+ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Розробка охоронної системи «розумного будинку» на основі Arduino»

зі спеціальності *126 Інформаційні системи та технології*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційні системи та технології*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Дмитро ЧЕРНОБАЙ
(підпис)

Виконав: здобувач вищої освіти групи ІСД-41
ЧЕРНОБАЙ Дмитро
(прізвище, ім'я)

Керівник Доктор філософії ДАНИЛЬЧЕНКО Валентина
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Інженерії програмного забезпечення автоматизованих систем
Ступінь вищої освіти Бакалавр
Спеціальність 126 Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедри ІПЗАС
Каміла СТОРЧАК
"___" _____ 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Чернобай Дмитро Олегович
(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Розробка охоронної системи «розумного будинку» на основі Arduino»

керівник кваліфікаційної роботи Данильченко Валентина, Доктор філософії
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024 року № 36.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи _____

3. Вихідні дані до кваліфікаційної роботи
рішення на базі контролерів Arduino;
наукова та технічна література, експлуатаційна документація, нормативні документи.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Постановка завдання: визначення потреби, вимог та загроз.
2. Архітектура системи: вибір Arduino, апаратне та програмне забезпечення.
3. Реалізація та тестування: збірка, тести та аналіз.

4. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 15.04.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення потреби та загроз. Формулювання вимог та обґрунтування.	15.03.2024 р.	
2.	Аналіз наукової та технічної літератури. Вибір Arduino та інших компонентів. Розробка апаратного та програмного забезпечення.	31.03.2024 р.	
3.	Збірка та підключення компонентів. Тестування з'єднань та основних функцій.	10.04.2024 р.	
4.	Оптимізація роботи системи та додаткові функції. Виправлення помилок та усунення недоліків.	25.04.2024 р.	
5.	Збір і аналіз результатів тестування.	10.05.2024 р.	
6.	Оформлення результатів дослідження. Написання та оформлення кваліфікаційної роботи.	15.05.2024 р	
7.	Підготовка доповіді до захисту.	27.05.2024 р.	

Здобувач вищої освіти _____ Дмитро ЧЕРНОБАЙ
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Валентина ДАНИЛЬЧЕНКО
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 66 сторінок, 33 рисунки, 4 таблиці 20 джерел.

Об'єкт дослідження – система охорони за допомогою Arduino.

Предмет дослідження – принципи, методи та технології, що лежать в основі розробки та використання «розумних будинків» на базі Arduino.

Мета роботи - дослідити можливості та переваги використання Arduino для розробки «розумного будинку», а також створити прототип такої системи, який би демонстрував її ефективність та потенційні можливості.

Методи дослідження – аналіз літературних джерел та наукових публікацій з питань безпеки та використання Arduino; експериментальне моделювання та тестування різних конфігурацій та алгоритмів роботи системи; аналіз результатів експериментів та порівняльна оцінка з іншими доступними рішеннями.

Система контролерів Arduino є актуальною та важливою проблемою в сучасному світі, оскільки велика кількість організацій та підприємств стикаються з постійно зростаючим обсягом даних та потребами в ефективному та надійному захисті критично важливих систем.

В роботі досліджено проблему недостатньої ефективності та високої вартості існуючих систем охорони, а також їх складність у встановленні та налаштуванні.

На основі досліджень, проведених в роботі, запропоновано варіант: Розробка системи охорони на базі Arduino, яка забезпечує ефективний моніторинг та реагування на потенційні загрози, при цьому має простоту у встановленні, налаштуванні та використанні, а також доступну ціну.

Галузь використання – Інформаційні системи та технології.

КОНТРОЛЕР ARDUINO, СИСТЕМИ ОХОРОНИ, ЕФЕКТИВНІСТЬ, СКЕТЧ, РЕАГУВАННЯ, АВТОМАТИЗАЦІЯ, RELIABILITY

ЗМІСТ

ВСТУП

Актуальність дослідження. Актуальність дослідження полягає у необхідності вдосконалення систем безпеки та охорони, особливо в умовах зростаючої комплексності загроз та потреби в ефективних, доступних та легко встановлюваних засобах захисту. Розробка «розумного будинку» на базі Arduino відкриває шлях до створення зручних та надійних рішень, що можуть бути використані в різних сферах, починаючи від домашнього використання і закінчуючи комерційними об'єктами, тим самим відповідаючи на зростаючий попит на інтелектуальні системи безпеки.

Контролери Arduino стали популярними завдяки своїй простоті використання та програмування, доступності за низькою ціною, наявності великої спільноти користувачів, яка обмінюється досвідом і знаннями, а також завдяки масовій доступності різноманітних додаткових модулів, які розширюють функціональність платформи. Крім того, Arduino підтримується на різних операційних системах, що робить її доступною для широкого кола розробників, а відкритий код сприяє активному розвитку та внесенню внесків у спільноті.

Вимоги до контролерів Arduino включають надійність, ефективність та простоту використання. Ці контролери повинні бути легкими у програмуванні та монтажі, мати можливість інтеграції з різноманітними датчиками та пристроями, а також забезпечувати стабільну роботу у різних умовах застосування, щоб відповідати вимогам сучасних проектів у галузі автоматизації, IoT та систем безпеки.

Методи дослідження, такі як опрацювання літератури, аналіз експлуатаційної документації та міжнародних стандартів, дозволяють отримати об'єктивну інформацію про можливості та обмеження контролерів Arduino, що сприяє ефективному процесу прийняття рішень при оптимізації системи охорони.

Таким чином, дане дослідження має велике значення для практичного застосування та вирішення актуальних проблем у сфері автоматизованих систем.

Результати цього дослідження допоможуть організаціям підвищити ефективність своїх систем охорони та забезпечити надійність їх функціонування в умовах постійно зростаючих вимог до інформаційних технологій.

Предмет дослідження – принципи, методи та технології, що лежать в основі розробки та використання «розумних будинків» на базі Arduino.

Мета роботи – дослідити можливості та переваги використання Arduino для розробки «розумного будинку», а також створити прототип такої системи, який би демонстрував її ефективність та потенційні можливості.Об’єкт дослідження – система охорони за допомогою Arduino.

Наукові завдання:

порівняння різних методів моніторингу та реагування на потенційні загрози в системах охорони на базі Arduino.

аналіз можливостей оптимізації програмного забезпечення для підвищення швидкодії та ресурсо ємності системи.

вивчення впливу різних типів датчиків на точність та надійність виявлення потенційних загроз.

розробка алгоритмів самодіагностики та виявлення несправностей в системах охорони.

дослідження можливостей інтеграції системи охорони на базі Arduino з іншими "розумними" пристроями та системами.

вивчення питань безпеки та захисту даних у системах охорони на базі Arduino з метою запобігання несанкціонованому доступу та кібератакам.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: розроблено рекомендації щодо проектування «розумного будинку» на базі контролерів Arduino.

1 ТЕОРЕТИЧНИЙ АНАЛІЗ АВТОМАТИЗОВАНИХ СИСТЕМ ОХОРОНИ

1.1 Визначення проблеми в сучасних системах охорони

Актуальність визначення проблеми в сучасних системах охорони надзвичайно важлива. З кожним днем технологічний ландшафт зазнає значних змін, а зловмисники постійно шукають нові шляхи для атак на організації та приватні особи. Визначення проблем допомагає ідентифікувати недоліки та вразливості у сучасних системах безпеки, а також створювати стратегії та рішення для їх подолання. Злочинці швидко адаптуються до нових технологій та використовують нові методи атак, що робить необхідним постійне оновлення та вдосконалення систем безпеки для запобігання втратам даних, фінансовим збиткам та порушенням конфіденційності [1].

З появою нових технологій, таких як Інтернет речей (IoT), обробка великих обсягів даних та штучний інтелект, виникають нові виклики для безпеки інформації та приватності. Визначення проблем у сучасних системах охорони дозволяє не лише реагувати на поточні загрози, а й адаптуватися до майбутніх тенденцій та вимог. Тому, постійне аналізування та визначення проблем в сфері безпеки є критичним елементом для забезпечення ефективного захисту інформації та інфраструктури в умовах швидко змінюючогося технологічного середовища.

Можна описати ряд проблем з якими стикаються сучасні системи охорони, і які можуть бути вирішені або полегшені за допомогою використання мікроконтролера Arduino.

1. Недостатня ефективність інтегрованих систем безпеки, багато сучасних систем охорони можуть бути складними у налаштуванні, неефективними або недостатньо гнучкими для вирішення конкретних потреб підприємства або домашнього користувача. Використання Arduino може допомогти створити більш

гнучкі та індивідуалізовані системи охорони, які відповідають конкретним потребам користувача.

Однією з головних проблем може бути наявність слабких місць у системах безпеки, які роблять їх вразливими перед новими типами кібератак або несподіваними загрозами. Також можуть виникати складнощі з інтеграцією систем безпеки з іншими компонентами інфраструктури, що призводить до порушень у збиранні та обробці даних. Обмежені можливості моніторингу та аналізу можуть ускладнити виявлення загроз та вчасну реакцію на них. Крім того, складність управління та налагодження інтегрованими системами безпеки може викликати затримки у виявленні та вирішенні проблем, а також збільшити загрози безпеці [1].

2. Високі витрати на системи безпеки, традиційні системи охорони часто вимагають значних витрат на обладнання та програмне забезпечення. Використання Arduino та компонентів, що доступні відразу, може допомогти знизити витрати на створення індивідуальних систем охорони.

Високі витрати на системи безпеки є серйозною проблемою для багатьох організацій та підприємств. При впровадженні сучасних систем безпеки, витрати можуть значно зростати через кілька факторів. По-перше, вартість необхідного обладнання та програмного забезпечення може бути високою, особливо якщо це вимагає спеціалізованої технології або ліцензій. Наприклад, вартість мережевих пристроїв, вогнеметів, систем виявлення вторгнень та інших рішень безпеки може становити значну частину бюджету безпеки організації.

По-друге, витрати на інсталяцію та налагодження також можуть виявитися великими. Це включає в себе оплату послуг фахівців з інсталяції та конфігурації, а також можливі витрати на додаткове обладнання для підтримки інтеграції нових систем безпеки. Крім того, витрати на підтримку та обслуговування таких систем можуть виявитися значними у подальшому, оскільки вони включають в себе оплату підписок на оновлення програмного забезпечення, відновлення та заміну обладнання, а також витрати на технічну підтримку та консультування [1].

Зважаючи на ці фактори, очевидно, що високі витрати на системи безпеки становлять серйозну трудність для бізнесу. Витрати можуть перевищувати

бюджетні обмеження та ускладнювати фінансове планування, особливо для менших підприємств та організацій. Тому важливо ретельно аналізувати потреби та можливості перед впровадженням нових систем безпеки, щоб мінімізувати витрати та забезпечити оптимальний баланс між безпекою та фінансовою ефективністю.

3. Складність установки та налаштування систем, багато інтегрованих систем безпеки можуть бути складними у встановленні та налаштуванні.

Використання Arduino та його простого інтерфейсу може полегшити цей процес, дозволяючи користувачам створювати та налаштовувати системи охорони самостійно.

Складність установки та налаштування систем безпеки може стати значним викликом для багатьох організацій. При впровадженні нових систем безпеки, які включають в себе різноманітні пристрої, програмне забезпечення та мережеві компоненти, необхідно враховувати ряд складних аспектів. По-перше, це може включати в себе фізичне розгортання обладнання та його підключення до мережі, що може вимагати спеціалізованих знань та навичок.

Додатково, складнощі можуть виникнути під час налаштування програмного забезпечення, включаючи встановлення та конфігурацію параметрів безпеки. Наприклад, налагодження прав доступу, налаштування правил файрволу та моніторингу мережевого трафіку може вимагати глибоких знань інформаційної безпеки та мережевих технологій.

Важливо враховувати інтеграцію нових систем безпеки з існуючими інфраструктурними рішеннями. Під час налаштування, можуть виникати конфлікти з іншими програмними продуктами або навіть з пристроями, які вже працюють у мережі. Такі конфлікти можуть призвести до зниження ефективності та надійності систем безпеки.

4. Потреба у вищому рівні гнучкості та масштабованості, деякі системи охорони можуть бути недостатньо гнучкими або неможливими у масштабуванні. Потреба у вищому рівні гнучкості та масштабованості в системах безпеки постійно зростає в умовах постійно змінюючогося оточення бізнесу та технологічного

прогресу. Одним з основних факторів, що призводить до цієї потреби, є зростання обсягу даних та різноманітність швидкозмінюваних загроз безпеці. Бізнес-середовище стає все більш динамічним, що вимагає від систем безпеки більшої гнучкості у виявленні та відверненні нових загроз.

З поширенням хмарних технологій та інтернету речей (IoT), масштабність стає ключовою властивістю систем безпеки. Вони повинні бути готові швидко масштабуватися відповідно до зростання обсягу даних та кількості пристроїв, що підключені до мережі. Це може включати в себе автоматизацію процесів масштабування та розгортання нових ресурсів безпеки у відповідь на зростаючі потреби.

Для задоволення цих потреб системи безпеки повинні бути здатні працювати у реальному часі, адаптуватися до нових умов та масштабуватися горизонтально та вертикально. Важливо також мати можливість інтеграції з іншими системами та стандартами безпеки, щоб забезпечити єдність та цілісність захисту даних та інфраструктури. Тільки в такий спосіб організації можуть бути впевнені в тому, що їхні системи безпеки відповідають найвищим стандартам ефективності та надійності [2].

Використання Arduino дозволяє створювати модулярні системи охорони, які можна легко розширювати та адаптувати до зміни потреб користувача. Описуючи проблеми в сучасних системах охорони у контексті розробки систем з використанням Arduino, ви можете підкреслити переваги та можливості використання мікроконтролера для створення більш ефективних, доступних та індивідуалізованих систем охорони.

1.2 Роль контролерів у побудові архітектури систем

Контролери Arduino – це мікроконтролери, які використовуються для створення різноманітних електронних пристроїв та систем, включаючи розумні будинки, робототехніку, медичні прилади та багато іншого. Основною перевагою контролерів Arduino є їхні простота використання, доступність, гнучкість та широкі можливості.

Роль контролерів Arduino у побудові архітектури розумного будинку є критичною та розширеною. Arduino – це відкрита платформа мікроконтролера, яка надає можливості для розробки різноманітних систем автоматизації та управління. У контексті розумного будинку, контролери Arduino виконують ключові функції у зборі, обробці та передачі даних, керуванні підключеними пристроями та виконанні автоматизованих завдань.

По-перше, контролери Arduino можуть використовуватися для збору даних з різних датчиків, таких як датчики температури, вологості, руху та інших параметрів середовища. Ці дані можуть використовуватися для моніторингу та аналізу умов у будинку та виконання певних дій в залежності від зареєстрованих подій.

