищена.



Рисунок 1.7 – Етикетки компаній щодо забезпечення безпеки

Системи безпеки розроблені, щоб виконувати певні завдання, коли зона яка охороняється порушена. Система безпеки професійно контролюється охороною компанією, охорона компанії буде попереджена коли в будинку раптово трапиться проблема з безпекою. Навчений фахівець з безпеки зв'яжеться з власником будинку через панель управління або подзвонить на екстренних контактний номер, який прив'язаний до аккаунта.

Системи безпеки взаємодіють з охоронною компанією одним з декількох способів, включаючи:

- по існуючих лініях домашнього телефону, які продовжують працювати під час перебоїв електричної енергії, при використанні резервного джерела живлення;
- передача мови по протоколу IP (VoIP), який зазвичай не працює при перебоях електричної енергії;
- через інтернет, який також зазвичай не працює при перебоях електричної енергії.

В разі фактичної надзвичайної ситуації охоронна компанія повідомить належний персонал екстреного реагування, який працює у певній області. Охоронна компанія також спробує встановити зв'язок з домовласником, поки команда екстреного реагування не прибуде будинок.

Існує багато систем безпеки DIY, які не взаємодіють з професійно контрольованими службами. У разі порушення захисту будинку, коли система безпеки DIY увімкнена, спрацьовує аварійний сигнал. Контакт з поліцією або іншими службами екстреного реагування буде ініціюватися домовласником, який змушений набрати потрібний номер в ручному режимі [10].

Деякі системи можуть підтримувати відправку текстових SMS-повідомлень на мобільний телефон домовласника в разі порушення захисту будинку, але деякі типи не підтримують таку функцію, в залежності від провайдера і системи, яку вибрав домовласник.

1.3.3 Системи контролю витоку газу

Останнім часом досить часто трапляються вибухи і пожежі, через витоки і поширення горючих газів. Навіть невеликий витік газу може привести до вибуху або пожежі, що може не тільки зашкодити конструкцію або зруйнувати будівлю, але і заподіяти серйозні пошкодження здоров'ю

людині яка знаходиться поруч. Саме тому дуже важливо стежити за справністю газового обладнання та вчасно виконувати профілактичне обслуговування.

Система контролю витоку газу забезпечується спеціальним механізмом, який дає можливість швидко закрити подачу газу в приміщення. Найпростіші датчики діагностують концепцію одного або декількох видів газу, і при перевищенні максимально допустимого рівня подають сигнал. Датчики як правильно виготовляються у вигляді компактних мобільних телефонів, які можна встановити в будь-якому зручному місці, але такі датчики використовуються тільки для особистого використання і власної безпеки в побутових умовах [2].



Рисунок 1.8 – Система контролю витоку газу

Дія системи контролю витоків газу полягає в використанні датчиків різних видів: електромеханічних, оптичних, термомеханічних та інших датчиків, які реагують на різні види газів.

Датчики витоку газу складаються з наступних основних елементів:

- первинний перетворювач – датчик, який приймає і визначає обсяг та концепцію газу в повітряному просторі;

- модуль вимірювання – пристрій, який приймає дані від первинного перетворювача, і проводить їх порівняння з допустимою величиною;
- виконавчий механізм – електромагнітний клапан, який перекриває подачу газу;
- джерело живлення – джерело електричного струму у вигляді акумулятора, гальванічного елемента або мережевого блоку живлення;
- Корпус пристрою.

1.3.4 Системи контролю протікання води

Поломка сантехнічного обладнання є однією з найпоширеніших проблем протікання води. Погодьтеся, бути винним потопу і його жертвою одночасно неприємно, але і накладно з фінансової сторони. Вчасно встановлений датчик контролю протікання води, допоможе уникнути катастрофи навіть у разі пошкодження труб і порушення цілісності системи будинку.

Принцип роботи стаціонарної системи контролю протікання води ґрунтується на різниці між електропровідністю води і повітря. Основою датчика контролю протікання води є звичайна пара електродів. Якщо на електроди потрапляє вода, то опір знижується і відбувається замикання електричного кола (рис. 1.9).

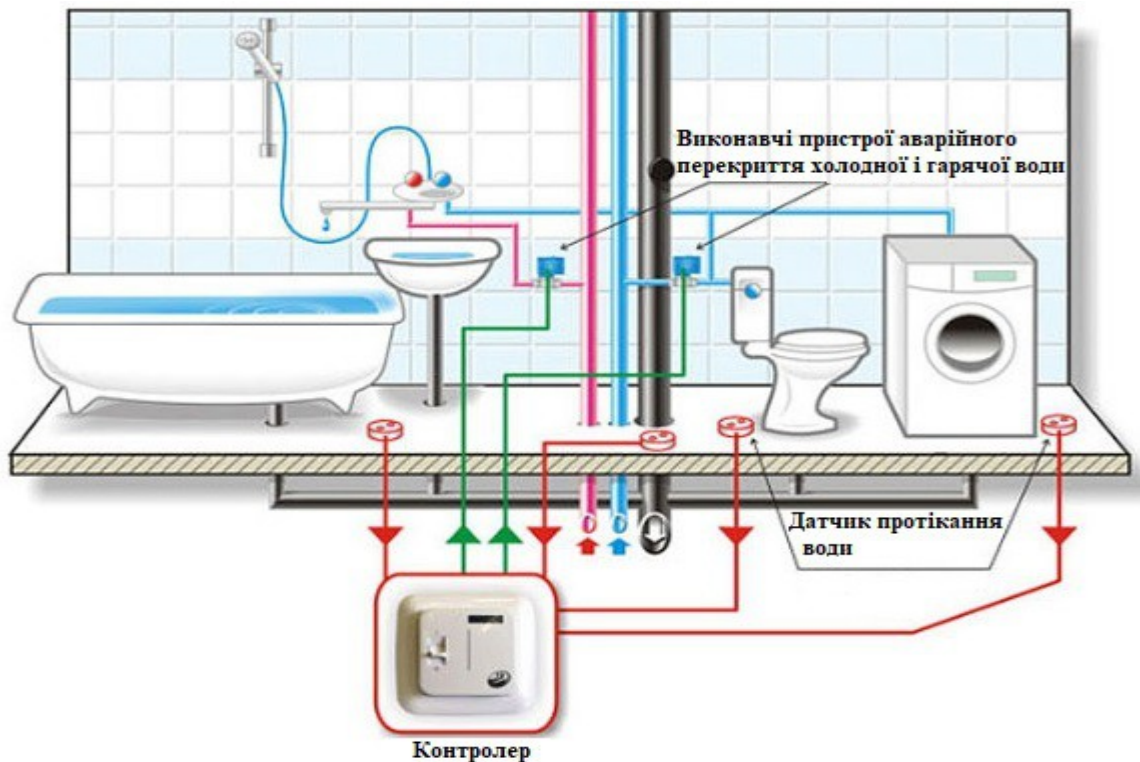


Рисунок 1.9 – Система контролю протікання води

Інформація про замикання ланцюга надходить на контролер, де відбувається розшифровка імпульсу і обробка інформації. Після цього контролер подає свій сигнал на закриття електромагнітного клапана, який розташований на основній трубі (стояку), безпосередньо на самому введенні системи. Вхідний кран буде перекритий до тих пір, поки не буде виявлена і повністю ліквідована причина протікання води. Після скоєння простих маніпуляцій з контролером робота системи контролю протікання води буде відновлена. Стационарна система працює автономно і вимагає втручання тільки в разі виявлення протікання і ліквідації несправностей в системі [3]. Існують наступні способи інформування про протікання:

- індикація на дисплеї контролера;
- індикація на дисплеє, супроводжується шумовими сигналами;
- шумова сигналізація, індикація и отправка сообщения.

Відправлення повідомлень можливе в тому випадку, якщо система обладнана GSM-модемом. В цьому випадку відбувається відправка SMS-повідомлення на мобільний номер домовласника, який зашитий в пам'яті пристрою.

1.3.5 Системи контролю будинку детектором руху

Система контролю детекторами руху є опорою системи безпеки, тому що це основний пристрій, який виявляє коли хтось перебуває в будинку. Детектор руху використовує одну або кілька технологій, щоб виявити переміщення в будинку. Коли детектор спрацьовує, сигнал відправляється на панель управління системи безпеки, яка з'єднується з центром спостереження, попереджаючи про потенційну загрозу в будинку.

Головна мета детекторів руху полягає в тому, щоб виявити зловмисника і надіслати попередження на панель управління. Детектори працюють, коли домовласник не перебуває вдома. Деякі системи безпеки можуть бути запрограмовані, щоб записувати події через камеру відеоспостереження, коли виявляється рух [24]. Приклад установки детектора руху можна побачити нижче на рисунку 1.10.



Рисунок 1.10 – Детектор руху

Детектори руху можуть:

- ініціювати спрацювання дверного дзвінка, коли хтось наблизиться до дверей;
- попередити, коли діти проникають в обмежені області будинку, такі як підвал або кімната для тренувань;
- зберігати електричну енергію, використовуючи освітлення детектора руху.

Існує кілька типів детекторів руху:

1) пасивні інфрачервоні детектори (PIR) виявляють тепло тіла (інфрачервона енергія). Пасивні інфрачервоні детектори – найбільш широко використовуються в домашніх системах безпеки. Коли система підключена, детектори руху активовані. Як тільки детектор нагрівається, він може виявити тепло і переміщення, створивши захисну «сітку». Якщо об'єкт, що рухається блокує занадто багато зон сітки, і інфрачервоні енергетичні рівні змінюються швидко, спрацювають (рис. 1.11);



Рисунок 1.11 – Принцип роботи пасивного інфрачервоного детектора руху

2) мікрохвильові детектори відсилають мікрохвильові імпульси і вимірюють відбиття від рухомого об'єкту. Детектори покривають більшу

область, ніж інфрачервоні детектори, але вони уразливі для електричної інтерференції і дорожчі (рис. 1.12);

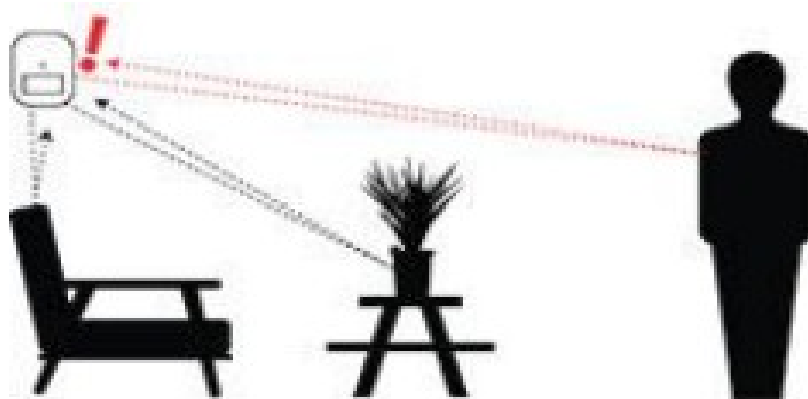


Рисунок 1.12 – Принцип роботи мікрохвильового детектора руху

3) комбіновані детектори руху можуть поєднувати функції в спробі зменшити ймовірність помилкових спрацьовувань тривоги. Наприклад, детектор з пасивним інфрачервоним випромінюванням (PIR) може бути об'єднаний з мікрохвильовим детектором. Так як кожен діє в різних областях спектру, і один з них активний, а інший – пасивний, в комбінованих детекторах руху ймовірність помилкових спрацьовувань тривоги значно менше, ніж в інших, тому що для аварійного сигналу обидва детектора повинні зареєструвати рух (рис. 1.13);

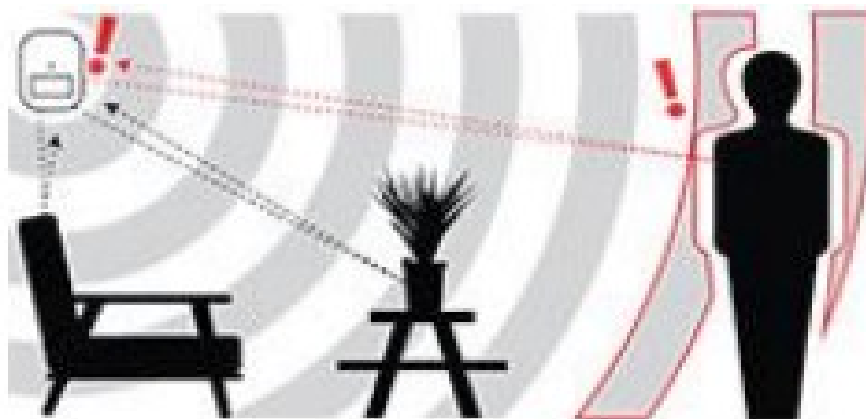


Рисунок 1.13 – Принцип роботи комбінованих датчиків руху

4) ультразвукові детектори руху відсилають імпульси ультразвукових хвиль і вимірюють відбиття від рухомого об'єкту. Активні ультразвукові детектори випускають звукові хвилі від кристалічних кварцових перетворювачів. Хвилі потрапляють на об'єкти в області виявлення, і поки не відбувається ніякого руху, хвилі не перериваються. Однак, коли відбувається рух, звукова хвиля переривається і відбивається назад до приймача системи. Приймач тоді передає сигнал модулю електронного управління, і в залежності від його чутливості і калібрування, модуль електронного управління визначає, чи гарантує руйнування сигналу безладний рух. Якщо так, тоді модуль передає сигнал до сигнального компонента, який викликає тривогу. Область виявлення слабшає з відстанню. Однак рух виявляється до відстані приблизно дванадцяти метрів.

Пасивні детектори працюють за принципом виявлення звуків, таких як розбиття скла або стукіт по металу, щоб піднімати тривогу. Такі звуки виробляють хвилі, які виявляються детекторами, як активні детектори, передають їх до модуля електронного урядування, щоб визначити, чи знаходиться зразок звукової хвилі в межах встановлених параметрами. Кваліфіковані грабіжники знають, як проникнути на об'єкт, не створюючи дуже гучних звуків, багато людей використовують ці детектори разом з пасивними інфрачервоними детекторами, щоб збільшити чутливість [28].

