ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Розробка IoT-рішення охоронної системи підприємства за допомогою Arduino.»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Іван НІКОНОВ

(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач(ка) вищої освіти гр. 41
Іван НІКОНОВ
Ім'я, ПРІЗВИЩЕ

Керівник: PhD Валентина ДАНИЛЬЧЕНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

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 кафедрою Каміла СТОРЧАК
Ім'я, ПРІЗВИЩЕ
«____»_____20__р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Ніконову Івану Миколайовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Розробка IoT-рішення охоронної системи підприємства за допомогою Arduino.

керівник кваліфікаційної роботи Данильченко Валентина Миколаївна, PhD
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024р.

3. Вихідні дані до кваліфікаційної роботи:
1. Науково-технічна література з теми бакалаврської роботи.
2. Принцип функціонування системи безпеки на основі Arduino.
3. Основні принципи роботи компонентів

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Інтернет-речей IoT. Визначення та можливості.
2. Інструменти та прийоми розробки охоронної системи
3. Розробка охоронної системи на основі Arduino

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «27» лютого 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	27.02-05.03.2024	
2	Обгрунтування актуальності роботи	06.03-11.03.2024	
3	Аналіз основних можливостей Arduino	12.03-27.03.2024	
4	Інструменти та прийоми розробки системи на Arduino	28.03-10.04.2024	
5	Розробка IoT-рішення охоронної системи підприємства за допомогою Arduino	11.04-15.05.2024	
6	Програмування та тестування системи	11.04-15.05.2024	
7	Оформлення роботи: вступ, висновки, реферат	16.05-22.05.2024	
8	Розробка демонстраційних матеріалів	23.05-24.05.2024	

Здобувач вищої освіти _____ Іван НІКОНОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Валентина ДАНИЛЬЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра (магістра): 78 стор., 40 рис., 0 табл., 20 джерел.

Мета роботи – Розробити та впровадити систему безпеки на основі Інтернету речей для компанії з використанням Arduino, яка може виявляти та сповіщати про порушення безпеки в режимі реального часу.

Об'єкт дослідження – Спроектувати та розробити систему безпеки на основі IoT з використанням Arduino. Інтегрувати датчики та актуатори з платою Arduino для виявлення та реагування на порушення безпеки. Розробити хмарну платформу для моніторингу та оповіщення в режимі реального часу. Протестувати та оцінити систему в реальних умовах.

Предмет дослідження – Предметом дослідження є розробка системи безпеки на основі IoT з використанням Arduino, яка може бути застосована в різних галузях промисловості та організаціях для підвищення їх безпеки та зменшення ризику крадіжок, вандалізму та інших порушень безпеки.

Короткий зміст роботи - Функціональна система безпеки на основі IoT з використанням Arduino. Покращена безпека та зменшений ризик крадіжок та вандалізму .Покращені можливості моніторингу та оповіщення в реальному часі. Підвищення ефективності та результативності роботи персоналу охорони.

КЛЮЧОВІ СЛОВА: ARDUINO, IoT, ОХОРОННА СИСТЕМА, ХМАРНА ПЛАТФОРМА, МОНІТОРИНГ.

ABSTRACT

The text part of the qualification work for obtaining a bachelor's (master's) degree: 78 pages, 40 figures, 0 tables, 20 sources.

Job Objective – Design and implement an IoT-based security system for a company using Arduino that can detect and notify security breaches in real-time.

Research object – Design and develop an IoT based security system using Arduino. Integrate sensors and actuators with an Arduino board to detect and respond to security breaches. Develop a cloud-based platform for real-time monitoring and alerting. Test and evaluate the system in real conditions.

Research Subject - The research subject is the development of an IoT-based security system using Arduino, which can be applied in various industries and organizations to increase their security and reduce the risk of theft, vandalism and other security breaches.

Summary of work - Functional security system based on IoT using Arduino. Improved security and reduced risk of theft and vandalism. Improved real-time monitoring and alerting capabilities. Increasing the efficiency and effectiveness of security personnel.

KEYWORDS: ARDUINO, IoT, SECURITY SYSTEM, CLOUD PLATFORM, MONITORING**.**

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут інформаційних технологій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Ніконов І.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)
на тему: «Розробка IoT-рішення охоронної системи підприємства за допомогою Arduino.».

Кваліфікаційна робота і рецензія додаються.

Директор ННІІТ _____ Андрій Бондарчук
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач _____

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача(ки) _____ на оцінку «_____» та присвоїти йому(їй) кваліфікацію _____.

Керівник кваліфікаційної роботи _____ Валентина Данильченко
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____»_____20___року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Ніконов І.М..* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Інженерії програмного забезпечення автоматизованих систем _____ Каміла Сторчак
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну роботу

на здобуття освітнього ступеня бакалавра

здобувача вищої освіти Ніконов Іван Миколайович

(прізвище, ім'я, по батькові)

на тему «Розробка IoT-рішення охоронної системи підприємства за допомогою Arduino.»

Актуальність.

У сучасному світі Інтернет речей (IoT) стає все більш поширеним, інтегруючись у різні сфери життя та діяльності. В умовах зростання складності бізнес-процесів та ризиків, пов'язаних з безпекою, питання захисту підприємств набуває особливої важливості. Традиційні системи безпеки, хоча і залишаються ефективними, часто не мають необхідної гнучкості та можливості швидкого масштабування.