По-друге, контролери Arduino можуть служити як центральний мозок системи розумного будинку, який керує підключеними пристроями. Вони можуть приймати рішення на основі отриманих даних та відправляти команди до різних пристроїв, таких як освітлення, опалення, системи безпеки та інші.

Крім того, контролери Arduino є дуже гнучкими та можуть інтегруватися з різними пристроями та технологіями. Вони підтримують широкий спектр комунікаційних протоколів, таких як Wi-Fi, Bluetooth, Zigbee тощо, що дозволяє їм взаємодіяти з різними пристроями та сервісами [2].

Контролери Arduino базуються на мікроконтролерах AVR або ARM та мають вбудований процесор, пам'ять для зберігання програмного коду та дані, а також входи та виходи для підключення датчиків, актуаторів та інших електронних пристроїв. Вони поставляються з рядом вбудованих аналогових та цифрових портів, що дозволяє підключати до них різноманітні сенсори, виконавчі пристрої, дисплеї та інші компоненти.

Основна перевага Arduino полягає в його простоті програмування. Для розробки програм для Arduino використовується мова програмування C/C++, яка є однією з найпоширеніших та добре відомих мов програмування. Крім того, Arduino має власне середовище розробки (Arduino IDE), яке має інтуїтивно зрозумілий інтерфейс та широкі можливості для розробки та налагодження програм [2].

Ще однією важливою особливістю контролерів Arduino є їхній відкритий характер та велике спільнота користувачів. Існує безліч різноманітних проектів, бібліотек та документації, що дозволяє швидко засвоїти пристрій та використовувати його в різних сферах.

У контексті розумного будинку, контролери Arduino можуть використовуватися для збору даних з датчиків (наприклад, температури, вологості, руху), керування підключеними пристроями (освітлення, опалення, кондиціонування повітря), виконання автоматизованих завдань та створення різноманітних інтерактивних систем управління. Контролери Arduino можуть бути легко інтегровані з іншими технологіями та сервісами, що робить їх важливим компонентом в сучасних системах розумного будинку [2].

Контроллери Arduino відіграють ключову роль у створенні архітектури розумного будинку, надаючи засоби для збору, обробки та передачі даних, керування підключеними пристроями та реалізації різноманітних автоматизованих функцій. Вони дозволяють створити ефективну та гнучку систему, яка відповідає потребам користувача та може бути легко розширена та налаштована.

1.3 Функції та можливості контролерів Arduino

Плати поділяються на контролери, екрани та аксесуари. Контролер є найважливішою частиною і являє собою плату, на якій встановлений мікроконтролер і записана виконувана програма. Плата є платою розширення і містить різні периферійні пристрої, якими керує контролер. Шилд розміщується поверх контролера, утворюючи своєрідний "сендвіч".

Контролери Arduino Uno, Arduino Leonardo і Arduino Pro - це пристрої на базі 8-бітних мікроконтролерів.

Arduino Due - пристрій на базі мікропроцесора Atmel SAM3X8E ARM Cortex-M3. Це перша плата Arduino на базі 32-розрядного мікроконтролера ARM [3].

Завдяки використанню 32-розрядного ядра ARM, Arduino Due багато в чому перевершує типові плати на базі 8-розрядних мікроконтролерів.

Найважливіші відмінності наступні:

1. 32-бітне ядро дозволяє обробляти 4 байти даних лише за один цикл. Тактова частота складає 84 МГц.

2. 96 КБ пам'яті SRAM; -.

3. 3. 3. 3. Програмна флеш-пам'ять 512 Кб.

Контролер DMA дозволяє звільнити центральний процесор від виконання ресурсоємних операцій з пам'яттю.Arduino YUN - це контролер з інтегрованим Wi-Fi модулем, що працює під управлінням Linux і системи команд Arduino.

Arduino YUN - це Wi-Fi під управлінням класичного Arduino Leonardo (на базі мікроконтролера ATmega32U4) і Linino (дистрибутив GNU/Linux на базі OpenWRT для мікропроцесорів MIPS). Комбінація "система-на-кристалі".

Arduino Robot - це перший офіційний реліз Arduino, який має колеса у своїй конструкції. Робот складається з двох плат, кожна з яких має власний мікропроцесор. Моторна плата керує роботою двигунів, в той час як плата управління зчитує дані з датчиків і приймає подальші рішення щодо руху. Кожна з двох плат є повноцінним пристроєм Arduino і може бути запрограмована за допомогою Arduino IDE.

Arduino Esplora - це мікропроцесорний пристрій, розроблений на основі Arduino Leonardo; Esplora відрізняється від попередніх плат Arduino тим, що включає в себе ряд готових до взаємодії датчиків. Esplora має вбудовані звукові та світлові індикатори (для виведення інформації), а також різноманітні датчики (для введення інформації), включаючи джойстик, повзунок, датчик температури, акселерометр, мікрофон та датчик освітленості [3].

Arduino ADK - це пристрій на базі мікроконтролера ATmega2560, який реалізує USB-хост для підключення смартфонів на базі операційної системи Android.

Плати розширення: наприклад, Arduino GSM, Arduino Ethernet, Arduino Wi-Fi, Arduino Motor, Arduino Proto.

Рис. 1.1. Плата Arduino Nano

Arduino Nano (рис.1.3) – це мікроконтролер, який є одним з найменших та найбільш компактних у лінійці Arduino. Він є ідеальним рішенням для проектів, де обмежена простір та потрібна низька вага. Arduino Nano має малі розміри (приблизно 45x18 мм), що робить його відмінним вибором для вбудованих систем та пристроїв з обмеженим простором.

Arduino Nano має компактні розміри, він все ще має значні можливості. Він базується на мікроконтролері ATMega328P, який працює на частоті 16 МГц та має 32 кілобайти флеш-пам'яті для програм та 2 кілобайти ОЗУ. Крім того, Arduino Nano має вбудований USB-інтерфейс, що дозволяє швидко та зручно програмувати його з комп'ютера.

Arduino Nano має широкий спектр вбудованих вхідних та вихідних портів, включаючи цифрові та аналогові входи/виходи, а також інтерфейси для підключення датчиків, LCD-дисплеїв, реле та інших пристроїв. Це робить його ідеальним вибором для проектів, які потребують збирання та обробки даних з різних джерел.

Arduino Nano також має велику спільноту користувачів, яка постійно розробляє нові проекти, бібліотеки та додатки для роботи з цим мікроконтролером. Це дозволяє швидко розгортати та реалізовувати різноманітні проекти з використанням Arduino Nano без значних зусиль.

Характеристики:

- Мікроконтролер: Atmel ATmega168 або ATmega328
- Робоча напруга (логічний рівень): 5В
- Напруга живлення (рекомендована): 7-12В

– Напруга живлення (гранична): 6-20В
– Цифрові входи / виходи: 14 (з яких 6 можуть використовуватися
– як ШІМ-виходи)
– Аналогові входи: 8
– Максимальний струм одного виведення: 40 мА
– Flash-пам'ять: 16 КБ (ATmega168) або 32 КБ (ATmega328) з яких 2 КБ використовуються завантажувачем
– SRAM: 1 КБ (ATmega168) або 2 КБ (ATmega328)
– EEPROM: 512 байт (ATmega168) або 1 КБ (ATmega328)
– Тактова частота: 16 МГц
– Розміри плати: 1.85 см x 4.3 см [4].

Рис. 1.2. Плата Arduino Uno

Arduino Uno (рис. 1.2) – це один з найпопулярніших та найбільш поширених мікроконтролерів у лінійці Arduino. Він володіє простим у використанні інтерфейсом та широкими можливостями, що робить його ідеальним вибором для початківців та досвідчених користувачів.

Arduino Uno базується на мікроконтролері ATMega328P від компанії Atmel. Він працює на частоті 16 МГц і має 32 кілобайти флеш-пам'яті для програм та 2 кілобайти оперативної пам'яті. Цей мікроконтролер оснащений вбудованими цифровими та аналоговими входами/виходами, що дозволяє підключати до нього різні датчики, актуатори та інші пристрої.

Arduino Uno має вбудований USB-порт, який дозволяє підключати його до комп'ютера для програмування та взаємодії з ним. Він підтримує різні способи програмування, включаючи Arduino IDE, яке є простим у використанні середовищем розробки для написання, завантаження та відлагодження програм.

Arduino Uno має широку спільноту користувачів та велику кількість різноманітних додатків, бібліотек та проектів, які розроблені для нього. Це дозволяє використовувати Arduino Uno для реалізації різноманітних проектів, включаючи автоматизацію домашніх систем, робототехніку, медичні пристрої та багато іншого.

Характеристики:

– Мікроконтролер: ATmega328
– Робоча напруга: 5 В
– Напруга живлення (рекомендована): 7-12 В
– Напруга живлення (гранична): 6-20 В
– Цифрові входи / виходи: 14 (з них 6 можуть використовуватися в якості ШІМ-виходів)
– Аналогові входи: 6
– Максимальний струм одного виводу: 40 мА
– Максимальний вихідний струм виводу: 3.3V 50 мА
– Flash-пам'ять: 32 КБ (ATmega328) з яких 0.5 КБ використовуються завантажувачем
– SRAM: 2 КБ (ATmega328)
– EEPROM: 1 КБ (ATmega328)

Тактова частота: 16 МГц Arduino Uno може живиться від USB або від зовнішнього джерела живлення - тип джерела вибирається автоматично [4].

Рис. 1.3. Плата Arduino Mega

Arduino Mega (рис. 1.3) – це великий та потужний мікроконтролер, який є одним з найбільш розширених у лінійці Arduino. Він розроблений для проектів, які вимагають більшої кількості входів/виходів та обробки даних, ніж може забезпечити Arduino Uno або Arduino Nano. Arduino Mega базується на мікроконтролері ATMega2560 від компанії Atmel. Він працює на тій же частоті, що і Arduino Uno - 16 МГц, але має більшу кількість пам'яті: 256 кілобайт флеш-пам'яті для програм та 8 кілобайт оперативної пам'яті. Це дозволяє Arduino Mega керувати більшим обсягом даних та виконувати складніші завдання [5].

Однією з основних переваг Arduino Mega є його більша кількість цифрових та аналогових входів/виходів. Він має 54 цифрових входи/виходи, з яких 14 можуть бути використані як аналогові входи, що дозволяє підключати до нього велику кількість датчиків, актуаторів та інших пристроїв.

Крім того, Arduino Mega має вбудований USB-порт для зручного програмування та взаємодії з комп'ютером. Він також підтримує різні способи програмування, включаючи Arduino IDE та інші середовища розробки.

Arduino Mega є популярним вибором для проектів, які потребують більшої кількості входів/виходів та обробки даних, таких як робототехніка, 3D-принтери, контроль обладнання та багато іншого. Велика кількість функціональності та підтримка спільноти роблять Arduino Mega потужним і універсальним інструментом для розробки різноманітних електронних проектів.

Характеристики

– Мікроконтролер: ATmega2560

– Робоча напруга: 5 В

– Вхідна напруга (рекомендована): 7-12 В

– Вхідна напруга (гранична): 6-20 В

– Цифрові Входи / Виходи: 54 (14 з яких можуть бути сконфігуровані як виходи ШІМ)

– Аналогові входи: 16

– Постійний струм через вхід / вихід: 40 мА

– Постійний струм для виводу 3.3 В: 50 мА

– Флеш-пам'ять: 256 КБ (з яких 8 КБ використовуються для завантажувача)

– ОЗУ: 8 КВ

– Незалежна пам'ять: 4 КБ

– Тактова частота: 16 МГц [6].

Arduino Mega може отримувати живлення як через підключення по USB, так і від зовнішнього джерела живлення. Джерело живлення вибирається автоматично.

Висновок

У сучасному світі системи охорони зіштовхуються зі складними викликами та проблемами, такими як швидка зміна технологій, розвиток кіберзлочинності та зростання обсягу даних. Визначення проблеми у сучасних системах охорони є першим кроком до створення ефективних та надійних рішень. Цей розділ включає в себе аналіз та опис основних проблем, з якими стикаються сучасні системи охорони, таких як вразливість до кібератак, нестабільність систем та складність управління.

Контролери грають важливу роль у побудові архітектури систем охорони. Вони використовуються для збору, обробки та аналізу даних з датчиків, камер відеоспостереження, систем відстеження та інших джерел. Крім того, контролери забезпечують зв'язок між різними компонентами системи та керування ними. Роль контролерів у побудові архітектури систем полягає в створенні ефективних, надійних та безпечних рішень для забезпечення безпеки та захисту.

Розглянуто функції та можливості контролерів Arduino та визначено їхню важливу роль у побудові архітектури систем охорони. Базуючись на їхній простоті використання, доступності та широкому функціоналі, контролери Arduino стають ефективним інструментом для забезпечення безпеки та захисту. Вони дозволяють збирати та аналізувати дані з різних джерел, керувати різними пристроями та виконувати автоматизовані завдання. Таким чином, контролери Arduino є важливою складовою сучасних систем охорони, які сприяють покращенню безпеки та захисту в різних сферах життя.

2 АНАЛІТИЧНИЙ ОГЛЯД ІСНУЮЧОЇ СИСТЕМ НА БАЗІ ARDUINO

2.1 Технології зв’язку Wi-Fi, Bluetooth, ZigBee, Z-Wave

Технології бездротового зв'язку, такі як Wi-Fi, Bluetooth, ZigBee та Z-Wave, стали неодмінною частиною сучасного світу, де все більше пристроїв стають "розумними" і можуть взаємодіяти між собою та з користувачами безпосередньо через бездротові мережі. Кожна з цих технологій має свої унікальні характеристики та застосування, що робить їх важливими компонентами для побудови систем "розумного будинку", мереж Інтернету речей (IoT), медичних технологій та багатьох інших сфер [7]. Давайте розглянемо кожну з цих технологій більш детально. Результати наведені в таблиці 2.1.

Для проекту розумного будинку на базі Arduino можна використовувати модулі Wi-Fi, які дозволяють підключати Arduino до мережі Wi-Fi для забезпечення бездротового зв'язку. Один з найпоширеніших модулів для цього - ESP8266 або його покращена версія ESP32, які мають вбудований Wi-Fi.

Для використання Wi-Fi з Arduino, потрібно:

1. Підключити модуль Wi-Fi до Arduino, підключення може бути здійснено через шину SPI або UART.
2. 2Використати бібліотеки, для роботи з Wi-Fi на Arduino можна використовувати різні бібліотеки, такі як WiFi.h для ESP8266 або WiFi.h та WiFiClient.h для ESP32.
3. Налаштувати з'єднання в коді Arduino можна налаштувати SSID та пароль для підключення до мережі Wi-Fi.
4. Взаємодія з іншими пристроями, після підключення до мережі Wi-Fi, Arduino може взаємодіяти з іншими пристроями через мережу, відправляти та отримувати дані, керувати пристроями тощо [8].