1.4 Недоліки розумних будинків

Технологія розумного будинку не позбавлена недоліків, недоліки також важливі як і переваги. Можливо, в майбутньому ситуація зміниться в кращу сторону, але поки що головною проблемою технології є її сумісність. Розумний будинок - це не якийсь абстрактний і готовий проект, а сукупність великої кількості пристроїв. З одного боку, це дозволяє користувачеві збирати унікальні конфігурації під свої конкретні вимоги. З іншого, все це викликає неминучі труднощі з сумісністю. Якщо ви використовуєте безліч

пристроїв від різних виробників, часом буває дуже складно змусити їх працювати разом. Якщо система використовує безліч пристроїв від різних виробників, часом буває дуже складно змусити їх працювати разом. Ця проблема вирішиться тільки в тому випадку, якщо виробники розумних гаджетів домовляться про якихось універсальних стандартах.

Другий найважливіший недолік розумного будинку – його ціна. Як сказано вище, розумний будинок допомагає економити, але і сам обходиться в чималу суму. Середня ціна одного окремо взятого пристрою, типу економного термостата - кілька сотень доларів. Чим розумніша система вашого будинку, тим більше в ньому електроніки, і тим дорожче все це коштує. Пройде не один рік, перш ніж економія себе окупить.

Третім недоліком є відведення окремого місця під обладнання. Для коректної роботи всієї системи необхідно використання стабілізаторів напруги щоб можна було контролювати скачки напруги і короткі замикання в мережі. Крім цього, для автономної роботи цілісності інженерних систем і охоронних функцій, слід використовувати резервне джерело живлення, в якості такого можуть виступати акумуляторні батареї або генератор, які також вимагають відводу певного місця [9].

1.5 Комерційні рішення і технології управління системою домашнього моніторингу

Комерційні рішення і технології управління системою домашнього моніторингу стали застосовуватися приблизно з 1975 року в США. Новатором в цій області стала компанія Pico Electronics, яка створила протокол зв'язку X10. Надалі зарубіжний ринок поповнився і іншими компаніями їх власними комунікаційними протоколами.

1.5.1 Комунікаційний протокол X10

Даний комунікаційний протокол і стандарт є найбільш старим і популярним в сфері систем автоматизації. Протокол розроблений в 1975 році компанією Pico Electronics для управління домашніми електроприладами.

Технологія X10 заснована на передачі сигналів по електропроводці будинку. Для передачі сигналів використовуються коливання на частоті 120 кГц тривалістю 1 мс. Спочатку технологія працювала при частоті 60 Гц і напруга мережі 110 В і використовувалася тільки на території США. X10 допомагає вирішити найрізноманітніші завдання домашньої автоматизації, починаючи від управління світловими приладами і закінчуючи системою безпеки.

Використання електромережі для управління електроприладами з одного боку є безперечною гідністю даної технології. Для підключення приладу до виконавчого модулю, немає необхідності прокладати нову проводку або використовувати дорогі датчики і контролери, оснащені бездротовим інтерфейсом. Управління електроприладами виконується безпосередньо, завдяки передавачів, які формують і відправляють команди X10 в електромережу [12].

З іншого боку, такий підхід несе безліч недоліків, таких як:

- низька швидкість передачі даних;
- низька перешкодозахищеність;
- проблема помилкового спрацьовування;
- можливі конфлікти пристроїв X10 різних виробників;
- можливий несанкціонований доступ до пристроїв X10 по електромережі.

1.5.2 Протокол бездротового зв'язку Z-Wave

Z-Wave являє собою бездротовий протокол передачі даних для домашньої автоматизації. Дана технологія орієнтована для забезпечення простого і надійного способу бездротового управління освітленням,

вентиляцією, системами безпеки, домашніми кінотеатрами, автоматичним воротам і елементам управління. У 2005 році компанією Zensys був створений альянс Z-Wave, в який увійшли різні компанії. На сьогоднішній день існують сотні сумісних продуктів Z-Wave, що продаються під різними марками.

Технологія Z-Wave призначена для забезпечення надійної і швидкої передачі простих, керуючих команд з малими затримками на швидкості до 100 кб/с. Z-Wave працює в діапазоні частот до 1 ГГц, це обумовлено невеликою кількістю можливих джерел електромагнітних полів. Пристрої можуть взаємодіяти один з одним за допомогою проміжних вузлів, це дозволяє обійти побутові перешкоди або «мертві зони». Найпростіша мережа являє собою єдиний керований прилад і первинний контролер. Додаткові пристрої можуть бути додані в будь-який час. Мережа Z-Wave може включати в себе до 232 пристроїв.

1.5.3 Протокол передачі даних KNX

KNX є стандартизованим протоколом зв'язку для автоматизації будівель. Продукція KNX поширювалася під декількома торговельними марками. Найбільш відомі Instabus, ABB i-Bus, Tebis, Theben.

Всі пристрої, що працюють за технологією KNX з'єднані між собою двопровідною шиною, що дозволяє їм обмінюватися даними. Функції окремих пристроїв визначаються на етапі планування проекту, але може бути змінений і адаптовані в будь-який час. До складу обладнання KNX входять наступні типи пристроїв:

- датчики;
- приводи;
- системні пристрої і компоненти.

Датчики є відправною точкою для кожної дії. Вони відповідають за фіксування тих чи інших зовнішніх подій. Наступ події повинен викликати певну реакцію системи. Після цієї події сенсор посилає по мережі керуючу

команду відповідному виконавчому пристрою. Виконавчі пристрої отримують пакети даних, які потім перетворюються в дії. Такими діями можуть бути управління жалюзі, вимикання світла або управління системою опалення та кондиціонування повітря.

KNX є повністю розподіленою мережею, яка вміщує до 65536 пристроїв в 16 біт індивідуального адресного простору. Логічна топологія дозволяє підключити до 256 пристроїв на одній лінії.

Однією з сильних сторін системи KNX, є те, що будь-який продукт, розроблений різними компаніями, але при цьому, що має сертифікацію KNX, може працювати спільно. Члени асоціації мають понад 7000 KNX сертифікованих продуктів. Цей широкий асортимент продукції дозволяє:

- керувати освітленням;
- контролювати опалювальні установки і системи кондиціонування;
- аналізувати аварійні сигнали;
- керувати енергоспоживанням природними ресурсами.

Головним недоліком комерційних рішень, які використовують власний протокол зв'язку є їх закритість, тобто використовуються протоколи передачі даних з фірмовим кодуванням, які не завжди дозволяють інтегрувати в єдину систему чуже обладнання [31].

2 ЕТАПИ РОЗРОБКИ

2.1 Мета і технічна задача дослідження

Метою дослідницької роботи є створення та впровадження поліпшеної системи інтелектуального моніторингу, розроблену з меншими витратами, яка підвищує безпеку і надійність розумного будинку за рахунок системи моніторингу з використанням GSM-модуля на пристроях за допомогою інтернету речей (IoT).

Система спеціалізується не тільки на забезпеченні безпеки шляхом виявлення грабіжників, але і на моніторингу безпеки будинку від можливих пожеж шляхом виявлення витоків газу, протікання води, крадіжок і тому подібних аномалій, є постійною турботою власників будинків.

У разі будь-якого виявлення модульними датчиками, власники будинку будуть попереджені через SMS-повідомлення, навіть якщо вони знаходяться далеко від дому.

Дослідження також підвищує безпеку завдяки новій функції, яка може відправляти SMS-повідомлення з інформацією про статус системи моніторингу та модульних датчиків, щоб бути в курсі можливих подій в залежності від даних, отриманих за допомогою датчиків.

Завдання дослідження:

- 1) зробити аналіз комерційних рішень на ринку домашньої автоматизації;
- 2) вибрати апаратне забезпечення системи;
- 3) спроектувати схему контролера сигналізації і модульних датчиків;
- 4) об'єднати мікроконтролер і модульні датчики в єдиний функціональний пристрій;

- 5) розробити програму, здатну відправляти повідомлення за допомогою SMS-повідомлень і отримувати повідомлення, аналогічно інтерпретуючи їх в команду;
- 6) перевірити безпеку і аутентифікацію пристрою.

Проаналізувавши вимоги, можна сказати, що вхідними даними буде інформація з спрацьованих модульних датчиків. Вихідними – спрацювання модуля активного звуку і відправка SMS-повідомлення за допомогою GSM-модуля домовласникові.

Для досягнення поставлених цілей були вибрані такі методи: використання C/C++ для Arduino, використання додаткових бібліотек, використання класів, системних функцій та розширень. GSM-модуль, Arduino Uno, датчик руху, датчик витoku газу, датчик протікання води, датчик відкриття дверей, модуль активного звуку і реле.

2.2 Вибір комплектуючих

2.2.1 Мікроконтролер Arduino Uno

Arduino – це платформа електроніки з відкритим вихідним кодом в основі апаратного і програмного забезпечення. Платформа Arduino дуже популярна по всьому світу завдяки зручності і простоті мови програмування. Пристрій програмується через USB без використання програматорів.

За багато років Arduino був мозком тисяч проектів, починаючи з предметів повсякденного користування і закінчуючи складними приладами для досліджень. Arduino дозволяє комп'ютеру вийти за рамки віртуального світу і фізично взаємодіяти з ним. Пристрої на базі Arduino можуть отримувати інформацію про навколишнє середовище за допомогою величезної кількості різних датчиків, також можуть управляти різними керуючими пристроями.

Мікроконтролер програмується за допомогою мови C і середовища розробки Arduino IDE, яке є повністю відкритим і доступним. Проекти

пристроїв, створені за допомогою Arduino, можуть працювати самостійно, або ж взаємодіяти з програмним забезпеченням на РС. Плати можуть бути припаяні користувачем самостійно або ж куплені вже готовими до використання [22]. Мікроконтролер Arduino Uno зображений на рисунку 2.1.

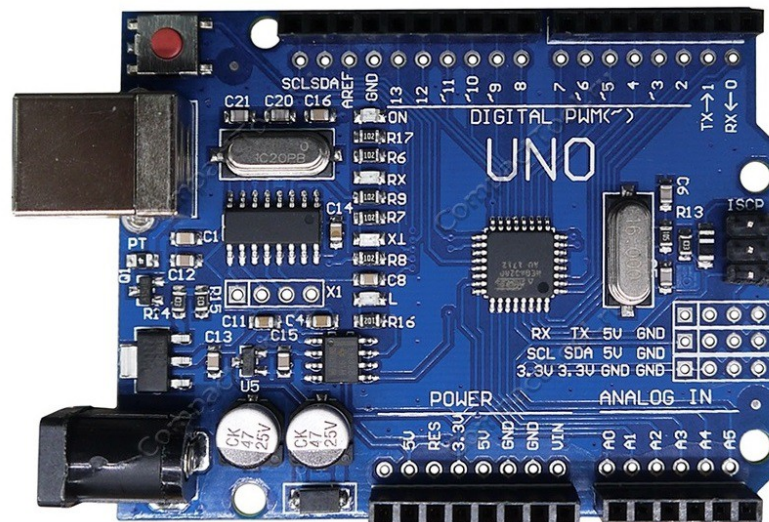


Рисунок 2.1 – Мікроконтролер Arduino Uno

Таблиця 2.1 – Характеристика плати Arduino Uno

Параметр	Значення
Мікроконтролер	ATmega328
Робоча напруга	5 В
Вхідна напруга (рекомендований)	7-12 В
Вхідна напруга (граничне)	6-20 В
Цифрові Входи / Виходи	14 (з них 6 можуть використовуватися в якості ШІМ виходів)
Аналогові входи	40 мА
Постійний струм через вхід / вихід	50 мА
Флеш-пам'ят	32 КБ з яких 0.5 КБ використовуються завантажувачем
ОЗУ	8 КБ

Arduino створено в інституті проектування як простий інструмент для швидкого аналізу прототипу, націлений на студентів без досвіду в електроніці та програмуванні. Як тільки ця ідея стала широко розповсюджуватися, платформу Arduino стали змінювати, що б адаптуватися

для нових потреб і проблем, диференціюючи свої пропозиції від простих 8-разрядних плат до продуктів для додатків IoT, переносних плат, плат придатних для 3D друку і вбудованих середовищ. Всі плати Arduino з повністю відкритим вихідним кодом, що дозволяє користувачеві створити їх незалежними, і в кінцевому рахунку адаптувати під власні потреби [23]. Опис цифрових входів/виходів Arduino Uno (рис 2.2).

1 – живлення USB, 2 – живлення Barrel Jack, 3 – стабілізатор напруги, 4 – кварцовий генератор, 5 – перезавантаження Arduino, 6 – 3.3В, 7 – 5В, 8 – GND, 9 – Vin, 10 – аналогові контакти, 11 – основний мікроконтролер, 12 – контакт ICSP, 13– LED індикатор живлення, 14 – TX і RX світлодіоди, 15 – цифровий вхід/вихід, 16 – AREF, 17 – RESET.

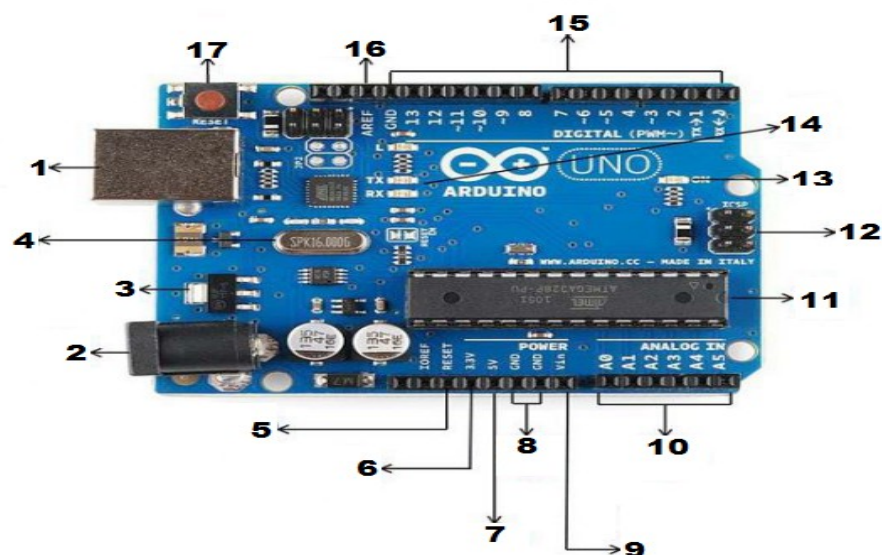


Рисунок 2.2 – Цифрові входи/виходи Arduino Uno

2.2.2 GSM-модуль Neoway M590

GSM-модуль Neoway M590 використовує мережу телефонного зв'язку оператора, для отримання і передачі сигналу на віддалений об'єкт управління. Наприклад, за допомогою СМС команд можна:

- отримувати сповіщення про стан об'єкту через використовувані датчики;
- дізнаватися про спрацювання сигналізації;
- вмикати і вимикати охоронну систему.

За допомогою GPRS, який також підтримує GSM-модуль, можна аналогічні команди обробляти через Internet.

За допомогою такого функціоналу можна організувати автономну сигналізацію на віддаленому об'єкті. Датчики фіксуватимуть зміна стану, а по каналах зв'язку транслюватиметься інформація про це на ваш смартфон. По суті, можна організувати «Розумний будинок» самостійно, поступово додаючи в схему додаткове обладнання.

Працює Neoway M590 (рис. 2.3) на базі плати Arduino Uno. Ніхто не забороняє використовувати плати Nano (mini-схема) або Mega якщо необхідно, але для зручності монтажу пристрою в мінімальній комплектації, досить буде плати Arduino Uno.

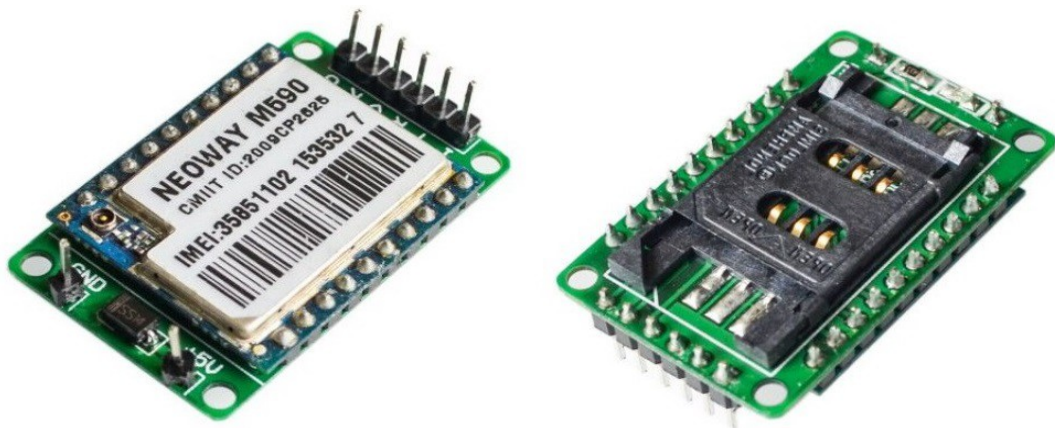


Рисунок 2.3 – GSM-модуль Neoway M590

За передачу GSM або GPRS відповідає модуль, який з'єднується з основною платою. Він розширює можливості Arduino Uno, дозволяючи приймати і здійснювати дзвінки, відправляти SMS, обмінюватися даними через GPRS. На ринку представлені кілька версій відмінних GSM-плат, які

можна зіставляти і програмувати через AT-команди на необхідний функціонал [26, 27]. З характеристиками GSM-модуля можна ознайомитись в таблиці нижче.

Таблиця 2.2 – Характеристика GSM-модуля Neoway M590

Параметр	Значення
Напруга живлення	Від 3,5 до 4,3 В
Робоча частота	900, 1800 МГц
Робоча температура	Від -40°C до +85°C
Пікове навантаження	2 А
Клас GPRS	10 клас
Швидкість передачі даних	9600 Бод

2.2.3 Пасивний інфрачервоний датчик руху HC-SR501

Модуль датчика руху HC-SR501 на основі піроелектричного ефекту складається з PIR-датчика 500BP на мікросхемі BISS0001 і лінзи Френеля, яка використовується для збільшення радіусу огляду та посилення інфрачервоного сигналу. Модуль використовується для виявлення руху об'єктів, випромінюючих інфрачервоне випромінювання.

Управління роботою датчика здійснює мікросхема BISS0001. На платі розташовані два потенціометра, за допомогою першого налаштовується дистанція виявлення об'єктів (від 3 до 7 м), за допомогою другого – затримка після першого спрацьовування датчика (5 - 300 сек) [11]. На рисунку 2.4 зображений датчик руху.



Рисунок 2.4 – Датчик руху HC-SR501

Таблиця 2.3 – Характеристика датчика руху HC-SR501

Параметр	Значення
Напруга живлення	4.5- 20 В
Струм на виході	<60 μ А
Дистанція виявлення	3 – 7 м (налаштовується)
Кут виявлення	До 110°
Тривалість імпульсу при виявленні	5 - 300сек. (Налаштовується)
Робоча температура	від -20 до +80°С
Режим роботи	L - одиночні захоплення, H -повторювані вимірювання

Принцип роботи інфрачервоного датчика руху HC-SR501 не такий простий як може здатися на перший погляд. Головна причина – велика кількість змінних, які впливають на його вхідні і вихідні сигнали (рис. 2.5). Щоб пояснити принцип роботи PIR датчика, ми використовуємо рисунок, наведений нижче [14].

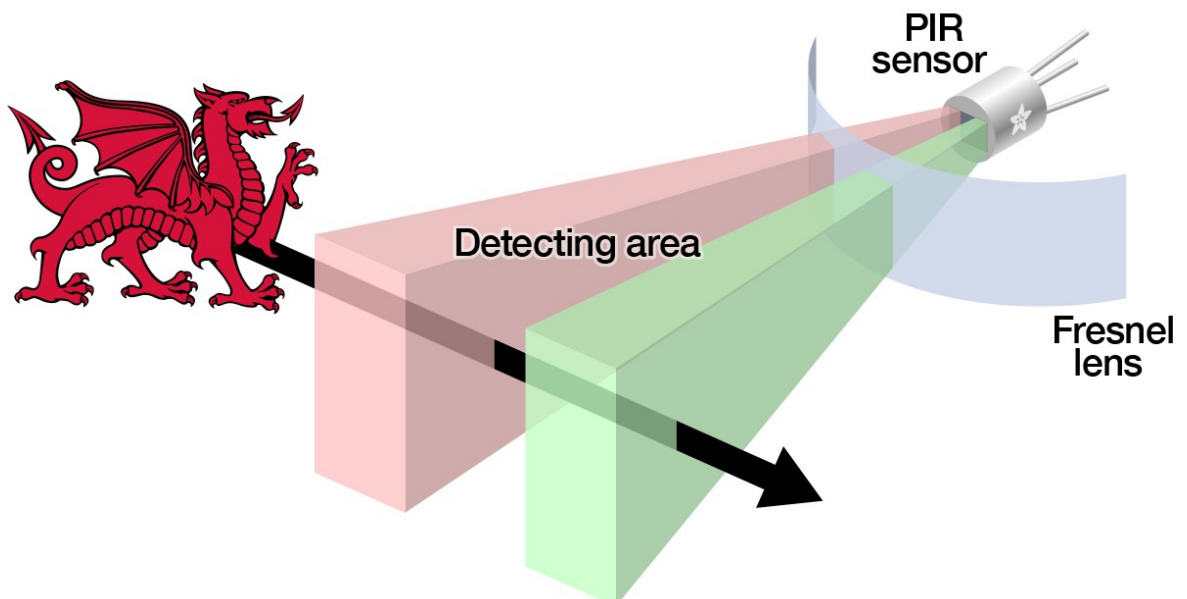


Рисунок 2.5 – Принцип роботи датчика руху

Піроелектричний датчик руху HC-SR501 складається з двох основних частин. Кожна з частин включає в себе спеціальний матеріал, чутливий до інфрачервоного випромінювання. В даному випадку лінзи особливо не впливають на роботу датчика, так що ми бачимо дві ділянки чутливості всього модуля. Коли датчик знаходиться в стані спокою, обидва сенсори визначають однакову кількість випромінювання [21].

Наприклад, це може бути випромінювання переміщення або ж навколишнього середовища. Коли людина проходить повз випромінювання датчика, вона перетинає зону чутливості першого сенсора, в результаті чого на модулі PIR датчика генерується два різних значення випромінювання. Коли людина залишає зону чутливості першого сенсора, значення вирівнюються. Саме зміни в показах двох сенсорів реєструють і генерують імпульси HIGH або LOW на виході.

2.2.4 Датчик широкого спектра газів MQ-2

Датчик широкого спектра MQ-2 визначає концентрацію вуглеводневих газів (пропану, бутану, метану і водню).

А ще його можна використовувати для визначення концентрації алкоголю у повітрі, контролю витоків промислового газу і задимлення. Датчик побудований на базі напівпровідникового газоаналізатора MQ-2 (рис. 2.6). На логічний вихід датчик видає аналоговий сигнал, пропорційний змісту газів в навколишньому середовищі.



Рисунок 2.6 – Датчик широкого спектра газів MQ-2

MQ-2 – це датчик газу типу метал-оксид-напівпровідник, також відомий як хімічний резистор, оскільки виявлення засноване на зміні опору чутливого матеріалу, коли газ вступає в контакт з цим матеріалом. Використовуючи простий ланцюг дільника напруги, можна виміряти концентрацію газу [2].

Таблиця 2.4 – Характеристика датчика широкого спектра газів MQ-2

Параметр	Значення
Напруга живлення	5 В
Реагує на	Пропан, метан, бутан, спирт, водень, дим, LPG
Робоча температура	Від -10 до +55°C
Вихідний сигнал	High/Low і аналоговий
Вимірювання концентрації	200-10000 ppm

2.2.5 Датчик протікання води FC-37

Модуль FC-37 являє собою датчик протікання з високою чутливістю і плату спроектовану на основі компаратора LM393. Мікросхема LM393 обробляє і передає сигнал на мікроконтролер в цифровому або аналоговому видах. Датчик дозволяє виявити появу протікання і вчасно відреагувати на це, наприклад, увімкнути сирену сигналізації. Нижче на рисунку 2.7 зображений датчик протікання води.

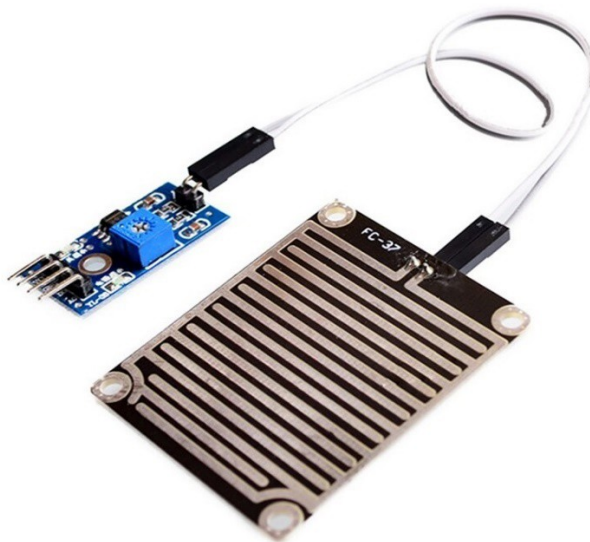


Рисунок 2.7 – Датчик протікання води FC-37

Принцип роботи модуля полягає в зміні вихідної напруги від опору датчика. Якщо плата мокра, опір збільшується, а вихідна напруга зменшується, відповідно, якщо датчик сухий, тоді опір зменшується, напруга збільшується [3].

Таблиця 2.5 – Характеристика датчика протікання води FC-37

Параметр	Значення
Напруга живлення	3,3 - 5 В
Мікросхема	LM393
Типи виходів	Аналоговий, дискретний
Розміри модуля	1,7 x 60 x 39 мм

2.2.6 Датчик відкриття дверей MC-38

Функціональне призначення MC-38 закладено в його назві – датчик відкриття дверей. Нескладна установка і підключення робить цей простий пристрій досить таки дієвим в охоронно-системних комплексах. У середині датчика знаходиться геркон з нормально-розімкнутими контактами. На рисунку 2.8 зображений датчик відкриття дверей.

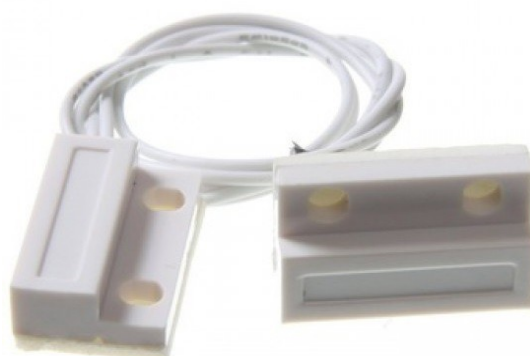


Рисунок 2.8 – Датчик відкриття дверей MC-38

Таблиця 2.6 – Характеристика датчика відкриття дверей MC-38

Параметр	Значення
Максимальна напруга	200 В DC
Контакти	SPST-NP
Відстань спрацьовування	від 15 мм до 25 мм

Принцип роботи MC-38 ґрунтується на підтримці постійного контакту між двома його частинами. Якщо для прикладу взяти дверний отвір, то одну частину датчика встановлюють на дверний короб, а другу на самі двері. При закритих дверях, коли магніт перебуває поруч з герконом, контакти датчика замкнені, як тільки двері відкривається, відбувається розрив контакту і датчик передає імпульс на центральну консоль системи [16].

Обробивши тривожний сигнал, центральна консоль негайно вмикає сирену і відправляє SMS-повідомлення на телефон, номер якого введено в систему.

2.2.7 Модуль активного зумера YL-44

Даний модуль використовується для звукового оповіщення в тих пристроях системи, де для функціонування в обов'язковому порядку потрібний звуковий сигнал.

Зумери поширені в різній побутовій техніці і іграшках, які використовують електронні плати. П'єзо-пищалка перетворює команди, створені на двохбітній системі числення 1 і 0, в звукові сигнали. На рисунку 2.9 зображений модуль активного зумера.