Bluetooth – це бездротовий протокол зв'язку, який дозволяє пристроям обмінюватися даними на короткій відстані. Для проекту розумного будинку на базі

Arduino можна використовувати модулі Bluetooth, такі як HC-05 або HC-06, для забезпечення бездротового зв'язку з іншими пристроями, такими як смартфони або планшети.

Основні характеристики технології Bluetooth для проекту розумного будинку на базі Arduino включають:

Підключення до Arduino, модулі Bluetooth підключаються до Arduino через інтерфейс UART, що дозволяє легко взаємодіяти з Arduino через простий протокол комунікації.

Взаємодія з іншими пристроями, після підключення до Arduino, можна взаємодіяти з іншими пристроями, що підтримують Bluetooth, наприклад, відправляти та отримувати дані, керувати пристроями тощо.

Інтерфейс з користувачем, для взаємодії з Arduino через Bluetooth можна використовувати спеціальні мобільні додатки або створювати власні застосунки, які можуть керувати пристроями у системі розумного будинку.

Зона покриття, Bluetooth має досить обмежену зону покриття (зазвичай до 10 метрів), що робить його ідеальним для використання в системах розумного будинку, де пристрої можуть бути розташовані поруч.

Технологія ZigBee є бездротовою мережевою технологією, яка спеціально розроблена для використання в системах "розумного будинку" та мережах Інтернету речей (IoT). Для проекту розумного будинку на базі Arduino можна використовувати модулі ZigBee, такі як XBee, для створення бездротової мережі для зв'язку різних пристроїв [9].

Основні характеристики технології ZigBee для проекту розумного будинку на базі Arduino включають:

1. ZigBee споживає дуже мало енергії, що робить його ідеальним для використання в батарейних пристроях, таких як датчики та вимикачі.
2. ZigBee підтримує мережеву топологію "зірка", "дерево" та "сітка", що дозволяє створювати складні мережі з великою кількістю пристроїв.

3. Швидкість передачі даних в ZigBee досить низька порівняно з Wi-Fi або Bluetooth, це достатньо для більшості застосувань у системах розумного будинку.

4. ZigBee має високу стійкість до перешкод та може працювати в умовах з великою кількістю перешкод.

5. ZigBee має вбудовані засоби захисту даних та конфіденційності, що робить його безпечним для використання у системах, де важлива безпека даних [10].

Таблиця 2.1

Порівняння технологій «розумного будинку»

Технологія	Де використовується	Наявність єдиного стандарту, щоб управляти всією технікою з однієї програми	Вартість
Wi-Fi	IP-камерах, телевізорах, аудіо/медіа-плеєрах і іншій техніці для передачі відеосигналу	Немає	Середня
Bluetooth	бездротові навушники, колонки і різні датчики на батарейках	Немає	Середня
ZigBee	для застосування в мережах з датчиків, таких як лічильники електроенергії, води, газу, датчики температури	Немає	Мала
Z-Wave	спеціально для домашньої автоматизації	Повна сумісність	Мала

2.2 Аналіз існуючих рішень системи "розумний будинок"

Розумний будинок – це будинок, обладнаний різноманітними електронічними пристроями, які автоматизують та забезпечують зручність та ефективність життя його мешканців. Ці технології можуть включати в себе системи автоматизації освітлення, опалення, кондиціонування повітря, безпеки, керування електроприладами, відеоспостереження, аудіо- та відеосистеми розваг та багато іншого [11].

Розумний будинок можна зібрати самому, розпочати зі схеми, використовуючи різні хаби, обрати плагін та налаштувати його під себе, керувати за допомогою додатків розроблених самостійно. Або обрати варіант готового стартового набору і придбати валідні пристрої, які співпрацюють з хабом, скачати готовий додаток бренду та керувати власним житлом.

Достатньо придбати базовий набір засобів контролю безпеки, в тому числі на випадок пожежі, протікання води або несанкціонованого проникнення.

Сьогодні існує безліч технологій для інтеграції та управління системами розумного будинку. Розглянемо деякі поширені готові рішення та проаналізуємо їхні переваги та недоліки:

Ajax StarterKit – це комплект (рис. 2.1) обладнання для створення системи безпеки "розумний будинок" від компанії Ajax Systems. StarterKit містить основні компоненти для початку: центральну станцію, датчики руху, відкривання дверей/вікон, брелок для деактивації/активації системи та інші [12].

Ця система працює на бездротовому протоколі зв'язку Jeweller, що забезпечує надійну комунікацію між всіма пристроями в системі на відстані до 2000 метрів на відкритій місцевості або через стіни. Ajax StarterKit дозволяє вам створити базову систему безпеки для вашого будинку або офісу, яка може бути легко розширена за потреби.

Рис. 2.1 Система «розумного будинку» Ajax StarterKit

Переваги набору Ajax StarterKit:

1. Простота встановлення, StarterKit поставляється з усім необхідним обладнанням і інструкціями для швидкого налаштування системи безпеки в будинку.

2. Надійність зв'язку, використання бездротового протоколу Jeweller забезпечує стійку та надійну комунікацію між всіма пристроями системи на великій відстані.

3. Легкість управління, систему можна керувати за допомогою спеціального додатку на смартфоні або планшеті, що робить її управління зручним та доступним з будь-якої точки світу.

4. Розширені можливості, StarterKit можна легко розширити, додавши до нього інші пристрої Ajax Systems для покращення функціональності системи.

5. Висока безпека, система має високий рівень захисту від взлому та перешкоджень, що забезпечує безпеку вашого будинку чи офісу [13].

Недоліки набору Ajax StarterKit:

1. Висока вартість, якщо порівняннювати з іншими системами безпеки, Ajax StarterKit може бути відносно дорогим варіантом.

2. Обмежені можливості стандартного набору, при купівлі стандартного StarterKit ви отримуєте обмежений набір пристроїв, що може бути недостатнім для певних потреб.

3. Залежність від інтернет-з'єднання, для деяких функцій, таких як отримання сповіщень на смартфон, потрібне постійне підключення до Інтернету.

4. Сумісність з іншими системами не завжди можлива інтеграція з іншими системами "розумного будинку", які використовують інші протоколи зв'язку.

Xiaomi Mijia – це бренд смарт-пристроїв для дому (рис. 2.2), що належить компанії Xiaomi, яка відома своїми інноваційними продуктами в галузі електроніки та технологій. Під брендом Мijia компанія випускає широкий асортимент смарт-пристроїв, таких як розумні датчики, освітлення, камери спостереження, пристрої для контролю за якістю повітря та води, електроніка для кухні та багато іншого [14].

Продукція Xiaomi Mijia зазвичай працює на платформі Mi Home, що дозволяє управляти різними пристроями за допомогою одного мобільного додатку на смартфоні. Продукти Мijia відомі своєю високою якістю, функціональністю та доступною ціною, що робить їх популярними серед користувачів, які бажають зробити свій дім більш "розумним" та зручним у використанні.

Рис. 2.2 Система «розумного будинку» Xiaomi Mijia

Переваги:

1. Доступна ціна, продукція Xiaomi Mijia відома своєю доступною ціною, що робить її привабливою для багатьох користувачів.

2. Широкий асортимент, бренд пропонує широкий вибір смарт-пристроїв, що дозволяє користувачам створювати повноцінні системи "розумного будинку".

3. Висока якість виготовлення, продукція Xiaomi Mijia відома своєю якістю виготовлення та надійністю.

4. Легкість встановлення та налаштування, багато пристроїв Mijia можна легко встановити та налаштувати за допомогою мобільного додатку Mi Home.

5. Інтеграція з іншими пристроями, продукція Xiaomi Mijia зазвичай підтримується іншими популярними платформами "розумного будинку", що дозволяє їх інтегрувати з іншими смарт-пристроями [14].

Недоліки:

Обмежені функціональність та можливості, якщо порівнянню вати з деякими іншими брендами, продукція Xiaomi Mijia може мати обмежені функціональність та можливості.

Залежність від інтернет-з'єднання більшість пристроїв Mijia вимагають постійного підключення до Інтернету для коректної роботи та взаємодії з іншими пристроями.

Сумісність з іншими пристроями, іноді можуть виникати проблеми зі сумісністю пристроїв Mijia з іншими платформами "розумного будинку".

Google – це американська технологічна компанія, відома своїми інноваційними продуктами та послугами у галузі IT та Інтернету. Одним з напрямків їхньої діяльності є розробка систем "розумного будинку", які базуються на їхній платформі Google Home та інших продуктах.

Системи "розумного будинку" від Google (рис. 2.3) дозволяють користувачам керувати різними пристроями та системами у будинку, такими як освітлення, термостати, камери безпеки, аудіо- та відеосистеми, за допомогою мобільного додатка Google Home або голосових помічників, таких як Google Assistant [14].

Рис. 2.3 Система «розумного будинку» Google Home

Основні переваги систем "розумного будинку" від Google включають:

Інтеграція з екосистемою Google, система працює в узгоджені з іншими продуктами Google, такими як Android, Chromecast, Google Calendar тощо.

Зручне управління, користувач може керувати системою за допомогою мобільного додатка або голосових команд, що робить керування простим та зручним.

Розширені можливості, система може бути легко розширена за допомогою додаткових пристроїв та інтеграції з іншими платформами "розумного будинку".

Висока якість та надійність, продукція Google відома своєю високою якістю та надійністю.

Недоліки можуть включати обмежену сумісність з деякими пристроями та системами "розумного будинку", а також можливість залежності від стабільного Інтернет-з'єднання для коректної роботи системи.

Amazon – це система "розумного будинку" (рис. 2.4)від компанії Amazon, яка базується на їхній платформі Amazon Alexa та інших продуктах. Система дозволяє користувачам керувати різними пристроями та системами у будинку за допомогою голосових команд або мобільного додатка Alexa.

Рис. 2.4 Система «розумного будинку» Amazon Alexa

Основні можливості Amazon розумного будинку включають:

1. Голосове керування, користувачі можуть використовувати голосові команди для управління освітленням, термостатами, аудіо- та відеосистемами та іншими побутовими пристроями.

2. Інтеграція з іншими пристроями, система сумісна з багатьма популярними платформами "розумного будинку", такими як Philips Hue, Samsung SmartThings, Nest тощо.

3. Смарт-розклади та автоматизація, користувачі можуть налаштовувати розклади роботи пристроїв та створювати автоматичні сценарії для певних подій або часів доби.

4. Мобільний додаток, крім голосового керування, користувачі можуть управляти системою через мобільний додаток Alexa на смартфоні або планшеті.

5. Широкий вибір пристроїв, amazon пропонує власні пристрої, такі як Echo-динаміки з вбудованим асистентом Alexa, а також співпрацює з іншими виробниками для розширення вибору сумісних пристроїв [14].

Amazon розумний будинок надає користувачам зручний спосіб автоматизувати та керувати побутовими пристроями та системами, роблячи життя вдома більш зручним та ефективним.

2.3 Найпоширеніші вразливості «розумних будинків» та атаки на розумні домашні пристрої

Дослідницький проєкт 2021 року показав, що типовий розумний будинок вразливий до витоку даних. Повідомлялося про атаки, коли хакери націлювалися на "розумні" будинки, дистанційно керуючи "розумним" освітленням і "розумними" телевізорами, відмикаючи двері з підтримкою Інтернету речей і дистанційно керуючи "розумними" камерами для потокового відео. Два найпоширеніші типи атак - це вразливі локальні мережі та вразливі пристрої Інтернету речей [15].

Вразливість локальної мережі "розумного будинку" може бути викликана різними факторами, що можуть загрожувати безпеці системи та даних користувачів. Однією з основних проблем є недостатня захищеність мережі та пристроїв від несанкціонованого доступу. Низький рівень захисту може дозволити зловмисникам перехоплювати дані, керувати підключеними пристроями або навіть використовувати їх для вторгнень у систему.

Іншою проблемою є використання застарілих програмних та апаратних засобів, які можуть мати відомі вразливості. Недостатнє оновлення програмного забезпечення або відсутність підтримки з боку виробників може створювати ризики для безпеки мережі.

Додатково, низький рівень свідомості користувачів щодо безпеки та недостатня увага до правил використання мережі можуть стати факторами, що сприяють вразливості мережі "розумного будинку". Наприклад, слабкі паролі, відсутність шифрування чи відкритий доступ до мережі можуть легко стати точкою входу для зловмисників.

Wi-Fi може бути вразливим через стандартні або слабкі SSID та паролі, а також слабкі протоколи шифрування. Стандартні облікові дані дозволяють зловмисникам отримати доступ до роутера без особливих труднощів. Надійні

паролі Wi-Fi дозволяють хакерам знаходити більш складні шлюзи для проникнення в мережу.

Підслуховування та шифрування - найпоширеніші методи злому. Під час підслуховування хакери перехоплюють пакети, що проходять між пристроєм і роутером, і відправляють їх на свій пристрій, використовуючи грубу силу. Зазвичай це займає лише кілька хвилин. Більшість Wi-Fi роутерів використовують протоколи безпеки: WPA (Wi-Fi Protected Access), WPA2 і WEP (Wired Equivalent Privacy).

WEP - це потоковий шифр RC4; одним з недоліків WEP є малий розмір вектора ініціалізації (24 біт IV), який, таким чином, використовується повторно. Це повторення створює вразливості в безпеці.

Більш безпечними варіантами є WPA і WPA2. Однак дослідники виявили серйозну вразливість у WPA під назвою KRACK, що розшифровується як Key Reload Attack (атака на перезавантаження ключа). Атака "зловмисника посередині" може використати її для викрадення конфіденційних даних, що передаються через WPA-зашифроване Wi-Fi з'єднання. Зловмисники можуть підслуховувати трафік і отримувати паролі, банківську інформацію та дані кредитних карток [15].

Вразливі пристрої Інтернету речей Дослідники протестували загалом 16 поширених пристроїв розумного дому від різних брендів і виявили 54 вразливості, які роблять користувачів вразливими для хакерів. Атаки варіювалися від відключення систем безпеки до крадіжки персональних даних, і близько 80% пристроїв Інтернету речей вразливі до різних атак.

Пристрої "розумного дому" вразливі, оскільки вони кастомізовані, а постачальники IoT не можуть надати необхідні індивідуальні рішення для забезпечення безпеки. Крім того, пристрої розумного будинку часто працюють на невеликих операційних системах, таких як INTEGRITY, Contiki, FreeRTOS і VxWorks, а їхні рішення для забезпечення безпеки не такі надійні, як системи на базі Windows або Linux.

Більшість існуючого обладнання після встановлення не можна модернізувати, щоб воно відповідало новим функціям кібербезпеки. Залежно від

пристрою та протоколу зв'язку, пристрої розумного дому можуть бути атаковані різними способами.

Таблиця 2.2

Основні види загроз

Види загроз	Опис
Конфіденційність	Це призводить до ненавмисного розголошення конфіденційної інформації. Наприклад, якщо конфіденційність не захищена в системі домашнього моніторингу, персональні медичні дані можуть бути ненавмисно розголошені. Навіть така, на перший погляд, невинна інформація, як температура в будинку або робота системи кондиціонування, може бути використана як передумова до пограбування, щоб визначити, чи є в будинку хтось, хто перебуває в ньому. Втрата конфіденційності таких речей, як ключі та паролі, створює ризик несанкціонованого доступу до систем.
Автентифікація	Ці загрози можуть призвести до підробки інформації та контролю. Наприклад, неавторизоване сповіщення про стан системи може змусити оператора будівлі повірити, що сталася надзвичайна ситуація, і спробувати екстрено втекти, відчинивши двері або вікно, хоча насправді це може призвести до незаконного проникнення.
Доступ	Несанкціонований доступ до контролера системи, особливо на рівні адміністратора, може залишити всю систему незахищеною. Це може бути наслідком неправильного управління паролем або ключами, або несанкціонованого

Продовження таблиці 2.2

Основні види загроз

	підключення пристроїв до мережі. Залишення несанкціонованих мережевих підключень без нагляду може також призвести до крадіжки пропускної здатності мережі або відмови в обслуговуванні законних користувачів. Багато пристроїв розумного будинку працюють у бездротових мережах з низьким рівнем заряду батареї або циклами роботи, тому переповнення мережі запитами може призвести до атак виснаження живлення, що є формою відмови в обслуговуванні.

Поширені методи атак включають в себе:

Витік даних та крадіжка особистих даних. Незахищені пристрої Інтернету речей генерують дані, надаючи кіберзлочинцям широкі можливості для атак на персональні дані. Це може призвести до крадіжки особистих даних та несанкціонованих транзакцій.

Крадіжка пристроїв і прослуховування. Смарт-пристрої можуть бути скомпрометовані, а контроль над ними переданий зловмисникам. Зловмисники можуть отримати контроль над пристроєм, порушити зв'язок між пристроями і навіть отримати контроль над іншими пристроями або мережею в цілому.

Розподілена відмова в обслуговуванні (DDoS) - це тимчасове або невизначене переривання обслуговування, що робить пристрій або мережевий ресурс недоступним для цільових користувачів.

Wipe - ця атака може пошкодити пристрій до такої міри, що його доведеться замінити.

Домашні мережі можуть бути незахищеними, і зловмисники можуть отримати доступ до всіх даних, що зберігаються в цих мережах. Наприклад, злочинці можуть відстежувати шаблони використання різних пристроїв, коли ви перебуваєте поза домом. Якщо домашньою мережею керує основний обліковий

запис в Інтернеті, то скомпрометованими можуть бути не лише дані з пристроїв Інтернету речей. Особиста інформація, така як електронна пошта, акаунти в соціальних мережах і банківські рахунки, також може бути скомпрометована, якщо її зламати [16].

Оскільки багато користувачів керують своїми підключеними до Інтернету речей будинками за допомогою смартфонів, ваш смартфон стає безцінною базою даних для тих, хто хоче порушити ваше життя. Тому ви піддаєтеся високому ризику, якщо ваш смартфон буде зламаний, викрадений або якщо комусь вдасться підслухати ваші з'єднання.

Безпека має вирішальне значення для успіху розумного будинку. Почуватися в безпеці у власному будинку - це основна потреба людини. Наші будинки наповнені пристроями Інтернету речей, багато з яких вразливі до цифрових загроз. Не секрет, що комп'ютери та смартфони становлять загрозу кібербезпеці, але сьогодні навіть розумні холодильники та радіоняні підключені до інтернету, що робить їх вразливими до атак і хакерів [16].

Близько 80% пристроїв Інтернету речей вразливі до різних атак. Очевидно, що взаємозв'язок раніше "автономних" розумних пристроїв, таких як освітлення, побутова техніка та замки, створює низку ризиків для кібербезпеки. Навіть підключені до Інтернету радіоняні вразливі до цифрових зловмисників, і багато наляканих батьків згодом дізнаються, що хакери спілкувалися з їхніми дітьми через заражені пристрої.

Як наслідок, доступність мережевих систем є основною вразливістю безпеки. Сучасні системи "розумного будинку" підключені до інтернету і тому можуть бути атаковані віддалено, або шляхом прямого доступу до веб-інтерфейсу управління, або шляхом завантаження шкідливого програмного забезпечення на пристрій.

Фізичний доступ до систем також є проблемою. Навіть якщо будинок повністю замкнений, матеріальний доступ до мереж і бездротових технологій поза домом можливий.

Невеликий розмір контролерів пристроїв (8-розрядні мікроконтролери) і обмеженість пам'яті та обчислювальних ресурсів обмежують реалізацію складних алгоритмів безпеки.

Багато постачальників пропонують пристрої з хорошим програмним забезпеченням і можливістю оновлення мережевих стандартів. Ці пристрої можуть мати мало або взагалі не мати документації про встановлену прошивку, операційну систему та механізми безпеки.

Виправлення прошивки також є проблемою. Лише деякі пристрої розумного будинку регулярно оновлюють своє програмне забезпечення для усунення вразливостей безпеки. Дехто підозрює, що наразі немає стимулів для оновлення програмного забезпечення або запобігання вразливостям у пристроях, які коштують сотні тисяч доларів.

Іншим слабким місцем є повільне впровадження стандартів. Хоча деякі спеціалізовані системи, такі як підсистеми моніторингу здоров'я, мають добре продуману безпеку, що відповідає стандартам, більшість існуючих пристроїв для розумного дому мають слабкий захист або взагалі його не мають. Але найбільшим недоліком є брак експертів з безпеки, які можуть керувати складними мережами розумного будинку. Небагато домогосподарств можуть дозволити собі найняти професіонала на повний робочий день для управління домашніми мережами. Замість цього домовласники повинні мати можливість самостійно керувати своїми системами в простий, безпечний і надійний спосіб. Налаштування розумного будинку з низкою заходів - це один із способів захистити мережу від небажаних зловмисників [16].

Висновок

Розглянуто технології бездротового зв'язку, які використовуються в системах "розумного будинку". Wi-Fi, Bluetooth, ZigBee та Z-Wave були проаналізовані з точки зору їхніх особливостей, переваг та недоліків у контексті використання в розумних пристроях та системах управління. Висвітлено їхню ефективність,

споживання енергії, стійкість до перешкод та інші характеристики, які важливі для вибору оптимального рішення для конкретного застосування.

Проведено аналіз існуючих рішень системи "розумний будинок". Розглянуто різноманітні пропозиції від виробників у цій галузі, включаючи стандартні рішення та спеціалізовані пристрої. Проаналізовано їхні можливості, функціональність, ефективність та зручність в управлінні. Також висвітлено переваги та недоліки різних підходів до створення систем "розумного будинку".

Проаналізовані найпоширеніші вразливості систем "розумний будинок" та типові атаки, які можуть бути спрямовані на розумні домашні пристрої. Розглянуті можливі загрози безпеці, які можуть виникнути внаслідок використання таких систем, а також вказані шляхи захисту від них. Результати аналізу допоможуть розуміти потенційні ризики та вибирати ефективні заходи для забезпечення безпеки в системах "розумного будинку".

3 РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБКИ СИСТЕМИ ОХОРОНИ НА БАЗІ ARDUINO

3.1. Вибір апаратного та програмного забезпечення для реалізації системи охорони

Обираючи плату Arduino UNO як головний модуль для управління проєктованою системою, було враховано кілька ключових факторів, які сприяли цьому вибору. Перш за все, Arduino UNO відома своєю низькою вартістю порівняно з іншими мікроконтролерами та розвиненими платформами, що робить її доступною для широкого кола користувачів, включаючи студентів, ентузіастів і професіоналів.

Однак, крім вартості, Arduino UNO також славиться своєю простотою в використанні та широким спектром додаткових модулів і програмних бібліотек, які розширюють її функціональні можливості. Це робить Arduino UNO відмінним вибором для проєктів з різноманітними потребами у взаємодії з сенсорами, приводами, комунікаційними модулями та іншими периферійними пристроями.

Зовнішній вигляд плати Arduino UNO є компактним і функціональним. Вона має ряд роз'ємів для підключення зовнішніх пристроїв, таких як сенсори, мотори, дисплеї та інші модулі. Крім того, на платі є мікроконтролер, що відповідає за обробку програмного коду, та інші компоненти, необхідні для правильної роботи пристрою.

Ключовими перевагами Arduino UNO є його простота в програмуванні, велика спільнота користувачів та розвитає програмна екосистема, що дозволяє швидко розробляти прототипи та впроваджувати різноманітні проекти. В цілому, вибір Arduino UNO як головного модуля для управління системою є розумним рішенням, що поєднує надійність, доступність і функціональність.

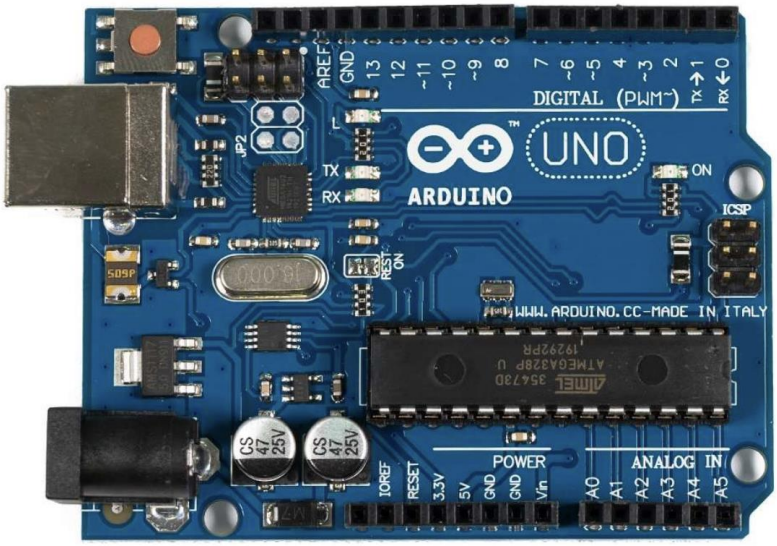


Рис. 3.1 – Основний модуль Arduino UNO

Плата Arduino Uno надійно взаємодіє з зовнішніми пристроями за допомогою шести вхідних аналогових і чотирнадцятьох цифрових виводів загального призначення. З цих виводів шість можуть використовуватися для генерації широтно-імпульсної модуляції (ШІМ), що є важливим для керування різноманітними пристроями, які підтримують цей тип сигналу. Крім того, плата має роз'єми USB і ISCP для програмування мікроконтролера, що дозволяє швидко та зручно завантажувати програмне забезпечення на пристрій [17].

Щодо живлення, плата може живитися кількома способами: через USB-роз'єм або через роз'єм для підключення зовнішнього джерела живлення. У вашому випадку, коли система сигналізації повинна працювати автономно, плата буде живитися від зовнішньої акумуляторної батареї, забезпечуючи незалежність від джерела електромережі.

Мікроконтролер ATmega328P, який використовується в платі Arduino Uno, є восьмибітним і має ряд виводів з різними функціями, такими як вхід, вихід, аналоговий ввід/вивід, інтерфейси зв'язку тощо. Ці виводи можна програмно налаштовувати для виконання потрібних завдань, що робить Arduino Uno дуже гнучкою платформою для розробки різноманітних проектів.

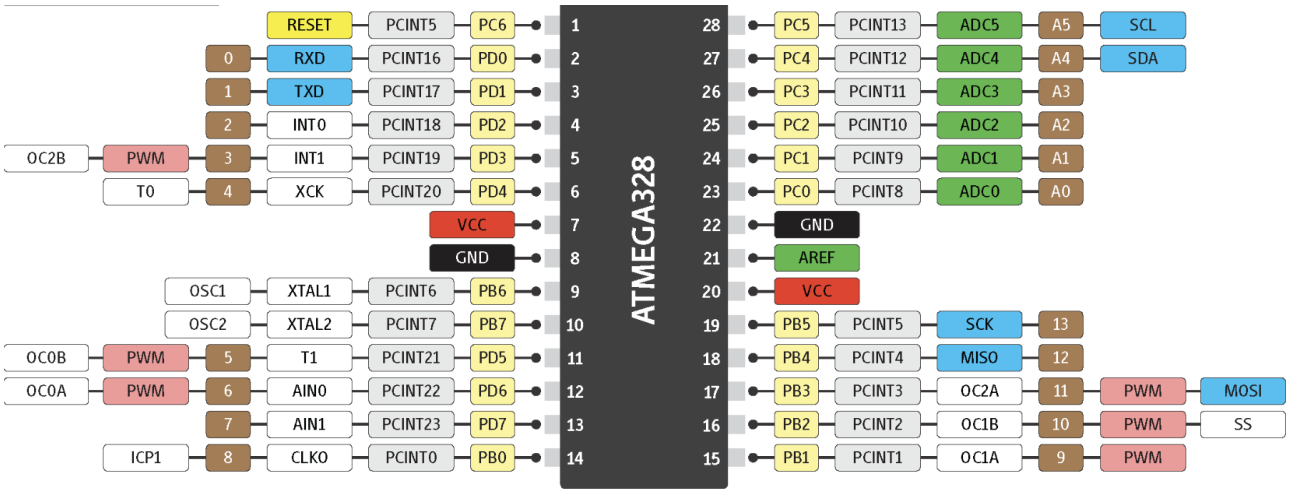


Рис. 3.2 – Позначення виводів контролера ATmega328P

ATMEGA328P-це мікроконтролер з розширеним віртуальним RISC Архітектура. Він характеризується високою ефективністю і високою продуктивністю. Щільність коду. Цей Мікроконтролер має 32 флеш-пам'яті Кілобайт, який використовується для зберігання п'ятисот байт Файл завантажувача. Крім того, ATMEGA328P містить 1 кілобайт у Жовтневому центрі EEPROM і 2 КБ SRAM. Мікроконтролер працює на тактовій частоті Його виробництво забезпечується кварцовими резонаторами. Він буде поміщений на дошку [17].

Мікроконтролер ATmega328P містить десятибітний АЦП, Важливим фактором при виборі цього була його присутність Спеціальна модель мікроконтролера. серед інтерфейсів, що надаються цим мікроконтро декомунізатором, є, Можна виділити I2C, SPI і UART.

Модуль датчика руху

Піроелектричний інфрачервоний модуль датчика руху PIR, заснований на сенсорному елементі HC-SR501, був обраний для визначення факту небажаної присутності прогнозованої системи безпеки. Цей датчик може виявляти рухи оточуючих людей в межах видимості. Принцип роботи датчика заснований на вимірюванні кількості інфрачервоних променів, що виділяються живими істотами.