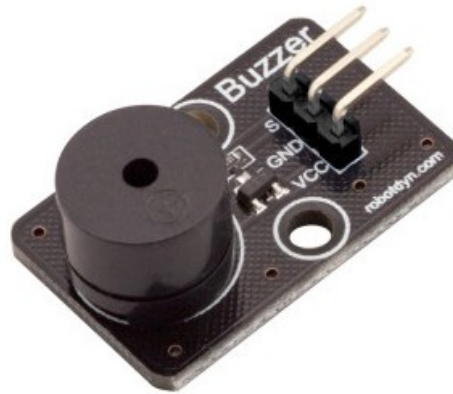


Рисунок 2.9 – Модуль активного зумера YL-44

Принцип дії зумера заснований на п'єзоелектричному ефекті. Згідно з ним, при подачі напруги на зумер він починає деформуватися. При цьому відбуваються удари об металеву пластинку, яка і виробляє «шум» потрібної частоти. Потрібно також пам'ятати, що зумер буває двох видів: активний і пасивний. Принцип дії у них однаковий, але в активному немає можливості змінювати частоту звучання, хоча сам звук голосніше і підключення простіше [16].

2.2.8 Двоканальне реле постійного струму 5VDC-C

Реле представляє з себе електричний перемикач. Такі пристрої використовують електромагніт для механічної роботи перемикача. Реле використовуються там, де необхідно контролювати електричний ланцюг, за допомогою сигналу малої потужності, або там де кілька схем повинні контролюватися одним сигналом. На рисунку 2.10 зображено двоканальне реле постійного струму.

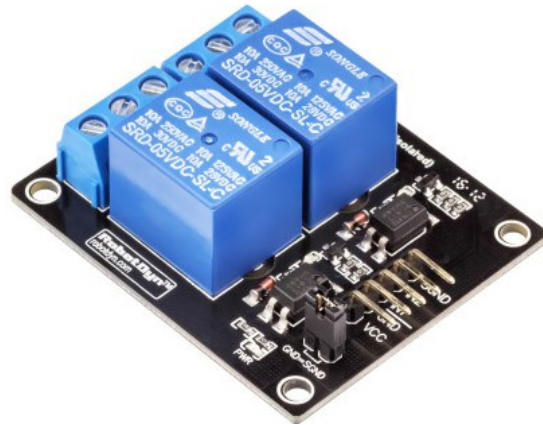


Рисунок 2.10 – Двоканальне реле постійного струму 5VDC-C

Роль реле в системі домашньої автоматизації велика. Реле є сполучним пристроєм між мікроконтролером і електричним приладом, що працює від мережі 220В. Хоч і регулятор напруги, складається всього лише з електромагнітної котушки та найпростішої електронної об'язки, без нього б не вийшло зв'язати мікроконтролер і побутовий або освітлювальний прилад, який постійно потребує у вмикані або вимикані з мережі.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ СИСТЕМИ

Для розробки даного проекту потрібно виділити дві частини, перша частина проекту – розробка програмно-апаратної частини системи, а друга частина – дизайн програмного забезпечення.

Для реалізації програмно-апаратної частини системи необхідно розробити структурну схему системи.

3.1 Структурна схема системи

На рисунку 3.1 зображена ілюстрація структурної схеми підключення всіх компонентів системи інтелектуального моніторингу розумного будинку, представленої в даній роботі.

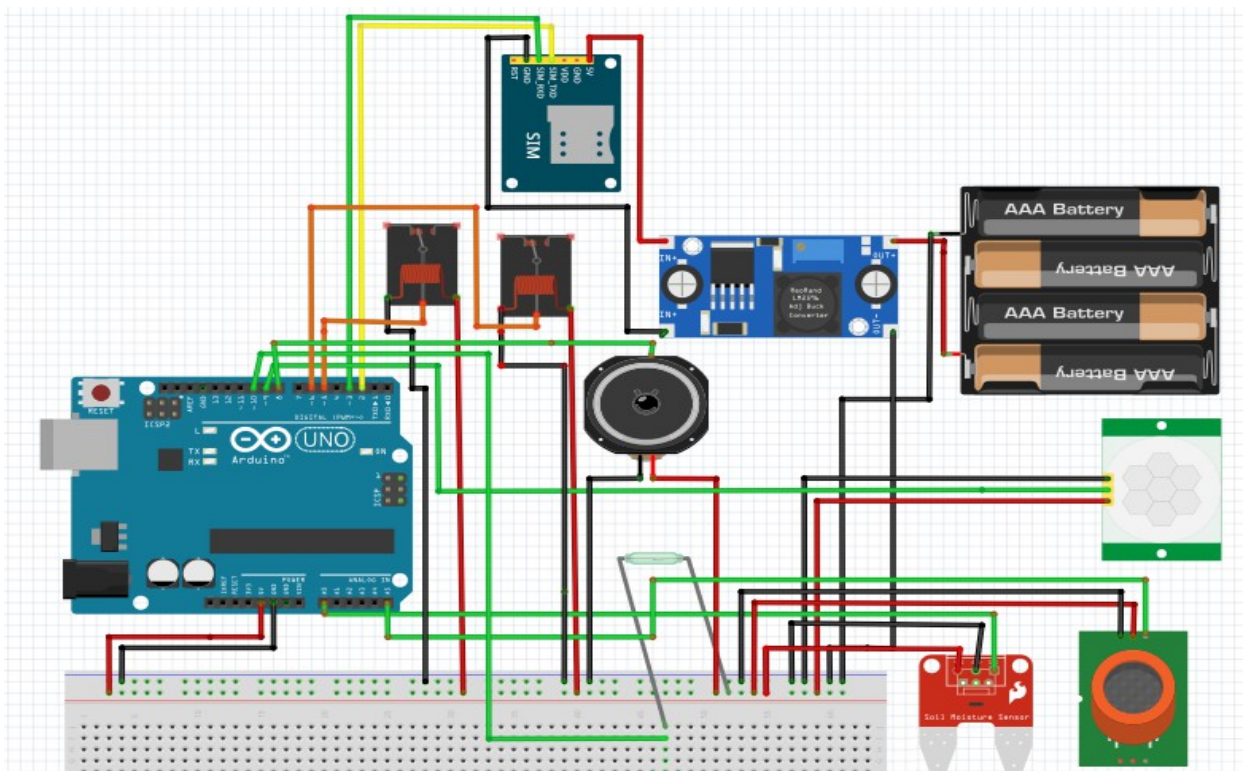


Рисунок 3.1 – Схема підключення всіх компонентів системи інтелектуального моніторингу

Розглянемо підключення кожного елемента системи до нашого мікроконтролера окремо.

Щоб правильно підключити модуль активного звуку і двоканальне реле до мікроконтролера необхідно до «VCC» підключити порт «5V» мікроконтролера для подачі живлення, а до «мінуса» підключити «GND» мікроконтролера, порт модуля звуку «S» і порти двоканального реле «IN1» і «IN2» підключити в один з цифрових виходів мікроконтролера для подачі сигналу (рис. 3.2).

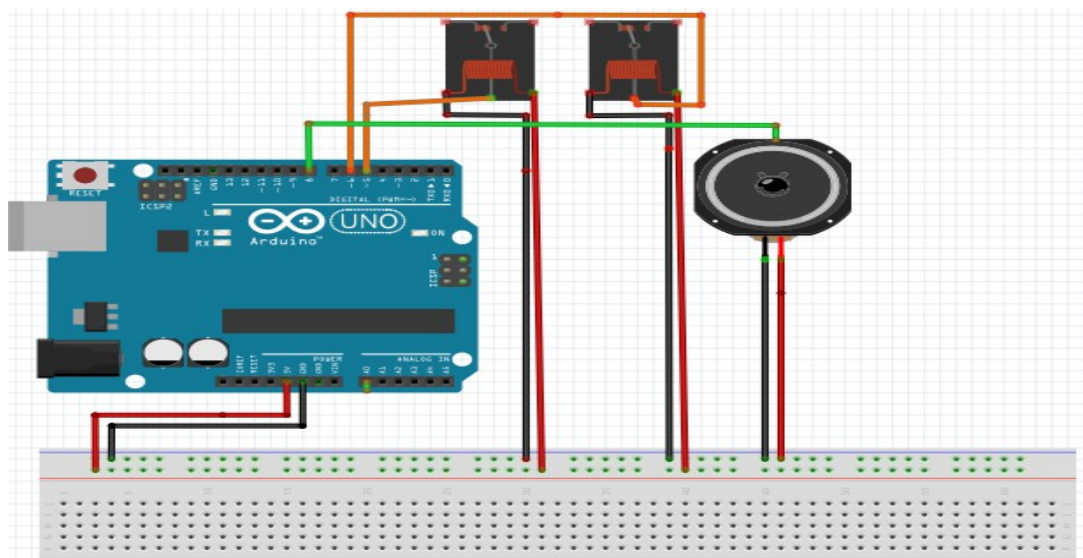


Рисунок 3.2 – Підключення модуля звуку і двоканального реле до Ardiono

Для підключення датчиків до мікроконтролера необхідно до «VCC» портів кожного датчика підключити порт «5V» мікроконтролера для подачі живлення на датчики, до «GND» порту кожного датчика потрібно підключити «GND» мікроконтролера, в порт «OUT» датчика руху та порти «A0» датчиків витoku газу і протікання води, отрібно підключити один з цифрових виходів Arduino Uno для передачі сигналу на датчик і від нього.

На рисунку 3.3 зображено підключення датчика руху до Arduino.

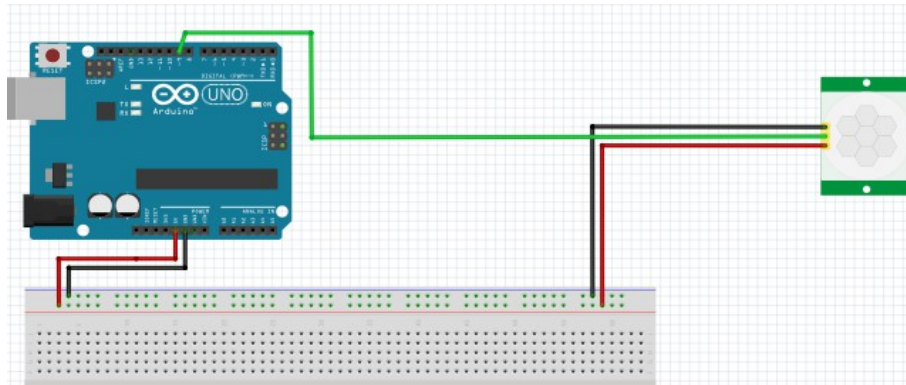


Рисунок 3.3 – Підключення датчика руху до Arduino

На рисунку 3.4 зображено підключення датчика витoku газу до Arduino.

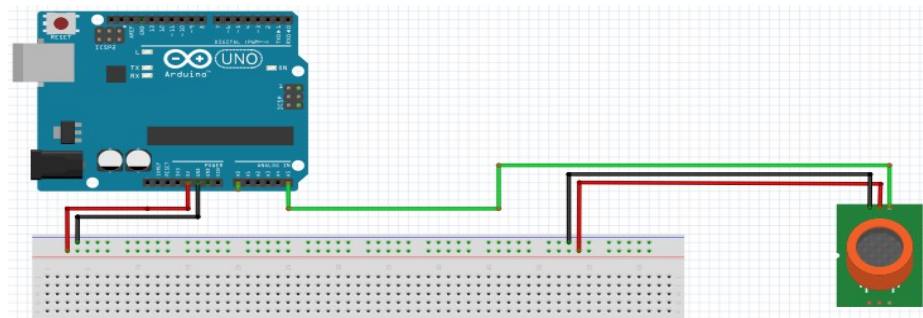


Рисунок 3.4 – Підключення датчика витoku газу до Arduino

На рисунку 3.5 зображено підключення датчика протікання до Arduino.

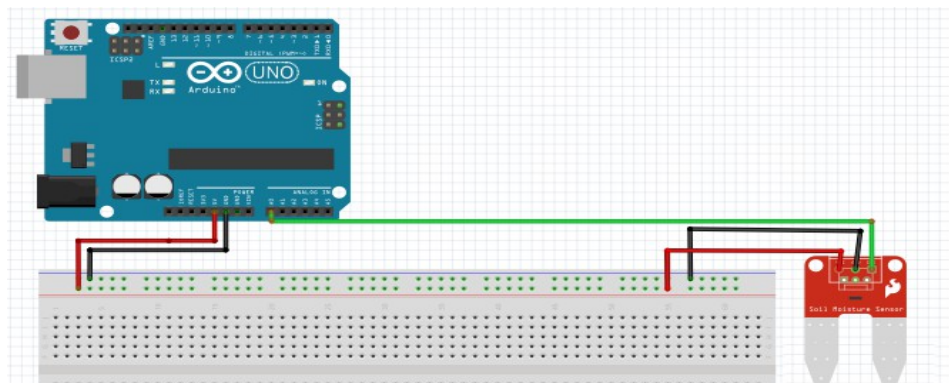


Рисунок 3.5 – Підключення датчика протікання до Arduino

Щоб підключити датчик відкриття дверей до мікроконтролеру необхідно до «плюса» датчика підключити один з цифрових виходів мікроконтролера для подачі живлення та спрацювання, а до «GND» порту датчика необхідно підключити «GND» мікроконтролера (рис. 3.6).

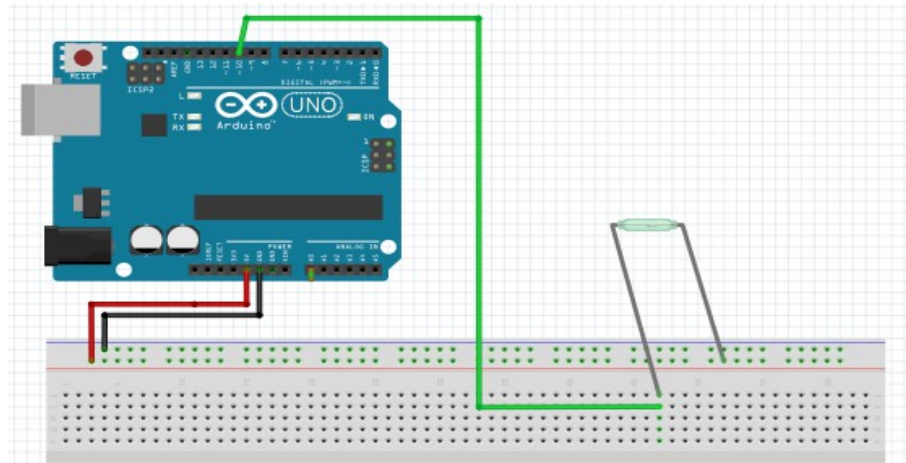


Рисунок 3.6 – Підключення датчика відкриття дверей до Arduino

Для підключення GSM-модуля до мікроконтролера потрібне додаткове підключення понижуючого перетворювача напруги, тому що даний модуль вимагає напруги 3,7 - 4,2В, але мікроконтролер Arduino має на своїх виходах тільки 3,3 і 5В.