Крім того, датчик може реагувати на інші об'єкти Він випромінює тепло. На малюнку 3.3 показаний зовнішній вигляд датчика руху [17].

Рис. 3.3 – Зовнішній вигляд модуля давача руху PIR HC-SR501

Модуль датчика оснащений лінзою Френеля, яка фокусує інфрачервоне випромінювання на піроелектричному чутливому елементі. Крім випромінювання від самого об'єкта, датчик вважається пасивним, оскільки він не вимагає додаткової енергії для виявлення руху. Чутливий елемент складається з 2 компонентів. Модуль управління мікрочіпом вловлює зміни сигналів від обох компонентів і виявляє рухомі об'єкти, що випромінюють інфрачервоні сигнали, беручи до уваги характер змін. Основні технічні параметри модуля датчика руху наведені в таблиці 3.1.

Таблиця 3.1

Технічні параметри давача руху

Параметр	Значення
Струм	50 мкА
Напруга	4,5-20 В
Вихідна напруга	3,3 В

Рекомендовані модулі мають невеликі розміри, прості в експлуатації, надійні і мають низьке енергоспоживання. Тому його зручно використовувати на пристроях, що працюють на автономних ресурсах. Чутливість модуля зменшується

зі збільшенням відстані. Важливо уникати джерел тепла і яскравого світла, які можуть потрапляти на поверхню лінзи модуля.

Датчик відкривання дверей.

Одним з найважливіших датчиків, розроблених Sos, є датчик відкривання дверей. Це герконовий перемикач, яким можна керувати за допомогою магнітного поля. Зовнішній вигляд датчика відкривання дверей МС-38 показаний на малюнку 3.4.

Рис. 3.4 – Зовнішній вигляд давача відкриття дверей МС-38

Номінальна потужність датчика становить 10 Вт, а максимальне споживання струму - 500 мА. Герконовий вимикач МС-38 спрацьовує на відстані 18 мм з похибкою 6 мм.особливістю цього датчика є те, що він зазвичай вимикається, коли перемикач закривається магнітом, тобто коли електричний ланцюг замикається.

При зачинених дверях, якщо магніт перебуває в безпосередній близькості від давача, його контакти є замкненими і розмикаються у випадку відкриття дверей.

Модуль давача розбиття скла

В якості давача розбиття скла для проєктованої системи було обрано звуковий модуль KY-037. Його можна налаштувати так, щоб він реагував на певний тип звукового сигналу. Зовнішній вигляд давача KY-037 зображений на рис. 3.5.

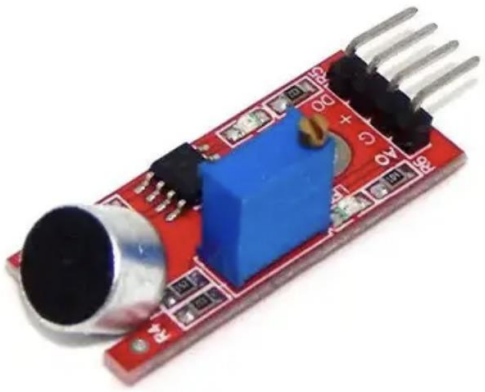


Рис. 3.5 – Зовнішній вигляд модуля KY-037

Принцип роботи датчика KY-037 полягає в тому, що вібрація мембрани мікрофона відбувається під дією звукових хвиль. В результаті конденсатор змінює свою ємність, викликаючи зміну рівня напруги на виході аудіодатчика, відповідного звуковому сигналу. Модуль KY-037 призначений для прийому гучних звукових сигналів, таких як Тріск скла. Він не реагує на тихі звуки, такі як людська мова [18].

GSM модуль SIM800L

Для відправки користувачеві повідомлення про надзвичайну ситуацію на об'єкті вибирається модуль GSM SIM8 0 0l, зовнішній вигляд якого показаний на рис. 3.6. Функціональність цього модуля практично повністю відповідає функціональності телефону.

З SIM800L ви можете приймати або здійснювати дзвінки, відправляти SMS-повідомлення, використовувати протокол TCP / IP, протокол GPRT і т.д. Ви можете підключитися до Інтернету, використовуючи його. Крім того, модуль підтримує 4-смугові мережі GSM. жовтень. Модуль заснований на використанні однойменного чіпа simcom SIM800L.

Рис. 3.6 – Зовнішній вигляд GSM модуля SIM800L

Модуль SIM800L має вбудовану антену, але для поліпшення якості сигналу можна підключити додаткову зовнішню антену. Жовтень 2000 р модуль SIM800L має вбудовану антену, але можна підключити додаткову зовнішню антену. На нижній стороні плати модуля розташований роз'єм для установки SIM-карти.

Підключення мікроконтролера до послідовного порту специфічно-цифровий вихід мікроконтролера Atmega328 має 5-вольтову логіку, а модуль SIM800L - 3,3 В, тому неможливо підключити лінію RXD безпосередньо до модуля GSM [18].

У зв'язку з цим рекомендується використовувати схему дільника напруги для зниження його рівня у вигляді двох резисторів номіналом 5 ком і 10 Ком 2. Перед запуском GSM-модуля необхідно вставити SIM-карту у відповідний роз'єм на карті і підключити антену. Висновок на висновок модуля SIM800L GSM показаний на малюнку 3.7.

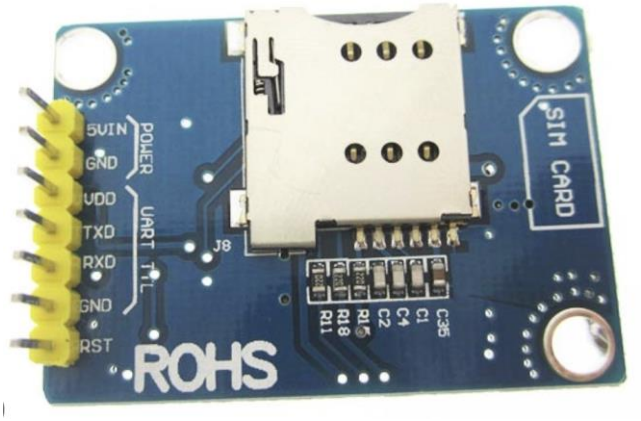


Рис. 3.7 – Призначення виводів GSM модуля SIM800L

Максимальне споживання струму модулем може становити 2 А, тому живлення від мікроконтролера неможливо. Він живиться від напруги, і його рівень

може варіюватися від 3,3 В до 4,4 В, що дозволяє використовувати для цих цілей звичайні літієві вторинні батареї. дека.

Модуль контролю заряду-розряду АКБ

В технічному завданні вказано, що охоронна сигналізація повинна бути автономною і отримувати живлення від акумуляторної батареї. Тому, в проєктованій системі необхідно передбачити пристрій, який забезпечуватиме процес зарядження акумулятора. Для цих цілей було обрано модуль на базі мікросхеми TP4056 (рис. 3.8). Процес зарядження акумуляторної батареї дуже схожий на зарядку смартфона. Завершення процесу зарядження супроводжується світінням яскравих світлодіодів [18].

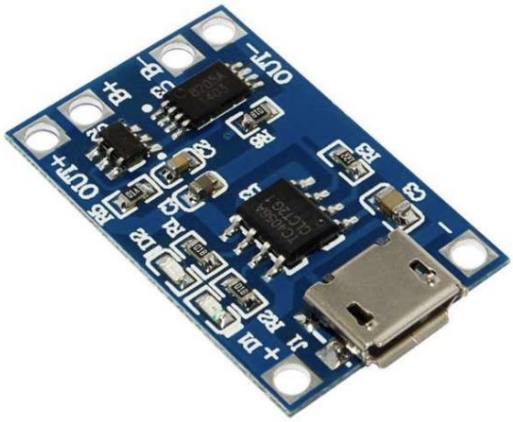


Рис. 3.8 – Зовнішній вигляд модуля TP4056

Напруга живлення може подаватися на модуль за допомогою роз'єму microUSB або за допомогою відповідних контактів, які можуть припаяти провідник.

Модуль п’єзодинаміка

Ми вирішили використовувати модуль Piezo Dynamics для звукових сповіщень, коли датчик активується в розробленій системі. Piezo Dynamic перетворює команди, отримані від мікроконтролера, в аудіосигнали. На рисунку 3.9 показано зовнішній вигляд модуля п'єзодинаміки.

Рис. 3.9 – Зовнішній вигляд модуля п’єзодинаміка

П'єзодинаміка - це металева пластина на поверхні з керамічним покриттям, яка може проводити струм. Принцип роботи п'єзодинаміки заснований на п'єзоелектричному ефекті, який полягає в деформації при протіканні струму. В результаті за рахунок впливу на металеву пластину генерується звуковий сигнал необхідної частоти. Для цього в його п'єзодинамічної конструкції передбачений частотний генератор для звуку. У таблиці 3.2 перераховані основні параметри модуля п'єзодинаміки.

Таблиця 3.2

Технічні параметри модуля п’єзодинаміка

Параметр	Значення
Частота звуку	2300 Гц
Струм	до 30 мА
Напруга	5 В

Дисплей

РК-дисплей системи безпеки використовується для відображення стану датчика, взаємодії з користувачем при введенні пароля під час установки і зняття з охорони приміщення. На рисунку 3.10 показаний зовнішній вигляд дисплея.

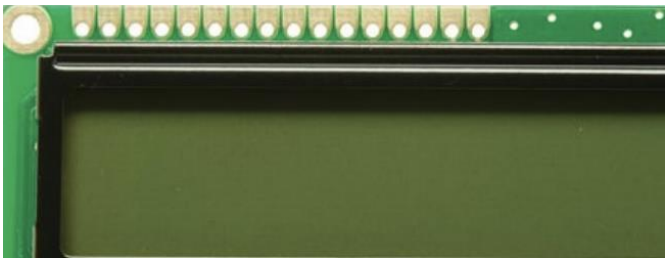


Рис. 3.10 – Зовнішній вигляд дисплея

За роботу цього дисплея відповідає контролер HD44780, який отримує дані з платформи Arduino через модуль I2C.

Модуль I2C

З метою економії виводів мікроконтролера та спрощення процесу передачі інформації на LCD дисплей застосовується модуль I2C на базі мікросхеми контролера вводу/виводу PCF8574T. На рис. 3.11 зображено зовнішній вигляд I2C модуля.

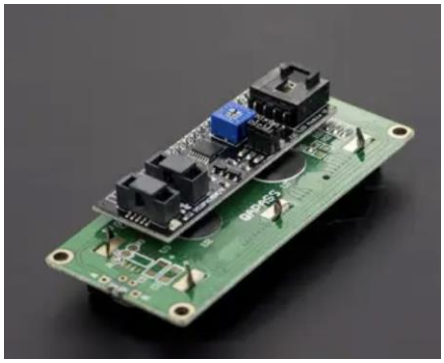


Рис. 3.11 – Зовнішній вигляд модуля I2C

Вихід SDA підключається до відповідного входу мікроконтролера, а вихід SCL підключається до цифрового виходу плати Arduino. За допомогою цих ліній інформація надсилається на модуль S2C, а потім на РК-дисплей.

Модуль клавіатури

Клавіатура цієї системи призначена для введення коду доступу при знятті з охорони приміщення. Його також можна використовувати для зміни системних налаштувань, таких як оновлення кодів доступу. Для цих завдань підійде модуль з набором з 12 мембранних кнопок. Він виконаний у вигляді матриці, що складається

з ліній 3x4, на перетині яких розташовані кнопки. На малюнку 3.12 показано зовнішній вигляд мембранної клавіатури з 12 кнопками.

Рис. 3.12 – Зовнішній вигляд мембранної клавіатури

Виводи модуля клавіатура підключаються до порта мікроконтролера, з яких три застосовуються для сканування, а чотири – для опитування їхнього стану.

Обґрунтування вибору середовища проектування електричних схем.

Додаток EasyEDA було обрано для розробки електричних ланцюгів для домашніх систем сигналізації. ДЕКА-це веб-середовище між платформами для автоматизації процесу проектування електронних схем. Сюди входять наступні компоненти:

- редактор для створення електричних принципових схем;
- середовище для розробки електронних компонентів;
- редактор для створення топології друкованих плат;
- хмарне сховище для зберігання файлів;
- систему керування проєктами;
- симулятор;
- засоби, які дозволяють замовити виготовлення друковані плати.

Зовнішній вигляд головного вікна додатку EasyEDA, який встановлений на ПК, зображений на рис. 3.13.

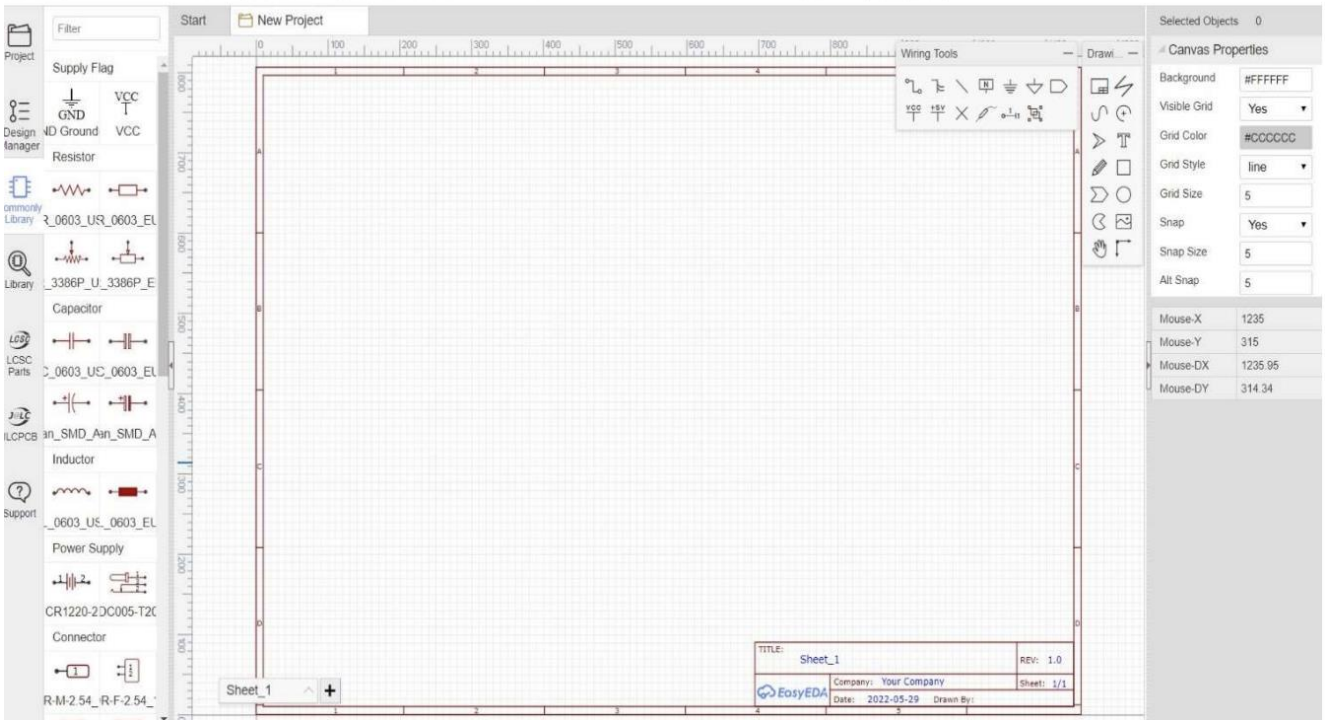


Рис. 3.13 – Зовнішній вигляд головного вікна додатку EasyEDA встановленого на комп’ютері

Працює з моделлю клієнт-сервер EasyEDA. Клієнтська частина програми може працювати в браузері, що підтримує html5. У той же час файл зберігається на хмарному сервері. Ви також можете встановити додаток EasyEDA на свій комп'ютер замість того, щоб працювати в браузері. У цьому випадку файл зберігається на диску комп'ютера з можливістю синхронізації з хмарним сховищем [19].