Для правильного підключення GSM-модуля до мікроконтролера необхідно «мінус» джерела живлення підключити до «GND» порту мікроконтролера, який підключається до «мінус» перетворювача напруги, «плюс» джерела живлення підключається до «плюс» перетворювача напруги, від перетворювача напруги виходять контакти («плюс» і «мінус») підключаємо до GSM-модулю дотримуючись полярності, «TXD» і «RXD» контакти на GSM -модулі з'єднуємо з цифровими виходами мікроконтролера (рис. 3.7).

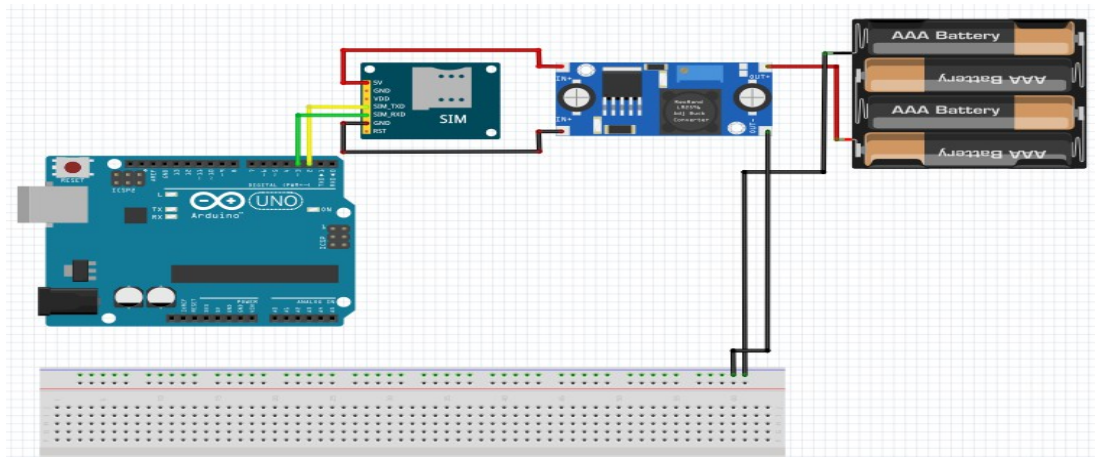


Рисунок 3.7 – Підключення GSM-модуля до Arduino

Таким чином всі окремі частини системи збираються і з'єднуються в одне ціле, створюючи систему охорони і моніторингу.

3.2 Опис роботи системи

Система моніторингу не повинна залежати від наявності в будинку WiFi або електроенергії, тому спроектована з використанням GSM-модуля і кожен елемент пристрою охорони підключений від зовнішнього акумулятора.

Управління системою відбувається за допомогою SMS команд, також по SMS пристрій інформує про стан будинку, якщо власник будинку відправляє SMS-повідомлення з текстом «System status» на номер сім карти, вставленої в GSM-модуль. Модуль у відповідь відправить SMS-повідомлення з інформацією про режим роботи системи та стан датчиків.

Для того щоб увімкнути систему моніторингу відправляється SMS-повідомлення з текстом «System-on» на номер сім-карти, встановленої в GSM-модуль. Модуль відправляє у відповідь SMS-повідомлення з текстом «System-on», яке інформує власника будинку про те, що система моніторингу увімкнена і будинок перебуває під охороною. Для відключення системи моніторингу необхідно відправити SMS-повідомлення з текстом «System-

off». Модуль відправляє у відповідь SMS-повідомлення з текстом «System-off», яке інформує власника будинку про те, що систему моніторингу відключено.

Система обладнана зовнішнім акумулятором ємністю 10000 мАг, що дозволяє пристрою в правильному налаштуванні працювати автономно до 4 місяців.

Також GSM-модуль можна запрограмувати на здійснення дзвінків, що, при підключенні до пристрою мікрофона, дозволяє виробляти прослуховування приміщення при виявленні руху в ньому.

Для дослідницької роботи систему зібрано на макетній платі. На рисунку 3.8 зображено готовий пристрій системи моніторингу без корпусу.

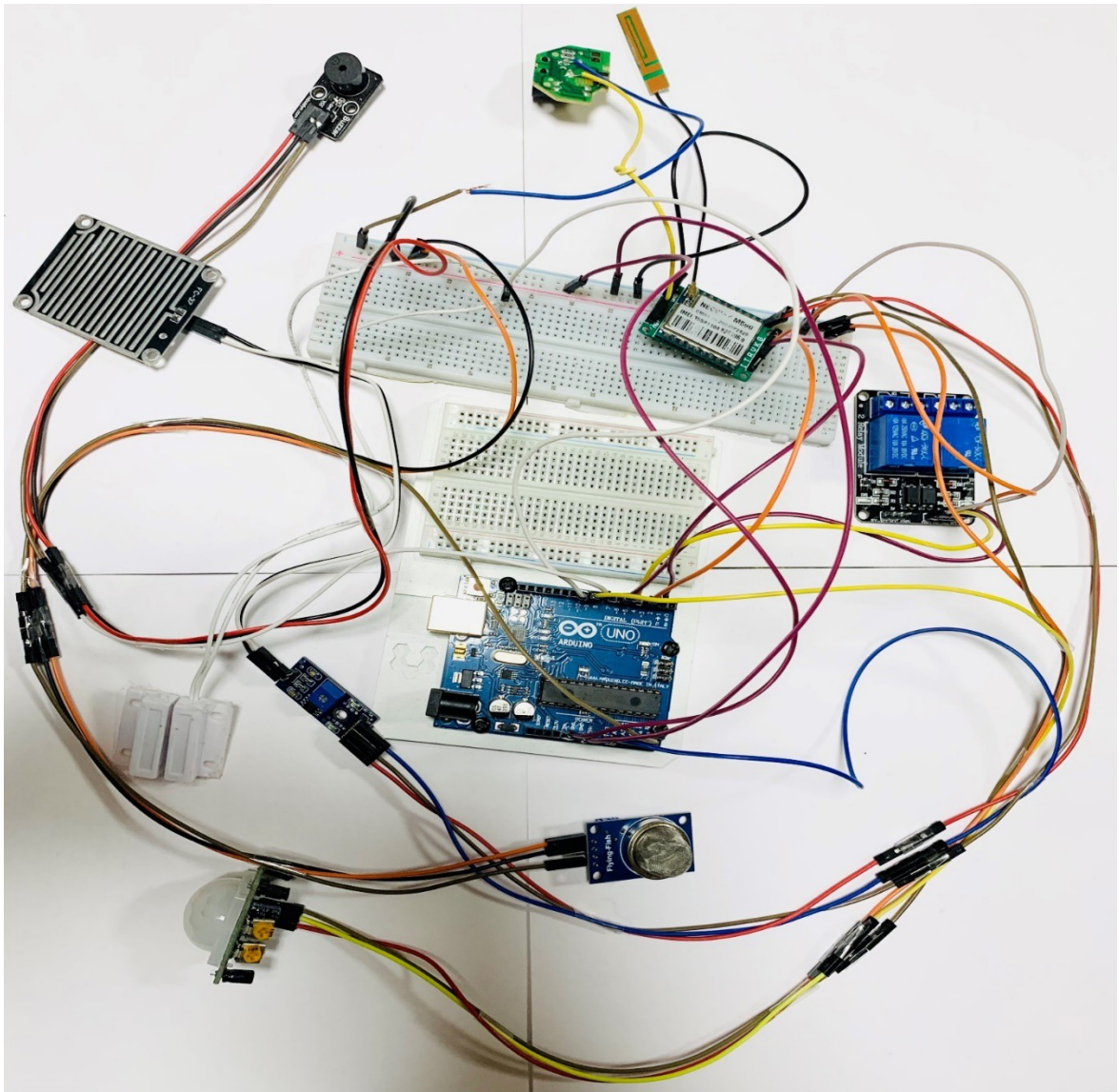


Рисунок 3.8 – Пристрій інтелектуального моніторингу розумного будинку на макетній платі

3.3 Середовище розробки програмного забезпечення Arduino

Програмування для мікроконтролера Arduino Uno здійснюється за допомогою програми на мові програмування C в середовищі розробки ArduinoIDE.

Середовище розробки Arduino складається із вбудованого текстового редактора програмного коду, області повідомлень, вікна виведення тексту(консолі), панелі інструментів з кнопками часто використовуваних команд і декількох меню. Для завантаження програм і зв'язку середовище розробки підключається до апаратної частини Arduino. На рисунку 3.9

загальне представлення середовища розробки .

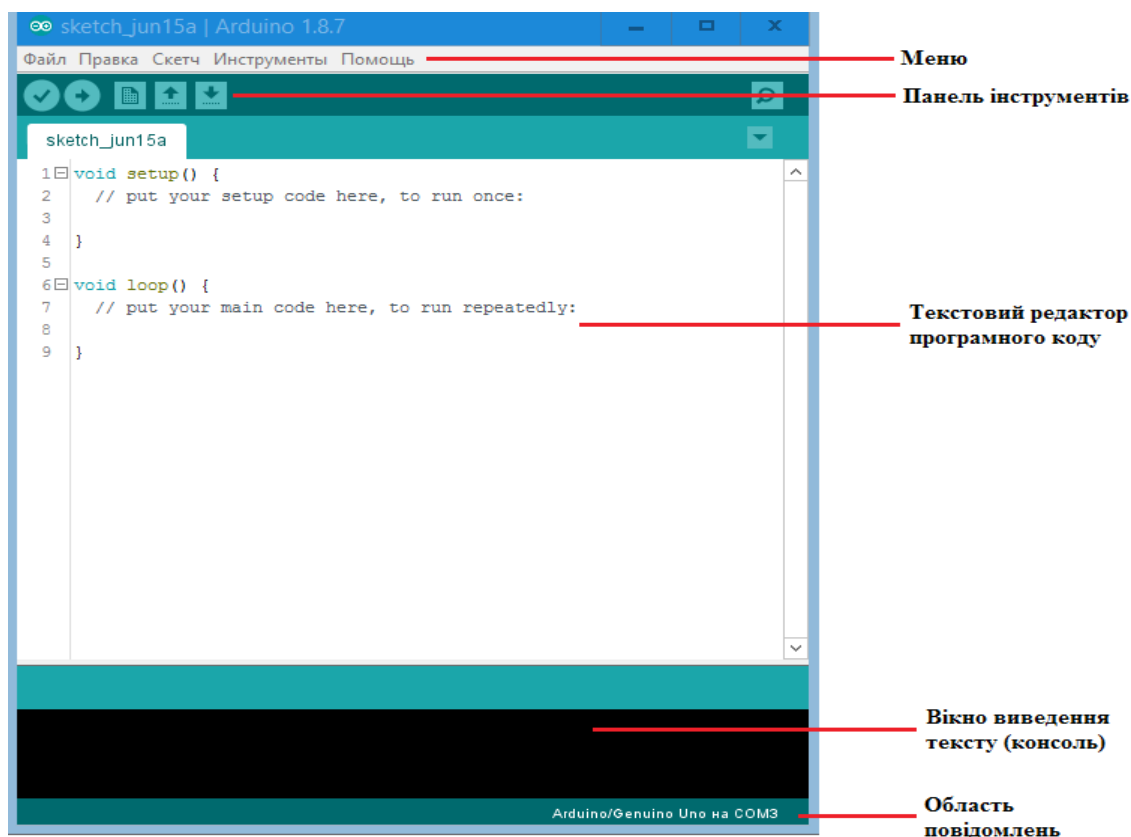


Рисунок 3.9 – Загальне представлення середовища розробки

Програма, яка написана у середовищі Arduino, називається скетч. Скетч пишеться в текстовому редакторі, що має інструменти вирізки/вставки, пошуку/заміни тексту. Під час збереження і експорту проекту в області повідомлень з'являються пояснення, також можуть відображатися виниклі помилки. Кнопки панелі інструментів дозволяють перевірити і записати програму, створити, відкрити і зберегти скетч, відкрити моніторинг послідовної шини [17, 32].

Для того, щоб прошити (запрограмувати) нашу плату Arduino Uno, необхідно зробити наступне:

- 1) підключити плату Arduino Uno до комп'ютера;
- 2) запустити Arduino IDE;
- 3) перейти в пункт меню «Інструменти – Плата» і обрати Arduino Uno;

- 4) перейти в пункт меню «Інструменти – Порт» і обрати потрібний порт, який буде використаний для завантаження програми;
- 5) перейти до панелі інструментів, натиснути кнопку «Перевірити» і дочекатися успішного завершення компіляції;
- 6) перейти до панелі інструментів і натиснути кнопку «Завантажити», скетч буде успішно завантажений в плату.

3.4 Програмна реалізація та опис

В першу чергу нам потрібно підключити бібліотеку <SoftwareSerial.h> яка дозволяє програмно створювати кілька послідовних портів, вказавши TX і RX. Далі використовуємо #define pirPin для оголошення змінної датчика руху, і #define MASTER використовуємо для перевірки номера телефону з якого відправлялося повідомлення на GSM-модуль, якщо повідомлення прийшло з іншого номера, система реагувати не буде.

Також, оголошуємо змінні для всіх датчиків: датчик витoku газу – gassensorpin, датчик протікання води – water, датчик відкриття дверей – door_sensor, модуль активного звуку – buzzer и реле - relay1, relay2.

Лістинг 3.1 – Оголошення бібліотеки і змінних системи

```
#include <SoftwareSerial.h>
SoftwareSerial mySerial(2, 3); // RX, TX
#define pirPin 9
#define MASTER "+380950200402"
int Count = 0;
int relay1 = 6;
int relay2 = 5;
int relay3 = 4;
int relay4 = 7;
const int gassensorpin = A5;
```

```
int gassensorvalue = 0;
int water = A0;
unsigned int waterValue = 0;
int Door_sensor = 10;
int Door_val = 0;
int buzzer = 8;
```

Функція `void setup()` – це функція для задання налаштувань роботи Arduino, вона викликається 1 раз у початку роботи. У ній встановлюється швидкість обміну даними по послідовному порту, час на ініціалізацію GSM-модуля, режим кодування СМС і режим кодування тексту, а також ініціалізація змінних і вмикання системи моніторингу.

Лістинг 3.2 – Функція `void setup()`

```
void setup() {

    gasSensorState = false;
    waterState = false;
    doorState = false;
    pirState = false;
    systemStatus = true;

    pinMode(pirPin, INPUT);
    pinMode(Door_sensor, INPUT);
    pinMode(relay1, OUTPUT);
    pinMode(relay2, OUTPUT);
    pinMode(relay3, OUTPUT);
    pinMode(relay4, OUTPUT);
    delay(2000);

    Serial.begin(9600);
    Serial.println("Signalization v1.0");
    mySerial.begin(9600);
```

```
mySerial.println("AT+CMGF=1");  
delay(100);  
mySerial.println("AT+CSCS=\"GSM\"");  
delay(100);  
mySerial.println("AT+CNMI=2,2");  
}
```

Після `void setup()` використовується функція `void loop()` в якій розміщені команди, які будуть використовуватися увесь час доки запущена Arduino послідовно – від початку до кінця, з кінця виконання перейде на початок.

Після відправки повідомлення на GSM-модуль, система виявляє повідомлення і порівнює номер телефону з номером власника будинку, якщо повідомлення від власника, то система починає читати вхідне SMS-повідомлення, і якщо виявлено кодове слово «System-off», система у відповідь відправляє SMS-повідомлення власнику будинку з текстом «System off» і вимикає роботу системи, включення системи працює за таким же алгоритмом, тільки відправляти SMS-повідомлення ми будемо з текстом «System-on», але якщо повідомлення відправлене на GSM-модуль не від власника будинку, ніяких дій відбуватися не буде (рис. 3.10).

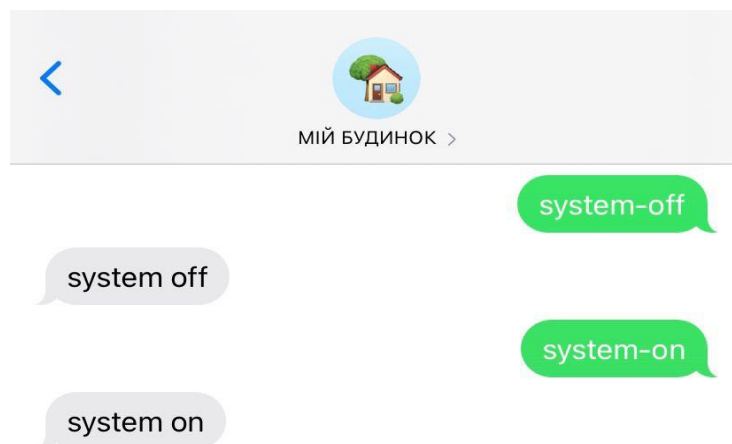


Рисунок 3.10 – Вмикання і вимикання системи моніторингу

Лістинг 3.3 – Вмикання і вимикання системи моніторингу

```
if (message.indexOf("+CMT") > -1) {  
    if (message.indexOf(MASTER) > -1) {  
        Serial.println("--- MASTER SMS DETECTED ---");  
        if (message.indexOf("System-off") > -1) {  
            Serial.println("System off");  
            mySerial.println("AT+CMGS="+380950200402+"\");  
            delay(100);  
            mySerial.print("System off");  
            mySerial.print((char)26);  
            systemStatus = false;  
        }  
        if (message.indexOf("System-on") > -1) {  
            Serial.println("System on");  
            mySerial.println("AT+CMGS="+380950200402+"\");  
            delay(100);  
            mySerial.print("System on");  
            mySerial.print((char)26);  
            systemStatus = true;  
        }  
    }  
}
```

Далі якщо GSM-модуль виявляє вхідне SMS-повідомлення з текстом «Status», він перевіряє чи активна зараз система, також відбувається опитування стану всіх датчиків і після цього система відправляє SMS-повідомлення про стан кожного датчика і системи. Це виглядає приблизно так (рис. 3.11).

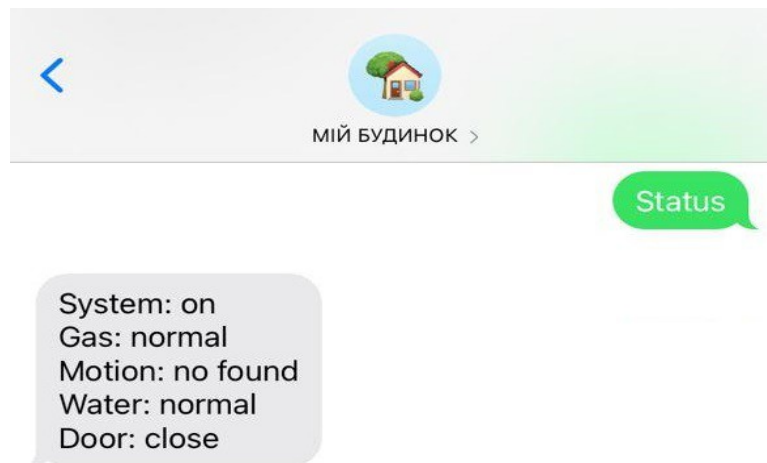


Рисунок 3.11 – Реагування GSM-модуля на повідомлення «Status»

Лістинг 3.4 – Визначення статусу системи

```

if (message.indexOf("Status") > -1) {
    Serial.println("Status");
    mySerial.println("AT+CMGS="+380950200402+"\n");
    delay(100);
    if (systemStatus) {
        mySerial.print("System: on\n");
        Serial.println("System: on");
    }
    else {
        mySerial.print("System: off\n");
        Serial.println ("system off");
    }
    gassensorvalue = analogRead(gassensorpin);
    if (gassensorvalue >= 600) {
        mySerial.print("Gas: alarm\n");
        Serial.println ("Gas: alarm");
    }
}

```

Продовження лістингу 3.4 визначення статусу системи.

```

else {
    mySerial.print("Gas: normal\n");
    Serial.println ("Gas: normal");
}

```

```

}
int pirVal = digitalRead(pirPin);
if (pirVal == HIGH){
    mySerial.print("Motion: found\n");
    Serial.println ("Motion: found; ");
}
else {
    mySerial.print("Motion: no found\n");
    Serial.println ("Motion: no found");
}
waterValue = analogRead(water);
if (waterValue < 300) {
    mySerial.print("Water: alarm\n");
    Serial.println ("Water: alarm");
}
else {
    mySerial.print("Water: normal\n");
    Serial.println ("Water: normal");
}
Door_val = digitalRead(Door_sensor);
if (Door_val == LOW) {
    mySerial.print("Door: open\n");
    Serial.println ("door open");
}
else {
    mySerial.print("Door: close\n");
    Serial.println ("Door: close");
}
mySerial.print((char)26);
}

```

Також, коли система активна, активні і все її датчики, при спрацьовуванні будь-якого з датчиків, система негайно вмикає гучну сигналізацію і відправляє відповідне SMS-повідомлення власнику будинку (рис. 3.12).

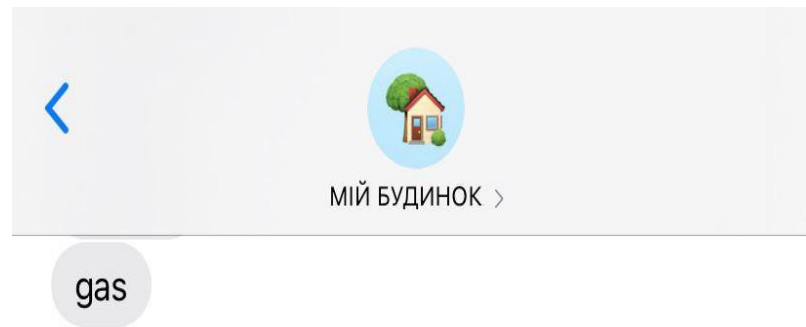


Рисунок 3.12 – Реагування системи на витік газу

Лістинг 3.6 – Реагування системи на витік газу

```

gassensorvalue = analogRead(gassensorpin);
  if (gassensorvalue >= 600) {
    if (!gasSensorState) {
      mySerial.println("AT+CMGS=\"+380950200402\"");
      delay(100);
      mySerial.print("gas");
      mySerial.print((char)26);
      Serial.println("ok");
      tone(buzzer, 1915);
      gasSensorState = true;
    }
    digitalWrite(relay1, LOW);
    delay(5000);
  }
  else {
    digitalWrite(relay1, HIGH);
    noTone(buzzer);
    gasSensorState = false;
  }

```

3.5 Опис алгоритму роботи пристрою

Після розробки програмного коду було розроблено повний і детальний алгоритм роботи пристрою.

Перша частина структурної схеми – це ініціалізація яка виконується один раз при включенні системи і більше не виконується (рис. 3.13).

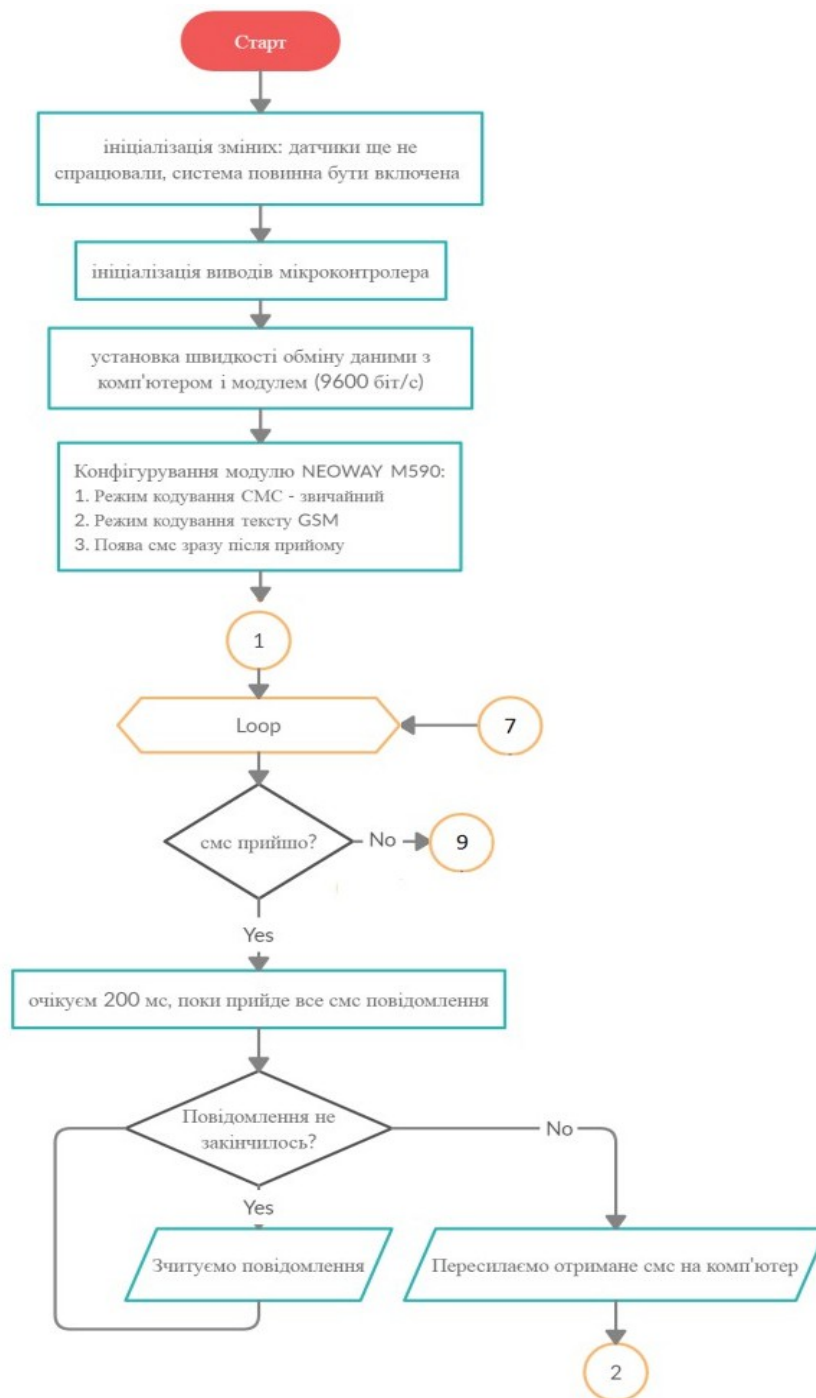


Рисунок 3.13 – Структурна схема ініціалізації системи

Друга частина структурної схеми – це аналіз отриманих SMS-повідомлень на GSM-модуль (рис. 3.14).