Розробка електричної схеми пристрою

На малюнку 3.14 показана електрична схема проектованої домашньої сигналізації, розробленої за допомогою програми EasyEDA.

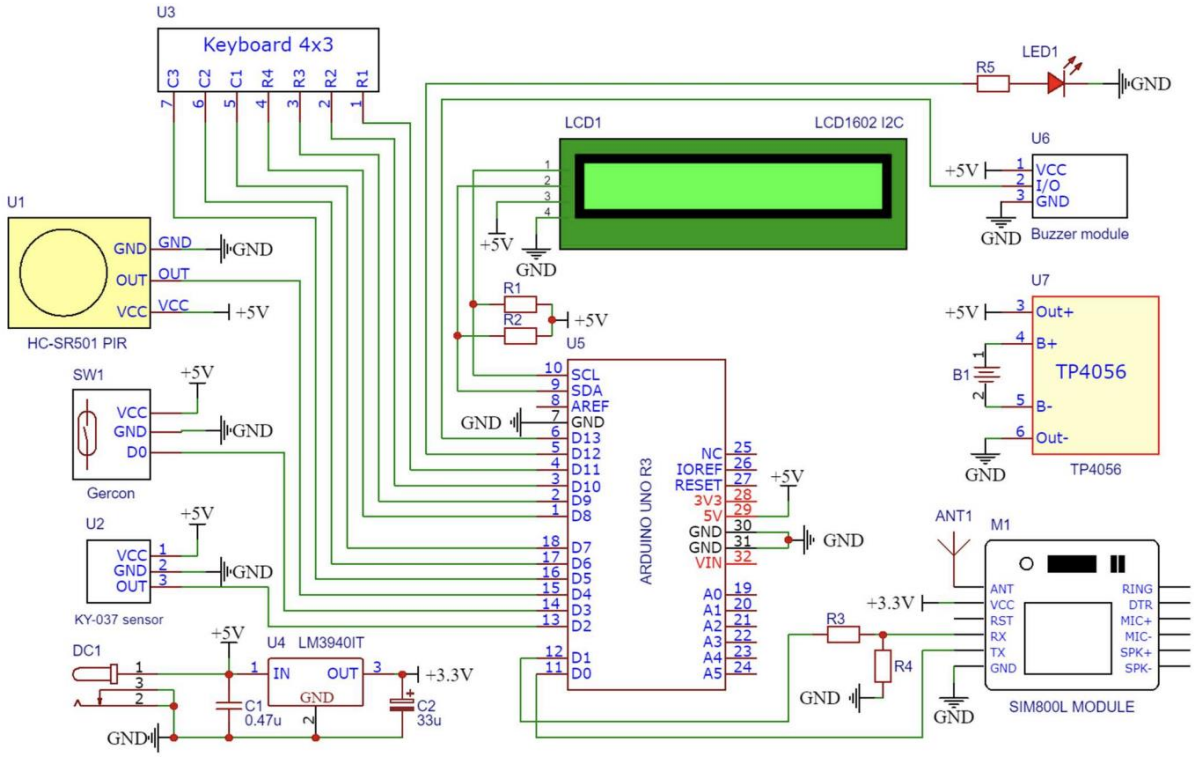


Рис. 3.14 – Електрична принципова схема системи побутової охоронної сигналізації

Живлення цього ланцюга може подаватися від акумулятора B1 через роз'єм DC1 від стандартного джерела живлення або через модуль контролю заряду / розряду U7. Модуль GSM SIM800L живиться від напруги 3,3 В, тому схема забезпечує регульований по напрузі lm4 з символом U390IT. Виходи датчика руху (U1), відкриття дверей (SW1) та розбиття скла (U2) підключені до цифрового входу платформи Arduino UNO, як показано на малюнку U5 [19].

РК-дисплей LCD1 у поєднанні з модулем i2c спілкується з мікроконтролером через лінії sda та SCL. Використовуючи резистори R1 і r2 з номінальними значеннями 10 кВт, затягніть ці лінії до напруги +5 В для правильної роботи і перемкніть їх з інтерфейсу на 2. Модуль GSM M1 взаємодіє з мікроконтролером платформи Arduino через інтерфейс Uart.

Резистори R3 і r4 утворюють дільник напруги, який відповідає рівню сигналу між мод деками U5 і M1 через різні напруги живлення. Антена ANT1 підключається до модуля M1GSM для підвищення рівня сигналу.

3.2. Розробка та налаштування алгоритмів моніторингу та реагування на потенційні загрози

Він починається з активації функції SOS. Після цього починається аналіз вхідного сигналу блоку управління, до якого підключені засіб аутентифікації і датчик. Мікроконтролер порівнює показання датчиків з пороговим значенням, відповідним нормальному стану, встановленому в Налаштуваннях перед першим використанням SOS. Коли один з датчиків змінює свій стан, блок управління негайно розпізнає цю подію і видає сигнал для активації інструменту повідомлень.1 у цій системі вони застосовуються у вигляді світлових і звукових сигналів. Крім того, модуль GSM відправляє повідомлення і/ або телефонний дзвінок власнику приміщення і відправляє його у відділ охоронної компанії, до якого при необхідності може бути підключена система сигналізації [19].

Щоб знешкодити кімнату, вам необхідно ввести відповідний код. Потім ви можете увійти в центр кімнати і змінити режим роботи системи. В цьому випадку датчики продовжують виконувати свої функції, але блок управління не реагує на зміни свого стану.

Програмне забезпечення мікроконтролера складається з 2 основних частин. Перший запускається лише один раз, відразу після включення мікроконтролера. Налаштуйте цифровий вихід і послідовний порт мікроконтролера. 2 до тих пір, поки на мікроконтролер не буде подано напругу живлення. порцію періодично повторюють. Блок-схема алгоритму СОС показана на рисунку 3.15 та рисунок 3.16.

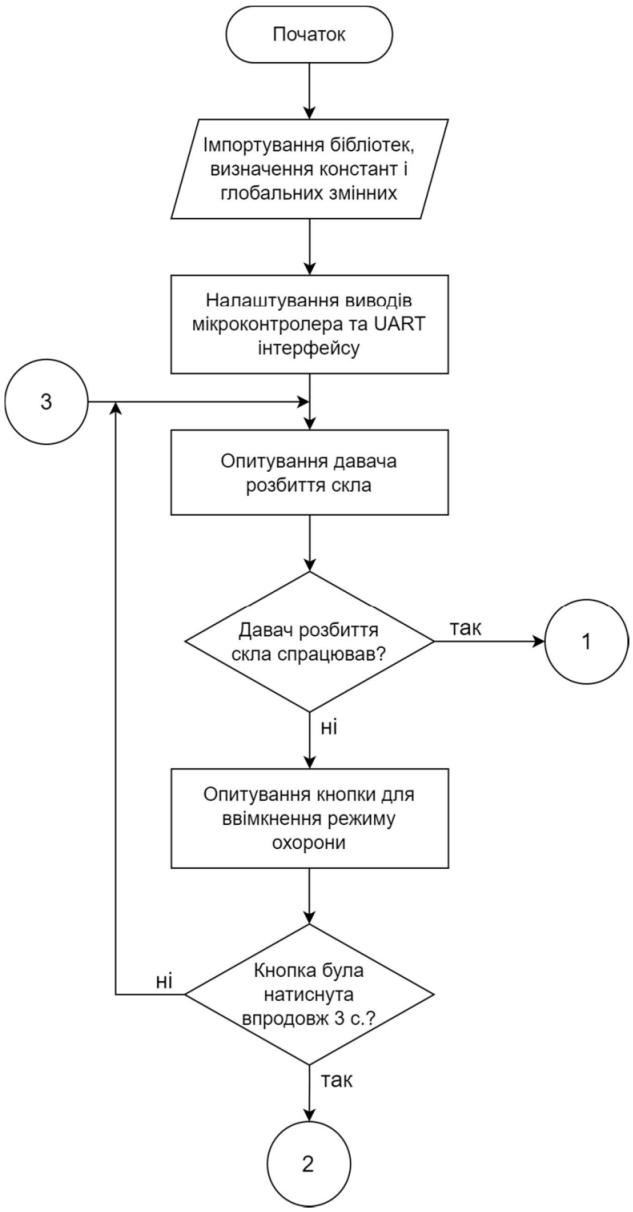


Рис. 3.15 – Блок-схема алгоритму роботи системи охоронної сигналізації

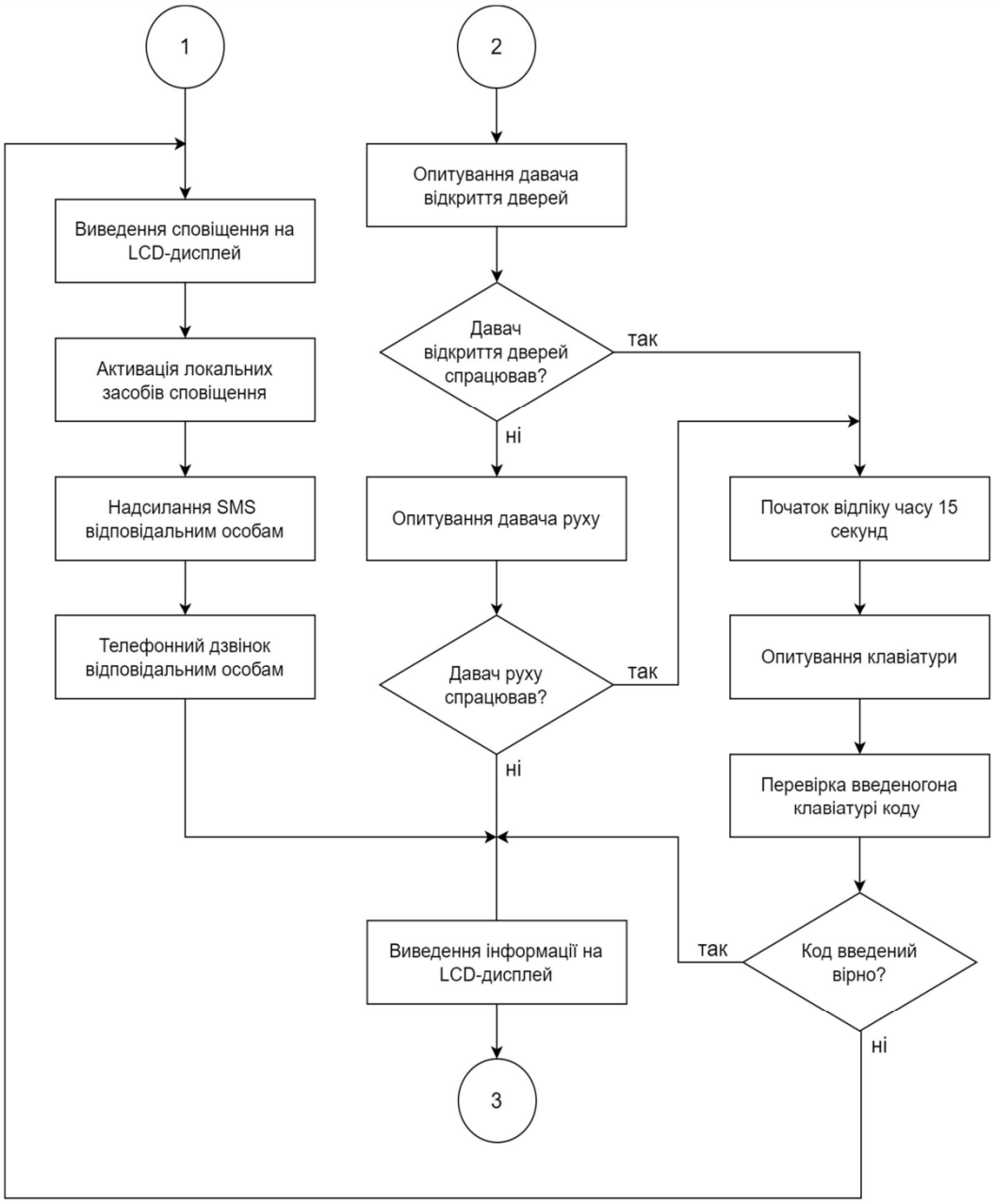


Рис. 3.16 – Блок-схема (продовження)

Програма починається з імпорту необхідних бібліотек і запуску режиму роботи виводу мікроконтролера. Блок-схема алгоритму програми складається з декількох елементів управління, 3 з яких пов'язані з опитуванням і перевіркою показань датчика, а 2 - з перевіркою стану кнопок і клавіатури.

Щоб реалізувати принцип модульності і підвищити зручність, програма розділена на наступні розділи:

1) одиниці вимірювання вхідних сигналів;

2) одиниці зміни стану системи;

Залежно від завдання СОС може бути в 4 режимах:

1) режим очікування: стан датчика ігнорується, і використання відбувається в звичайному режимі.

2) режим безпеки: всі датчики активні, а кімната захищена.

3) режим тривоги: спрацьовує датчик руху або відкривання дверей, користувачеві потрібно 15 секунд, щоб ввести секретний код.

4) режим роботи: інструмент сповіщення буде активовано.

Основна програма, що працює в циклі, починається з процесу зчитування значень всіх висновків мікроконтролера, до якого підключений датчик. Це цифрові та аналогові входи для клавіатури.

Після запису всіх даних у відповідну змінну починається процес обробки. Зокрема, це стосується клавіатури і кнопок, одна з 12 інших кнопок на клавіатурі, необхідна для зміни режиму роботи системи з режиму " очікування "в режим "захисту".

Для цього натисніть кнопку і утримуйте її протягом 3 секунд, а потім залиште кімнату протягом 15 секунд. Протягом цього часу Мікроконтролер перестає виконувати свої функції і гарантує, що користувач встигне вийти з кімнати, щоб сигналізація не відключилася.

Спочатку перевірте датчик розбиття скла. Якщо від нього отримано сигнал, система переходить в режим "спрацьовування". Потім дані з датчика руху обробляються, і двері відкриваються. Якщо ви подасте сигнал про спрацювання 1 з них, система перейде в режим "тривога". У програмному забезпеченні є фрагмент коду, який відповідає за налагодження [19].

Значення змінних, в які записуються дані з датчиків і інформація про стан системи, регулюються шляхом відправки через послідовний порт, що дозволяє відстежувати зміни режиму системи з плином часу. Наступна частина коду-це блок для розшифровки режиму роботи системи.

Цей код призначений для виконання дій, що відповідають певному режиму роботи. У цьому коді певна дія виконується на основі певного набору умов.

1) захист – оскільки система не повинна включатися в цьому режимі, низький рівень напруги подається на клеми, до яких підключені п'єзодинамічний модуль і світлодіодний модуль.

2) тривога - це початок часового інтервалу. Якщо правильний код не введено протягом певного періоду часу, система змінить режим роботи на "тригер".

3) Робота-попередження високий рівень напруги подається на клему, до якої підключено пристрій.

Використовуючи стандартну бібліотеку, створюється команда, яка відправляє SMS-повідомлення з зумовленим текстом і викликає вказаний номер абонента. Після виконання цієї частини коду аудит переходить до початку циклу.

Це дозволяє постійно контролювати стан кімнати за допомогою домашньої сигналізації. У наступному підрозділі ми більш детально розглянемо програмний код і його властивості, що виконуються в операціях, описаних в розглянутому алгоритмі системи [19].

3.3. Фізична реалізація системи: збірка та налаштування компонентів контролера

Мова обробки використовується для програмування мікроконтролера, що використовується платформою Arduino. Він заснований на спрощеній версії мови c / C ++, що підтримується багатьма бібліотеками. Для написання коду було обрано середовище розробки Arduino IDE, багатоплатформну програму, написану на Java.

На рисунку 3.17 показаний вигляд головного вікна середовища Arduino IDE.

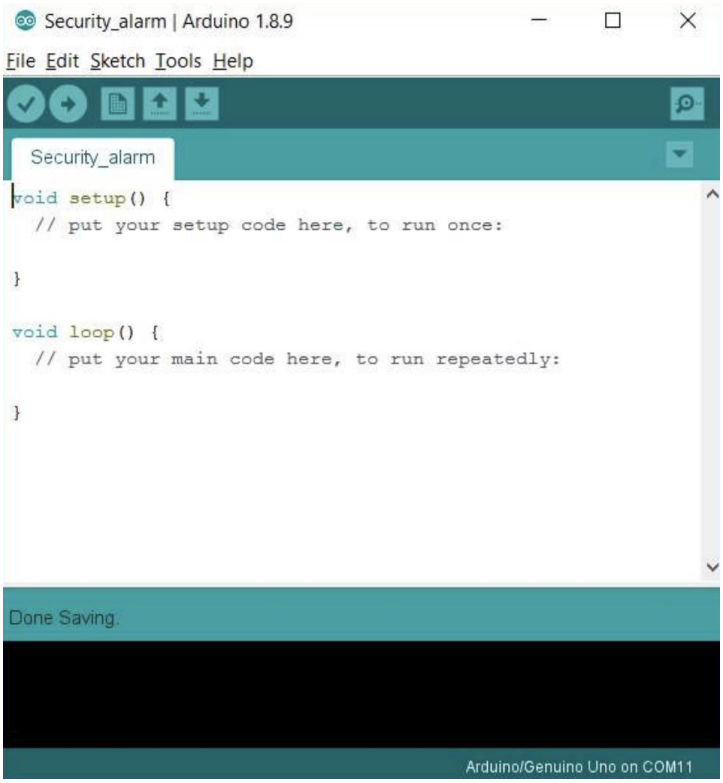


Рис. 3.17 – Зовнішній вигляд головного вікна додатку Arduino IDE

Додаток Arduino IDE містить в собі такі компоненти:

– редактор для написання коду;
– компілятор коду;
– модуль для надсилання прошивки в мікроконтролер.

Підключення бібліотеки для роботи з GSM модулем:

Щоб використовувати модуль SIM800L GSM, вам потрібно встановити відповідну бібліотеку програмного забезпечення у вашому додатку Arduino IDE. Для цього в пункті меню "Інструменти" був обраний пункт "управління бібліотекою". Після відкриття колоди " менеджер бібліотек "я ввів пошуковий термін" SIM800L "у поле" Тип "і натиснув кнопку" Завантажити " поруч із відповідною назвою бібліотеки (рис. 3.18).

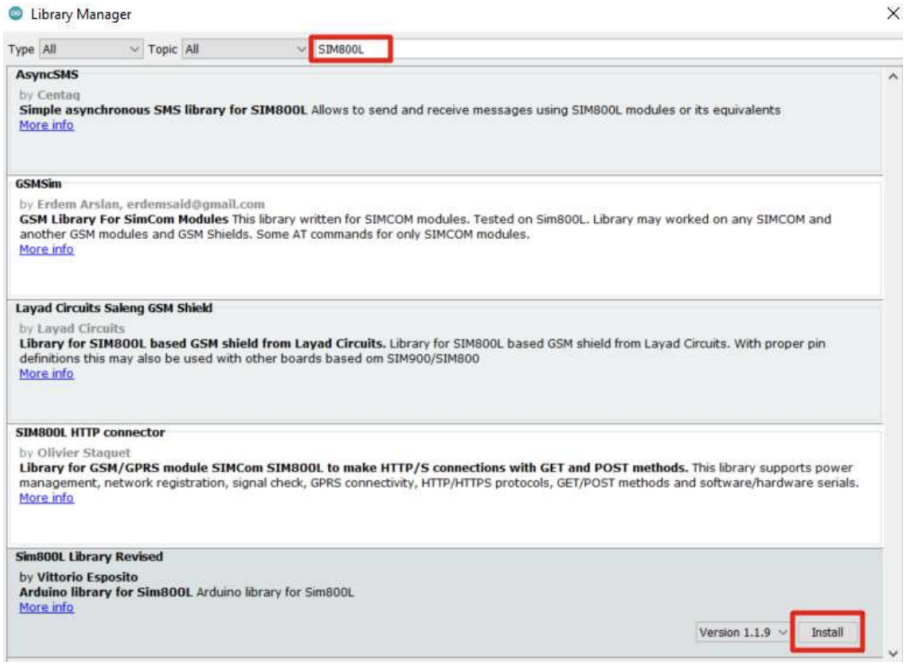


Рис. 3.18 – Встановлення бібліотеки для роботи з модулем SIM800L

В даному підрозділі описані програмні функції, та код програми, який виконується мікроконтролером для реалізації усіх можливостей системи побутової охоронної сигналізації.

Код для опитування клавіатури

Для запуску клавіатури константи для запуску її кнопок визначаються на початку програми (рис. 3.19).

```
1  const int Row[] = {11, 10, 9, 8}; //вивід рядків
2  const int Col[] = {7, 6, 5}; //вивід стовпців
3  const char k3x4 [3][4] = {
4      {'1','2','3'}
5      {'4','5','6'}
6      {'7','8','9'}
7      {'*','0','#'},
8  }; //символи на клавіатурі
```

Рис. 3.19 – Розробка коду з визначенням констант для роботи з клавіатурою

В функції setup() в циклі призначено режим роботи виводів мікроконтролера, які приєднані до рядків клавіатури як цифрові виходи з високим рівнем напруги, а

ті виводи, які приєднані до стовпців – як цифрові входи з підтяжкою до рівня логічної одиниці (рис. 3.20).

```
for (int i=0; i <= 3; i++) {
    pinMode(Row[i], OUTPUT);
    digitalWrite(Row[i], HIGH);
}
for (int i = 0; i <= 2; i++)
pinMode(Col[i], INPUT_PULLUP);

Serial.begin(9600);
Serial.println("begin");
```

Рис. 3.20 – Призначення режиму роботи виводів МК для клавіатури

В функції loop() з періодичністю 50 мс на виводи рядків в циклі послідовно виставляється низький рівень напруги, а у вкладеному циклі опитуються виводи стовпців. Якщо на стовпці виявиться рівень логічного «0», то значить рядок і замкнутий зі стовпцем j, тому натиснута кнопка k3x4(i, j).

Виведення інформації на LCD дисплей.

Перш ніж ви зможете працювати з РК-дисплеєм, вам потрібно підключити бібліотеку для роботи з ним і встановити тему та розміри РК-модуля:

```
#include <LiquedCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x3F,16,2);
```

В функції setup() здійснюється ініціалізація LCD дисплею, та виведення на екран початкового повідомлення (рис. 3.21).

```
lcd.begin();
lcd.backlight();
lcd.print("Alarms          ");
lcd.setCursor(0, 1);
lcd.print("                ");
```

Рис. 3.21 – Розробка коду для ініціалізації LCD дисплею

Код для обміну даними з GSM модулем

Оскільки обмін даними з GSM модулем відбувається по UART інтерфейсу, тому в програмі використана бібліотека SoftwareSerial.h (рис. 3.22).

```
#include <SoftwareSerial.h>
SoftwateSerial SIM800serial (0, 1);
void setup() {
    Serial.begin(9600);
    Serial.println("Alarm        ");
    SIM800serial.begin(9600);
    SIM800serial.println("AT         ");
}
```

Рис. 3.22 – Реалізація коду для ініціалізації UART інтерфейсу для обміну даними між мікроконтролером і GSM модулем

В підпрограмі loop() використовуються функції available() і write() для надсилання та отримання даних (рис. 3.23).

```
if (Serial.available()) {
    SIM800serial.write(Serial.read());
}
if (SIM800serial.available()){
    Serial.write(SIM800serial.read());
}
```

Рис. 3.23 – Розробка коду для надсилання та отримання даних по UART інтерфейсу

На рис. 3.24 наведений лістинг функції для надсилання sms повідомлення через GSM модуль.

```
void sms(String text, String phone)
{
    Serial.println("SMS send started");
    SIM800serial.println("AT+CMGS=\"" + phone + "\"");
    delay(1000);
    SIM800serial.print(text);
    delay(300);
    SIM800serial.print((char)26);
    delay(300);
    Serial.println("SMS send finish");
    delay(3000);
}
```

Рис. 3.24 – Розробка функції для надсилання sms повідомлення через GSM модуль

Команди DTMF

Команда DTMF використовується для набору номера телефону. З їх допомогою генерується багаточастотний двотональний аналоговий сигнал, діапазон дії якого є реалізацією автоматичних телефонних сигналів між пристроями. Зокрема, такі сигнали можуть використовуватися для управління з'єднаннями між аналоговими пристроями (наприклад, між Міні-АТС і телефоном).

Крім того, звуковий сигнал використовується в процесі ручного введення абонентами команд для різних систем, зокрема голосових автовідповідачів. Команди DTMF також часто використовуються на телевізійних та комерційних радіостанціях. Технологія DTMF також широко використовується в системах охоронної сигналізації і"розумного будинку" [20].

У розробленій системі DTMF команда використовується для дистанційного керування сигналізацією за допомогою модуля sim800L. якщо номер записаний в пам'ять SIM-карти, то її власником є користувач, який має можливість включати або вимикати сигналізацію. Номер з ім'ям ADMIN вважається адміністраторським. Якщо в пам'яті SIM-карти такого номера немає, статус адміністратора отримує перший користувач, який дзвонить на нову SIM-карту.

При цьому його номер зберігається в пам'яті телефонної книги. Єдиним користувачем, який може надсилати SMS-повідомлення та команди DTMF, є адміністратор. Команда DTMF використовується для проектованої системи, яка показана на малюнку 3.25.

```
enum
{
    GUARD_ON = 1; // встановлення на охорону
    GUARD_OFF,    // зняття з охорони
    GPRS_ON_OFF, // включити(виключити) GRPS
    SMS_ON_OFF, // включити(виключити) SMS
    TEL_ON_OFF, // включити(виключити) дзвінок при тривозі
    GET_INFO, // збір та відправлення усіх даних дивачів
    EMAIL_ADMIN_PHONE, // надсилання на пошту номер адміна
    EMAIL_PHONE_BOOK, // надсилання на пошту телефонної книги
    ADMIN_NUMBER_DEL, // адміністративний номер більше не адмін
    SM_CLEAR, // видалити всі номери з сім карти
    MODEM_RESET, // перезавантаження модуля
    BAT_CHARGE, // показує інформацію про заряд батареї
    CONNECT_ON_OFF // інвертує прапорець CONNECT_ALWAYS
};
```

Рисунок 3.25 – Список DTMF команд

GSM модуль налаштований на те, щоб підняти трубку при телефонному дзвінку з адміністративного номера. Це реалізовано з метою використання DTMF команд. Телефонні дзвінки, отримані від інших номерів будуть автоматично скидатися. DTMF команди можуть надсилатися адміністратором. Система скине дзвінок, якщо команда буде прийнята. На пошту надійде звіт про виконання команди. Після цього потрібно ввести будь-яку цифру і знак #, що вказує на завершення процесу введення команди. На останньому етапі модуль завершить телефонний дзвінок і запустить на виконання одержану команду [20].

Висновок

У сучасному світі системи охорони зіштовхуються зі складними викликами та проблемами, такими як швидка зміна технологій, розвиток кіберзлочинності та зростання обсягу даних. Визначення проблеми у сучасних системах охорони є першим кроком до створення ефективних та надійних рішень. Цей розділ включає в себе аналіз та опис основних проблем, з якими стикаються сучасні системи охорони, таких як вразливість до кібератак, нестабільність систем та складність управління.

Контролери грають важливу роль у побудові архітектури систем охорони. Вони використовуються для збору, обробки та аналізу даних з датчиків, камер відеоспостереження, систем відстеження та інших джерел. Крім того, контролери забезпечують зв'язок між різними компонентами системи та керування ними. Роль контролерів у побудові архітектури систем полягає в створенні ефективних, надійних та безпечних рішень для забезпечення безпеки та захисту.

Розглянуто функції та можливості контролерів Arduino та визначено їхню важливу роль у побудові архітектури систем охорони. Базуючись на їхній простоті використання, доступності та широкому функціоналі, контролери Arduino стають ефективним інструментом для забезпечення безпеки та захисту. Вони дозволяють збирати та аналізувати дані з різних джерел, керувати різними пристроями та виконувати автоматизовані завдання. Таким чином, контролери Arduino є

важливою складовою сучасних систем охорони, які сприяють покращенню безпеки та захисту в різних сферах життя.