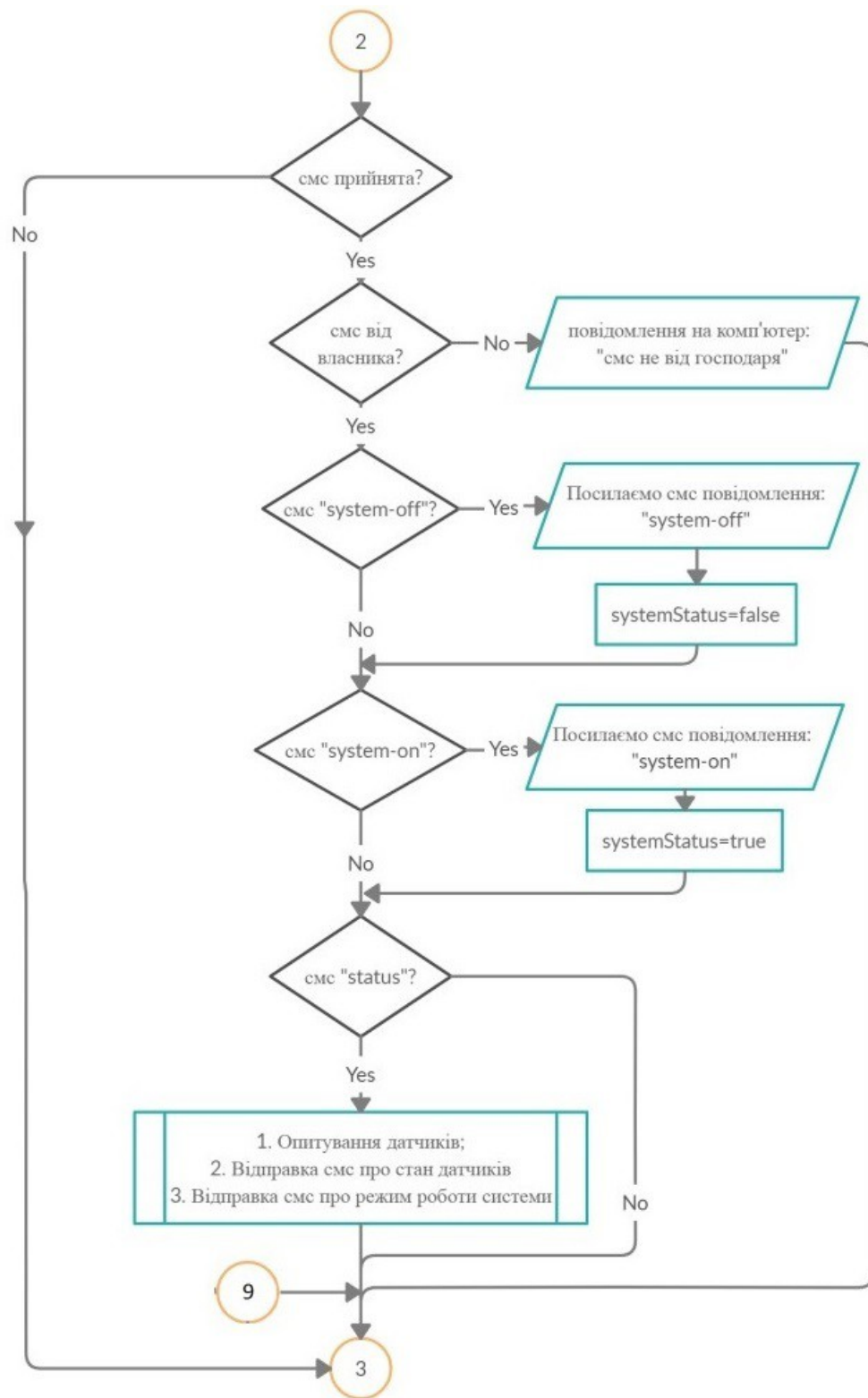


Рисунок 3.14 – Структурна схема аналізу отриманих SMS-повідомлень

Третя частина структурної схеми – це алгоритм роботи датчика витоку газу (рис. 3.15).

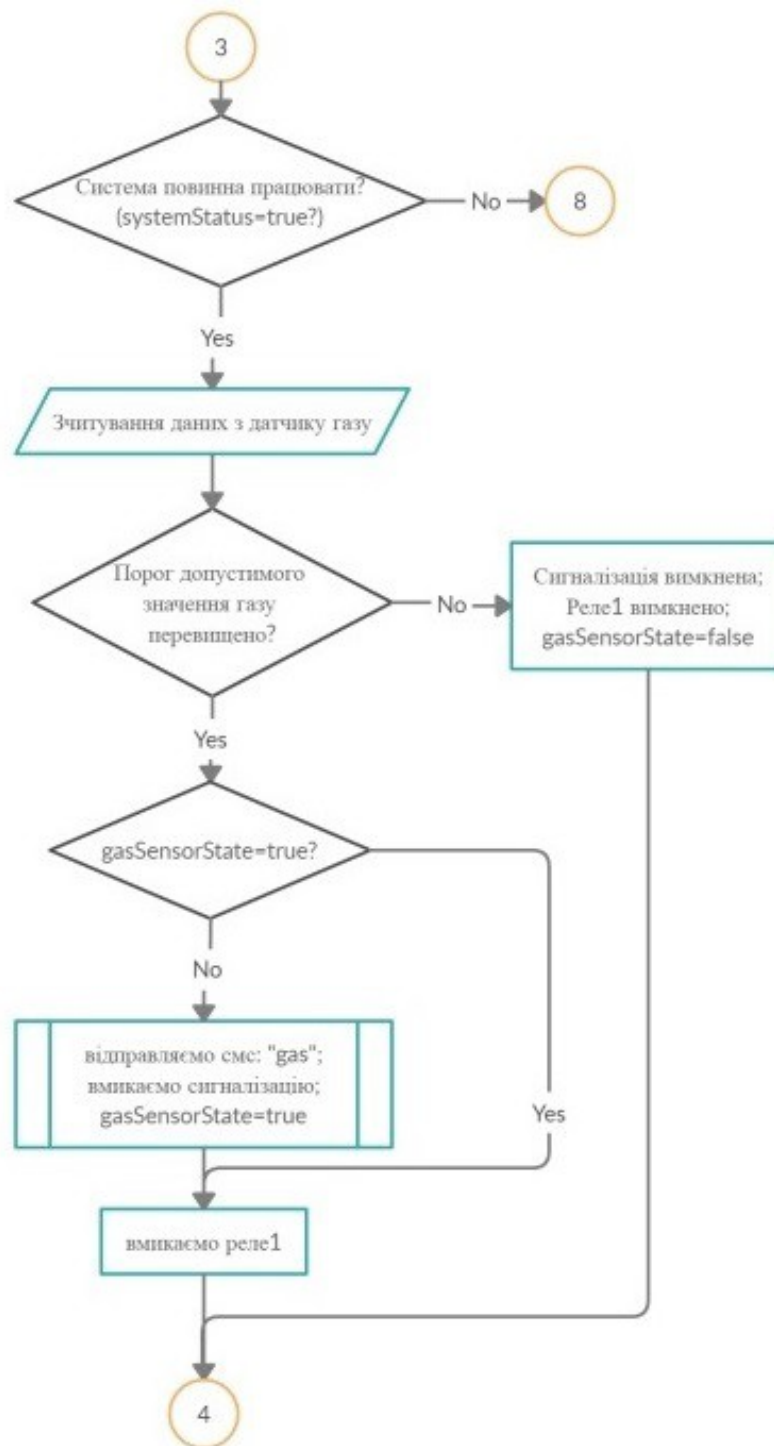


Рисунок 3.15– Структурна схема датчика витоку газу

Четверта частина структурної схеми – це алгоритм роботи датчика руху (рис. 3.16).

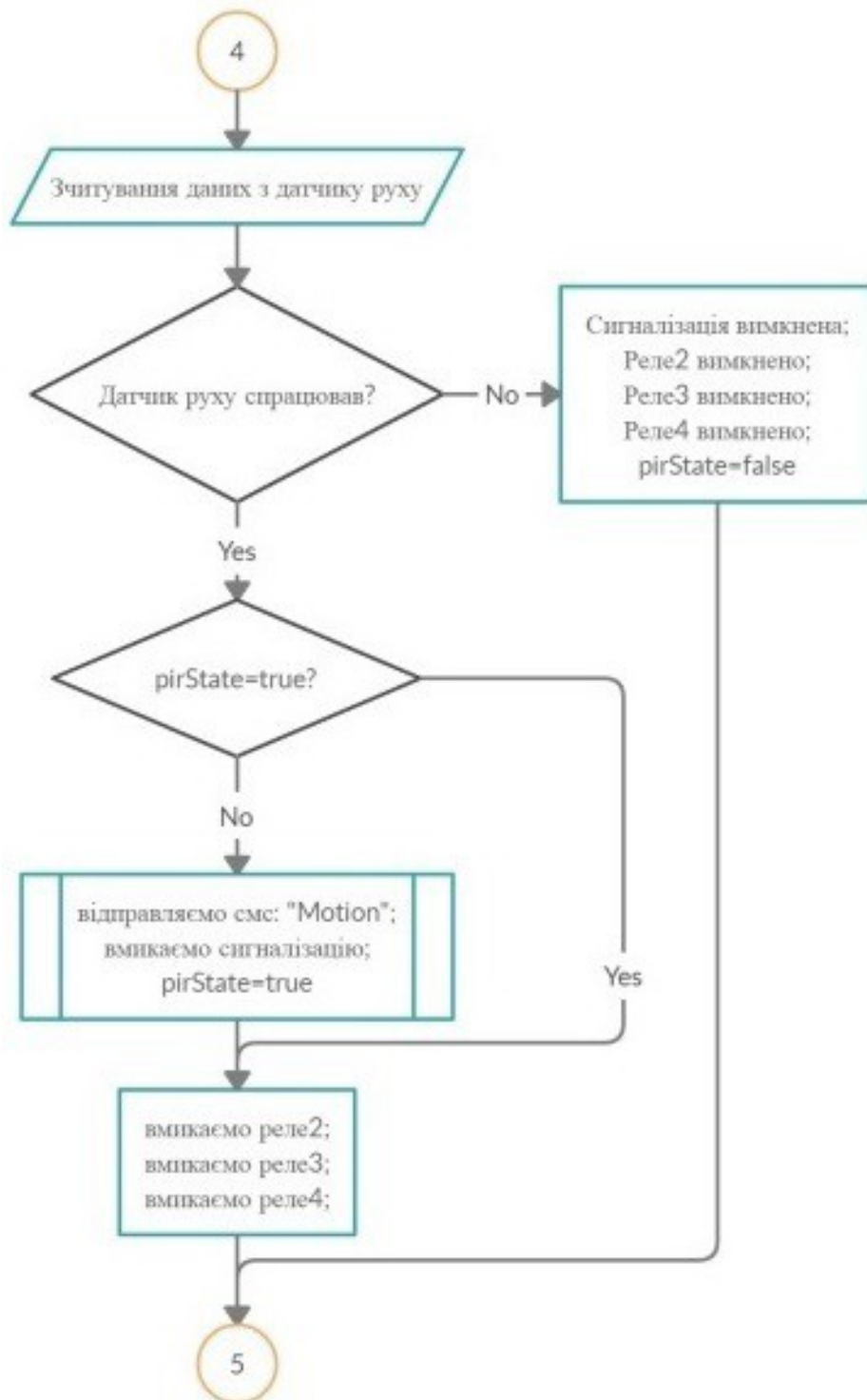


Рисунок 3.16– Структурна схема датчика руху

П'ята частина структурної схеми – це алгоритм роботи датчика протікання води (рис. 3.17).

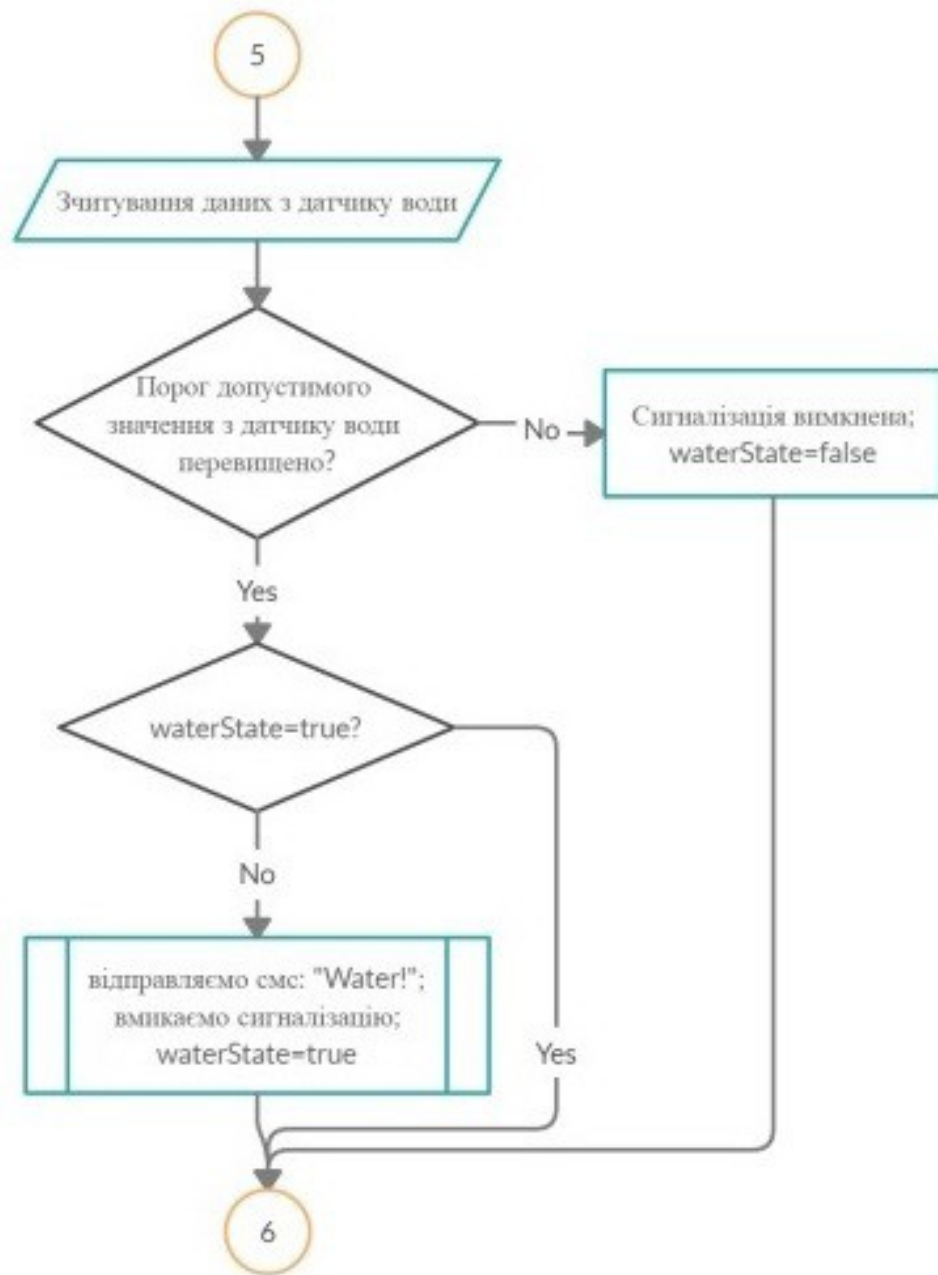


Рисунок 3.17 – Структурна схема датчика протікання води

Шоста частина структурної схеми – це алгоритм роботи датчика відкриття дверей (рис. 3.18).