У реалізації системи охорони велике значення має правильний вибір апаратного та програмного забезпечення. Підбір відповідного обладнання, такого як мікроконтролер Arduino Uno, є ключовим етапом, оскільки він забезпечує базовий функціонал для взаємодії з різноманітними датчиками та пристроями.

Налаштування алгоритмів моніторингу та реагування на потенційні загрози вимагає вміння аналізувати дані в реальному часі та приймати відповідні рішення, що можуть бути реалізовані з використанням різних програмних бібліотек та коду.

Фізична реалізація системи включає збірку та налаштування компонентів контролера, встановлення датчиків, пристроїв сповіщення та інших необхідних елементів. Цей етап вимагає уважності та дотримання технічних вимог, щоб забезпечити правильну роботу всієї системи

Загальною метою є створення надійної та ефективної системи охорони, яка забезпечує вчасне виявлення та реагування на потенційні загрози. Використання апаратного та програмного забезпечення, а також правильна фізична реалізація, допомагають досягти цієї мети, забезпечуючи захист об'єктів та майна.

ВИСНОВКИ

У сучасному світі системи охорони зіштовхуються зі складними викликами та проблемами, такими як швидка зміна технологій, розвиток кіберзлочинності та зростання обсягу даних. Визначення проблеми у сучасних системах охорони є першим кроком до створення ефективних та надійних рішень. Цей розділ включає в себе аналіз та опис основних проблем, з якими стикаються сучасні системи охорони, таких як вразливість до кібератак, нестабільність систем та складність управління.

Контролери грають важливу роль у побудові архітектури систем охорони. Вони використовуються для збору, обробки та аналізу даних з датчиків, камер відеоспостереження, систем відстеження та інших джерел. Крім того, контролери забезпечують зв'язок між різними компонентами системи та керування ними. Роль контролерів у побудові архітектури систем полягає в створенні ефективних, надійних та безпечних рішень для забезпечення безпеки та захисту.

Розглянуто функції та можливості контролерів Arduino та визначено їхню важливу роль у побудові архітектури систем охорони. Базуючись на їхній простоті використання, доступності та широкому функціоналі, контролери Arduino стають ефективним інструментом для забезпечення безпеки та захисту. Вони дозволяють збирати та аналізувати дані з різних джерел, керувати різними пристроями та виконувати автоматизовані завдання. Таким чином, контролери Arduino є важливою складовою сучасних систем охорони, які сприяють покращенню безпеки та захисту в різних сферах життя.

Розглянуто технології бездротового зв'язку, які використовуються в системах "розумного будинку". Wi-Fi, Bluetooth, ZigBee та Z-Wave були проаналізовані з точки зору їхніх особливостей, переваг та недоліків у контексті використання в розумних пристроях та системах управління. Висвітлено їхню ефективність, споживання енергії, стійкість до перешкод та інші характеристики, які важливі для вибору оптимального рішення для конкретного застосування.

Проведено аналіз існуючих рішень системи "розумний будинок". Розглянуто різноманітні пропозиції від виробників у цій галузі, включаючи стандартні рішення та спеціалізовані пристрої. Проаналізовано їхні можливості, функціональність, ефективність та зручність в управлінні. Також висвітлено переваги та недоліки різних підходів до створення систем "розумного будинку".

Проаналізовані найпоширеніші вразливості систем "розумний будинок" та типові атаки, які можуть бути спрямовані на розумні домашні пристрої. Розглянуті можливі загрози безпеці, які можуть виникнути внаслідок використання таких систем, а також вказані шляхи захисту від них. Результати аналізу допоможуть розуміти потенційні ризики та вибирати ефективні заходи для забезпечення безпеки в системах "розумного будинку".

У реалізації системи охорони велике значення має правильний вибір апаратного та програмного забезпечення. Підбір відповідного обладнання, такого як мікроконтролер Arduino Uno, є ключовим етапом, оскільки він забезпечує базовий функціонал для взаємодії з різноманітними датчиками та пристроями.

Налаштування алгоритмів моніторингу та реагування на потенційні загрози вимагає вміння аналізувати дані в реальному часі та приймати відповідні рішення, що можуть бути реалізовані з використанням різних програмних бібліотек та коду.

Фізична реалізація системи включає збірку та налаштування компонентів контролера, встановлення датчиків, пристроїв сповіщення та інших необхідних елементів. Цей етап вимагає уважності та дотримання технічних вимог, щоб забезпечити правильну роботу всієї системи

Загальною метою є створення надійної та ефективної системи охорони, яка забезпечує вчасне виявлення та реагування на потенційні загрози. Використання апаратного та програмного забезпечення, а також правильна фізична реалізація, допомагають досягти цієї мети, забезпечуючи захист об'єктів та майна.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Петін В.А. Практична енциклопедія Arduino / В. А. Петін, А. А. Біняковський. – Москва: ДМК Прес, 2020. –- 166 с.

Крамчанинов С.С., Черкесова Л.В. Розробка системи автоматизації будинку (Розумний будинок) / С.С. Крамчанинов, Л.В. Черкесова // Молодий дослідник Дона.– №6. – 2017. – С. 57-62.

Arduino Playground [Електронний ресурс]. Режим доступу https://playground.arduino.cc/

Forum Arduino [Електронний ресурс]. Режим доступу https://forum.arduino.cc/

Мельничук Р.А., Ларченко Л.В. Системи безпеки розумного будинку. / Р.А. Мельничук, Л.В. Ларченко // CXIII Міжнародна інтернетконференція «Розвиток науки та техніки під час воєнного стану». – м. Херсон, 28 листопада, 2022.– С. 156-158.

Forum Arduino [Електронний ресурс]. Режим доступу https://forum.arduino.cc/

Patrascu M. Integrating Services and Agents for Control and Monitoring: Managing Emergencies in Smart Buildings. Service Orientation in Holonic and MultiAgent Manufacturing and Robotics. / Patrascu., 2014. – 544 с

Dickson B. How to prevent your IoT devices from being forced into botnet bondage [Електронний ресурс] / Dickson. – 2015. – Режим доступу до ресурсу: https://techcrunch.com/2016/08/16/how-to-prevent-your-iot-devices-from-being- forcedinto-botnet-slavery/.

Power Load Event Detection and Classification Based on Edge Symbol Analysis and Support Vector Machine [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.hindawi.com/journals/acisc/2012/742461/.

An Overview of Home Automation Systems [Електронний ресурс]. – 2017. –

Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7791223/.

Granzer W. P. Security in Building Automation Systems / Wolfgang Praus Granzer. Munich: Appress, 2018. – 578 с.

Що таке розумний будинок? Все що потрібно знати про систему Розумний Дім [Електронний ресурс]. – Режим доступу до ресурсу: https://bron.ua/article/schotake-rozumnij-budinok-vse-scho-potrbno-znati-pro-sistemu-rozumnij-dm/5/

Технологія розумного будинку: як AI створює простір, комфортний для життя [Електронний ресурс]. – Режим доступу до ресурсу: https://www.everest.ua/tehnologiya-rozumnogo-budynku-yak-ai-stvoryuye-prostirkomfortnyj-dlya-zhyttya/

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.

Моніт Я.В. Система «Розумний будинок» з відкритим програмним забезпеченням/ Я.В.Моніт // XIX науково-технічна конференція студентів та молодих учених «Гіротехнології, навігація, керування рухом та конструювання авіаційно-космічної техніки», 15-16 лютого 2016 р. – К.: «Політехніка», 2016. – С. 43-44.

Тиш Є.В., Зима О.В. Методи та засоби підвищення ефективності безпровідних телеметричних мереж. Збірник тез доповідей VIII Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій». 2019. С. 101.

Vasylkivskyi I., Ishchenko V., Pohrebennyk V., Palamar M., Palamar A. System of water objects pollution monitoring. International Multidisciplinary Scientific GeoConference Surveying Geology and Mining Ecology Management (SGEM 2017), Vienna, Austria. 2017. Vol. 17, No. 33. P. 355-362.

Palamar A. Intelligent control and monitoring module for uninterruptible power supply system. II International Scientific and Practical Conference «Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs» (MC&FPGA-2020), Kharkiv, Ukraine. 2020. P. 12-13.

Зеркалов Д.В. Безпека життєдіяльності. Навчальний посібник. К.: Основа. 2011. 526 с.

Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. 2011. 215 с.

ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ

Державний університет інформаційно-комунікаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

Кваліфікаційна робота на тему:

«Розробка охоронної системи «розумного будинку» на основі Arduino»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав: ЧЕРНОБАЙ Дмитро ІСД-41
Науковий керівник роботи: ДАНИЛЬЧЕНКО Валентина

КИЇВ - 2024

Актуальність теми: Розробка «розумного будинку» за допомогою Arduino відображає сучасні тенденції в галузі безпеки та інтернету речей. Використання Arduino, як доступної та гнучкої платформи, сприяє створенню ефективних та доступних рішень для захисту об'єктів будь-якого типу - від домашніх квартир до комерційних об'єктів.

Мета роботи – дослідити можливості та переваги використання Arduino для розробки «розумного будинку», а також створити прототип такої системи, який би демонстрував її ефективність та потенційні можливості.

Об'єкт дослідження – система охорони за допомогою Arduino.

Предмет дослідження – принципи, методи та технології, що лежать в основі розробки та використання «розумних будинків» на базі Arduino.

Наукові завдання:

- порівняння різних методів моніторингу та реагування на потенційні загрози в системах охорони на базі Arduino.
- вивчення впливу різних типів датчиків на точність та надійність виявлення потенційних загроз.
- розробка алгоритмів самодіагностики та виявлення несправностей в системах охорони.
- дослідження можливостей інтеграції системи охорони на базі Arduino з іншими "розумними" пристроями та системами.
- вивчення питань безпеки та захисту даних у системах охорони на базі Arduino з метою запобігання несанкціонованому доступу та кібератакам.

2

Розумний дім на базі Arduino

4

"Розумний дім" на базі Arduino — це система автоматизації та управління різними аспектами домашнього середовища з використанням мікроконтролера Arduino. Вона дозволяє створювати інтерактивні та інтелектуальні системи, які забезпечують комфорт, безпеку та енергоефективність.

Контролерів Arduino

5

Рисунок 1 Плата Arduino Nano

Рисунок 2 Плата Arduino Uno

Рисунок 3 Плата Arduino Mega

В роботі як головний модуль для управління проєктованою системою використовувалась плата Arduino UNO.

Аналіз існуючих рішень системи "розумний будинок"

6

Рисунок 4 Система «розумного будинку» Ajax StarterKit

Рисунок 5 Система «розумного будинку» Xiaomi Mijia

Рисунок 6 – Система «розумного будинку» Google Home

Рисунок 7 – Система «розумного будинку» Amazon Alexa

Апаратне та програмне забезпечення для реалізації системи охорони

7

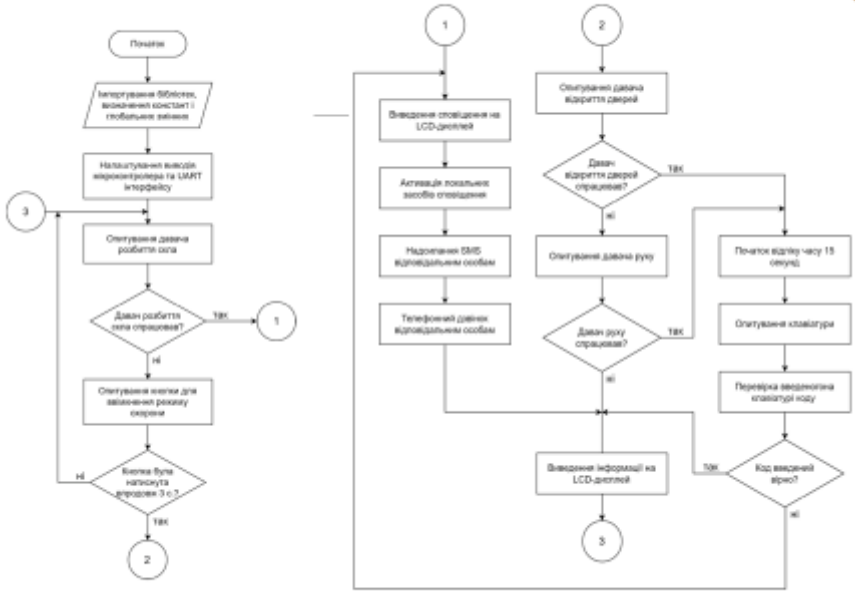
Рисунок 8 – Основний модуль Arduino UNO

Рисунок 9 – Мікроконтролер ATmega328P, який використовується в платі Arduino Uno

Рисунок 10 – Додаток EasyEDA було обрано для розробки електричних ланцюгів для домашніх систем сигналізації

Блок-схема алгоритму роботи системи охоронної сигналізації

8



Збірка та налаштування компонентів контролера

9

Рисунок 11 – Зовнішній вигляд головного вікна додатку Arduino IDE

```
const int Row[] = {11, 10, 9, 8}; //вивід рядків
const int Col[] = {7, 6, 5}; //вивід стовпців
const char k3x4 [3][4] = {
    {'1','2','3'}
    {'4','5','6'}
    {'7','8','9'}
    {'*','0','#'},
}; //символи на клавіатурі
```

Рисунок 12 – Розробка коду з визначенням констант для роботи з клавіатурою

```
#include <LiquedCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x3F,16,2);
```

Рисунок 13 – Виведення інформації на LCD дисплей

```
lcd.begin();
lcd.backlight();
lcd.print("Alarms          ");
lcd.setCursor(0, 1);
lcd.print("                ");
```

Рисунок 14 – Розробка коду для ініціалізації LCD дисплею

Рисунок 15 – Розробка функції для надсилання sms повідомлення через GSM модуль

ВИСНОВКИ

10

- Розглянуто функції та можливості контролерів Arduino та визначено їхню важливу роль у побудові архітектури систем охорони. Базуючись на їхній простоті використання, доступності та широкому функціоналі, контролери Arduino стають ефективним інструментом для забезпечення безпеки та захисту.

- Розглянуто технології бездротового зв'язку, які використовуються в системах "розумного будинку". Wi-Fi, Bluetooth, ZigBee та Z-Wave були проаналізовані з точки зору їхніх особливостей, переваг та недоліків у контексті використання в розумних пристроях та системах управління.

- Проаналізовані найпоширеніші вразливості систем "розумний будинок" та типові атаки, які можуть бути спрямовані на розумні домашні пристрої.

- Проведено налаштування та підключення компонентів: режим роботи виводів, виведення інформації LCD, обміну даними з GSM модулем. Для написання коду було обрано середовище розробки Arduino IDE.

- Розроблена функція для надсилання sms повідомлення через GSM модуль.

Дякую за увагу!
Доповідь закінчено