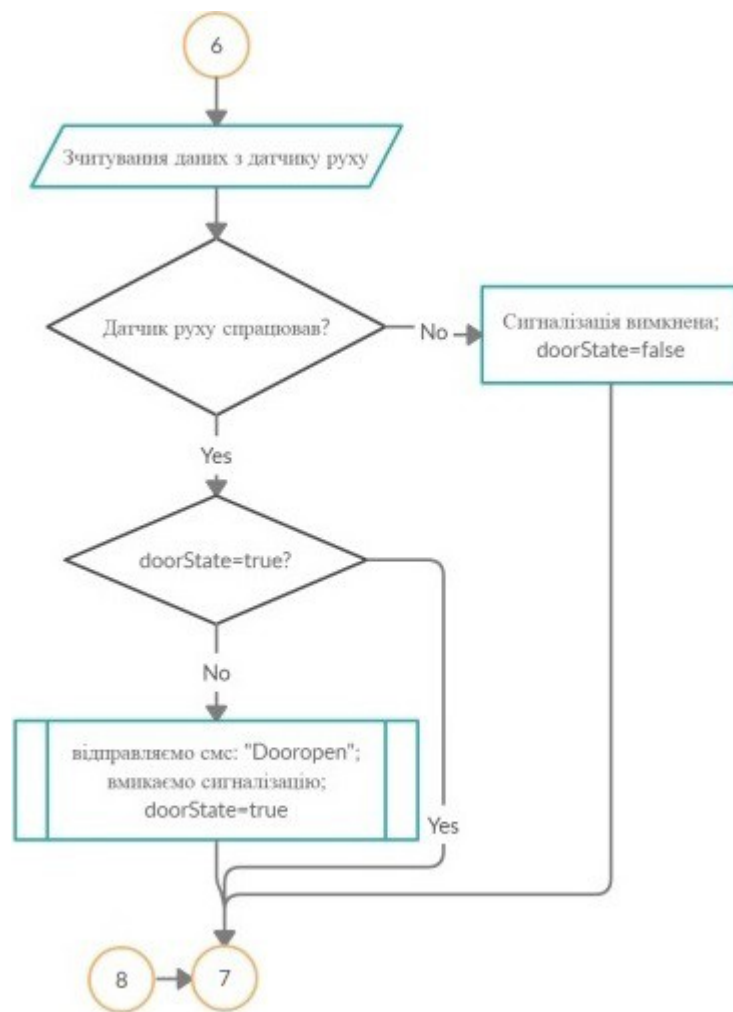


Рисунок 3.18 – Структурна схема датчика відкриття дверей

3.6 Надійність пристрою моніторингу та охорони

Однією з найважливіших завдань при проектуванні системи охорони є розробка модулів і пристроїв, здатних виконувати покладені на них функції протягом тривалого періоду часу без збоїв і необхідності ремонту, настройки або заміни. Надійність описує можливість системи або компонента функціонувати при встановлених умовах протягом встановленого періоду часу. Надійність може також описувати можливість функціонувати в зазначений момент або інтервал часу.

Збій в роботі системи може бути викликаний декількома причинами: виходом з ладу компонентів системи, обривом зв'язку і деякими іншими. Однак для користувача системи моніторингу та охорони не має значення, чому система перестала функціонувати. Власник будинку має бути гарантований певний проміжок часу, протягом якого показники якості обслуговування не будуть падати нижче заданих. Цей проміжок повинен бути досить великим.

Збої в роботі системи можуть обернутися колосальними втратами для користувача даної системи. Таким чином, актуальними є питання збільшення середнього часу напрацювання на відмову системи і збільшення ймовірності того, що система буде в працездатному стані в проміжках між виконанням профілактичного обслуговування або ремонту.

Середній час напрацювання на відмову і середній час після збою є параметрами вирішення задачі забезпечення надійної і стабільної системи охорони.

Знаючи середній час напрацювання на відмову для кожного елемента системи можна визначити інтенсивність відмов λ кожного елемента за формулою:

(3.1)

Інтенсивність відмов датчика руху:

Інтенсивність відмов мікроконтролера:

Інтенсивність відмов GSM-модуля:

Інтенсивність відмов датчика газу:

Інтенсивність відмов датчика води:

Інтенсивність відмов всієї системи в цілому обчислюється за формулою:

(3.2)

де – інтенсивність відмов кожного елемента системи.

Знаючи інтенсивність відмов всієї системи можна визначити середній час напрацювання на відмову системи за формулою:

(3.3)

Імовірність безвідмовної роботи - імовірність того, що протягом заданого інтервалу часу відмови в системі не виникне. Імовірність

безвідмовної роботи системи визначається за формулою:

$$, \quad (3.4)$$

де - час випробування.

За час випробування візьмемо такі значення: 24 , 720 , 2184 , 8760.

Використовуючи середній час напрацювання на відмову і середній час відновлення після збою , можна обчислити коефіцієнт готовності.

Коефіцієнт готовності - ймовірність того, що система буде в працездатному стані в проміжках між виконанням профілактичного обслуговування або ремонту. Коефіцієнт готовності можна визначити за формулою:

$$(3.5)$$

Порівнявши розрахункові параметри з нормативними показниками були зроблені висновки про стан надійності системи. Так як середній час напрацювання на відмову системи складає більше 350 діб і коефіцієнт готовності становить понад 0,99, то дану систему безпеки можна вважати надійною [1].

ВИСНОВКИ

В рамках дослідницької роботи було розглянуто поняття «Інтернет речей», можливість підключення великої кількості пристроїв між собою і їх взаємодія. Були досліджені системи охорони будинків, такі як системи відеоспостереження, системи контролю точок входу і виходу, системи контролю датчиком руху, системи контролю витoku газу і протікання води.

Для реалізації було обрано використовувати платформу Arduino з набором необхідних датчиків, а також GSM-модуль для передачі даних. Проаналізовані їх параметри а також переваги над аналогами. Розроблено програмне забезпечення в Arduino IDE для прошивки мікроконтролеру цієї системи.

Таким чином, варто відзначити, що поставлені цілі і завдання по створенню системи моніторингу будинку досягнуті повністю, а саме:

- зроблено аналіз сучасних систем автоматизації будинків, результати яких дозволили обґрунтувати вибір інструментальних засобів розробки програмного забезпечення;
- розроблено архітектуру, що включає програмні і апаратні компоненти, відмінною рисою є гнучкість і масштабованість системи;
- розроблено програмно-апаратний комплекс розумного будинку який реалізує запропоновану архітектуру;
- розроблено функціонування системи управління і системи контролю, що дозволяють віддалено в реальному часі контролювати і управляти системою;
- був проведений розрахунок надійності пристрою охорони і зроблено висновок про те, що пристрій можна вважати надійним;
- результати тестування показали, що розроблена система задовольняє вимогам технічного завдання.

Результатом дослідницької роботи є програмно-апаратний продукт – система моніторингу та охорони будинку, що має необхідний набір функціоналу для вирішення поставлених перед нею завдань. У роботі докладно описуються всі комплектуючі системи та принцип їх підключення до мікроконтролеру, також описується принцип роботи самої системи.

Також в майбутньому представлену систему моніторингу і охорони будинку можна розвивати, додатково обладнавши систему відеокамерами для запису того, що відбувається в приміщенні і трансляції відео в реальному часі після спрацьовування датчиків, а також додатково обладнавши GSM-модуль мікрофоном для можливості прослуховування приміщення після спрацьовування датчика руху.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Дружинин В. Г. Надежность автоматизированных систем / Василий Григорьевич Дружинин. – Москва: Энергия, 1977. – 536 с.
2. Датчик широкого спектра газов MQ-2 [Электронный ресурс] // Amperka. – 2018. – Режим доступа до ресурсу: <http://wiki.amperka.ru/продукты:mq2> (дата звернення: 10.09.2020). – Назва з екрана.
3. Датчик протечки и дождя ардуино [Электронный ресурс] // Arduinomaster. – 2019. – Режим доступа до ресурсу: <https://arduinomaster.ru/datchiki-arduino/datchik-protechki-i-dozhdya-v-arduino-opisanie-shemy-sketchi/> (дата звернення: 5.10.2020). – Назва з екрана.
4. Дубровин Д. А. Разработка системы "Умный дом" [Электронный ресурс] / Д. А. Дубровин // Финансовый университет Російської Федерації. – 2017. – Режим доступа до ресурсу: <https://docplayer.ru/40483209-Razrabotka-prototipa-sistemy-umnyu-dom-development-of-a-prototype-of-the-smart-home-system.html> (дата звернення: 21.10.2020). – Назва з екрана.
5. Кашкаров А. П. Справочное пособие по системам охраны с пироэлектрическими датчиками / Андрей Петрович Кашкаров., 2016. – 110 с.
6. Кашкаров А. П. Датчики в электронных схемах: от простого к сложному / Андрей Петрович Кашкаров., 2017. – 202 с.
7. Кашкаров А. П. Электронные системы охраны с пироэлектрическими датчиками и способы их нейтрализации / Андрей Петрович Кашкаров., 2017. – 97 с.
8. Кашкаров А. П. Системы видеонаблюдения. Практикум / Андрей Петрович Кашкаров., 2017. – 154 с.
9. Недостатки "Умного дома" [Электронный ресурс] // Электрик Инфо. – 2017. – Режим доступа до ресурсу: <http://elektrik.info/main/voprosy/398-nedostatki-umnogo-doma.html> (дата звернення: 16.10.2020). – Назва з екрана.

10. Охранная сигнализация. Что выбрать: пультовую, автономную или GSM-сигнализацию? [Электронный ресурс] // FORTER. – 2016. – Режим доступа до ресурсу: <https://www.forter.com.ua/news-and-articles/ohrannaja-signalizacija-cto-vybrat-pultovuju-avtonomnuju-ili-gsm-signalizaciju/> (дата звернення: 30.10.2020). – Назва з екрана.
11. Пироэлектрический инфракрасный (PIR) датчик движения и Arduino [Электронный ресурс] // Arduino-DIY. – 2016. – Режим доступа до ресурсу: <https://arduino-diy.com/arduino-piroelektricheskiy-infrakrasnyy-PIR-datchik-dvizheniya> (дата звернення: 03.11.2020). – Назва з екрана.
12. Протокол X10 [Электронный ресурс] // IQhome. – 2015. – Режим доступа до ресурсу: <https://www.iq-home.ru/tech/x10.html> (дата звернення: 9.11.2020). – Назва з екрана.
13. Системы безопасности «умного дома» [Электронный ресурс] // ВИРА-АРТСТРОЙ. – 2019. – Режим доступа до ресурсу: <https://www.ereмонт.ru/enc/engineer/clever/security-system-smart-home.html> (дата звернення: 13.11.2020). – Назва з екрана.
14. Сукачев Д. В. Инфракрасные датчики движения и присутствия [Электронный ресурс] / Д. В. Сукачев // Энергосовет. – 2010. – Режим доступа до ресурсу: http://www.energosoвет.ru/bul_stat.php?idd=43 (дата звернення: 18.11.2020). – Назва з екрана.
15. Сэмюэл Г. Интернет вещей. Будущее уже здесь / Грингард Сэмюэл., 2016. – 188 с. – (Альпина Паблишер).
16. Тесля Е. В. «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире / Елена Владимировна Тесля., 2008. – 224 с.
17. Улли С. Программирование микроконтроллерных плат Arduino/Freeduino / Соммер Улли., 2017. – 256 с.
18. An overview of home automation systems [Электронный ресурс] // IEEE. – 2016. – Режим доступа до ресурсу:

- <https://ieeexplore.ieee.org/document/7791223> (дата звернення: 25.11.2020). – Назва з екрана.
19. Arduino Education [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: <https://www.arduino.cc/education> (дата звернення: 27.11.2020). – Назва з екрана.
20. Arduino Uno [Електронний ресурс]. // Arduino. – 2020. – Режим доступу до ресурсу: <https://doc.arduino.ua/ru/hardware/Uno> (дата звернення: 25.11.2020). – Назва з екрана.
21. Arduino и HC-SR501 (датчик движения) [Електронний ресурс] // Вольтик. – 2018. – Режим доступу до ресурсу: <https://voltiq.ru/arduino-and-sensor-hc-sr501/> (дата звернення: 29.11.2020). – Назва з екрана.
22. Banzi M. Getting Started with Arduino / Massimo Banzi., 2015. – 262 с.
23. ElectronicParts «Arduino. Базовый набор» Інструкція користувача, 2015. – 38 с.
24. Garcia M. L. Design and Evaluation of Physical Protection Systems / Mary Lynn Garcia., 2007. – 376 с.
25. Granzer W. P. Security in Building Automation Systems / Granzer. – Munich: Appress, 2018. – 578 с.
26. GSM модуль NEOWAY M590 связь с Ардуино [Електронний ресурс] // stD. – 2016. – Режим доступу до ресурсу: <https://istarik.ru/blog/arduino/68.html> (дата звернення: 30.11.2020). – Назва з екрана.
27. GSM модуль NEOWAY M590 – описание и команды управления [Електронний ресурс] // RadioLaba. – 2015. – Режим доступу до ресурсу: <https://radiolaba.ru/microcontrollers/gsm-modul-neoway-m590-opisanie-i-komandyi-upravleniya.html> (дата звернення: 02.12.2020). – Назва з екрана.
28. Use Evaluation of Thermocoax Piezoelectric Weigh-In-Motion Sensors, 2001. – 80 с.
29. Halonen T. GSM, GPRS and EDGE Performance: Evolution Towards 3G/UMTS / T. Halonen, R. Javier, M. Juan., 2004. – 656 с.

30. Is IoT Security a Ticking Time Bomb? [Электронный ресурс] // SecurityIntelligence. – 2016. – Режим доступа до ресурсу: <https://securityintelligence.com/is-iot-security-a-ticking-bomb/> (дата звернення: 06.12.2020). – Назва з екрана.
31. KNX [Электронный ресурс] // Википедия. – 2006. – Режим доступа до ресурсу: <https://ru.wikipedia.org/wiki/KNX> (дата звернення: 15.10.2020). – Назва з екрана.
32. Purdum J. Beginning C for Arduino: Learn C Programming for the Arduino / Jack Purdum., 2012. – 297 с.
33. Stuckmann P. The GSM Evolution: Mobile Packet Data Services / Peter Stuckmann., 2003. – 256 с.