Позитивні сторони.

1. Гнучкість та масштабованість
2. Економічність
3. Широкий спектр можливостей

Недоліки.

1. Складність налаштування та обслуговування
2. Обмежені ресурси та потужність

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи бакалаврської .

Висновок: *кваліфікаційна робота на здобуття ступеня бакалавра заслуговує оцінку "Відмінно", а здобувач* Ніконов І.М.

заслуговує присвоєння кваліфікації: Інформаційні системи та технології

Рецензент:

науковий ступінь, вчене звання _____ *підпис* _____ *Ім'я, ПРІЗВИЩЕ*

ЗМІСТ

ВСТУП

Актуальність теми. Сьогодні Інтернет речей (IoT) відіграє все більш важливу роль у багатьох аспектах суспільства, надаючи інноваційні рішення, які підвищують ефективність і безпеку в різних галузях. Одним із таких напрямків є безпека підприємства. Це стає дедалі важливішим із зростанням складності та ризиків, пов'язаних із сучасним бізнесом. Забезпечення надійної безпеки стає критичним завданням для кожної організації. Використання мікроконтролерів Arduino для створення систем безпеки на основі IoT не тільки підвищує ефективність захисту, але й забезпечує гнучкість, масштабованість та економічну доцільність таких систем.

Мета і завдання дослідження. Основними цілями цього дослідження є теоретичний огляд та аналіз, систематизація та дослідження наявних знань щодо застосування технології Інтернету речей на основі мікроконтролерів Arduino для забезпечення безпеки підприємства. Для досягнення цілей роботи необхідно вирішити такі науково-практичні завдання:

1. Огляд існуючих технологій Інтернету речей, які реалізовані та використовуються в безпеці підприємства.
2. Дослідіть можливості мікроконтролерів Arduino під час створення систем безпеки.
3. Визначте перспективи та можливі обмеження використання IoT та Arduino для підвищення безпеки вашого підприємства.
4. Оцініть ефективність використання датчиків та інших компонентів на основі Arduino в інтегрованій системі безпеки підприємства.

Предмет дослідження. Система безпеки підприємства, що використовує технологію Інтернету речей на основі мікроконтролерів Arduino.

Метод дослідження. У дослідженні використовувалися такі наукові методи, як теорія системного аналізу, теорія моделювання, методи порівняльного аналізу та емпіричні методи.

Практичне значення отриманих результатів. Проаналізовані результати можуть бути використані для розробки нових підходів до забезпечення безпеки підприємства та оптимізації систем безпеки та контролю доступу. Це зменшує ризик несанкціонованого доступу, підвищує безпеку та зменшує витрати на безпеку. Мікроконтролери Arduino та технологія IoT дозволяють створювати гнучкі, масштабовані та економічно ефективні рішення, які можна швидко адаптувати до конкретних потреб підприємства та умов роботи.

1. ОГЛЯД КОНЦЕПЦІЇ ІНТЕРНЕТУ РЕЧЕЙ (ІОТ)

Інтернет речей (IoT) є однією з найбільш важливих інноваційних концепцій в сучасній технологічній сфері. Вона передбачає створення мережі зв'язаних між собою фізичних пристроїв, які можуть обмінюватися даними та взаємодіяти один з одним через Інтернет. Ця концепція відкриває безліч можливостей у різних галузях, від промисловості та транспорту до медицини та побутових пристроїв.

Основною метою IoT є забезпечення зв'язку та обміну даними між фізичними пристроями, що раніше були відокремлені. Це дозволяє створювати інтелектуальні системи, які можуть автоматизувати багато процесів, полегшити життя людей та підвищити продуктивність промислових процесів. Наприклад, в сільському господарстві системи IoT можуть використовуватися для моніторингу урожаю та автоматичного поливу, що дозволяє знизити витрати та підвищити врожайність.

Для реалізації концепції IoT використовуються різноманітні технології та пристрої. Сенсори та датчики забезпечують збір різноманітної інформації про навколишнє середовище, а мережеве обладнання дозволяє передавати ці дані через Інтернет. Управління та аналіз даних здійснюється за допомогою спеціального програмного забезпечення, яке дозволяє реалізувати різноманітні застосунки IoT.

Інтернет речей вже знаходить застосування в різних галузях. У медицині він використовується для віддаленого моніторингу стану пацієнтів та підтримки життєво важливих функцій. У промисловості IoT дозволяє автоматизувати виробничі процеси та вдосконалити системи контролю якості. В транспорті він може використовуватися для відстеження та моніторингу транспортних засобів та вантажів. У побуті системи IoT можуть допомагати в керуванні будинком та забезпеченні його безпеки.

Загалом, Інтернет речей відкриває безмежні можливості для впровадження технологій у різні сфери життя. Він є однією з ключових технологічних тенденцій XXI століття і очікується, що в майбутньому він стане ще більш поширеним та важливим інструментом для забезпечення зв'язку та автоматизації різних процесів.

Рисунок 1 - Програми IOT

1.1 Основні компоненти систем безпеки підприємства

Системи безпеки підприємства включають в себе ряд ключових компонентів, які спрямовані на захист майна, співробітників і конфіденційної інформації. Ці компоненти інтегровані в комплексну систему на основі Arduino (Рисунок 1.1 плата Arduino), яка повинна захистити підприємство від різних загроз, таких як крадіжки, вандалізм, пожежі та кібератаки.

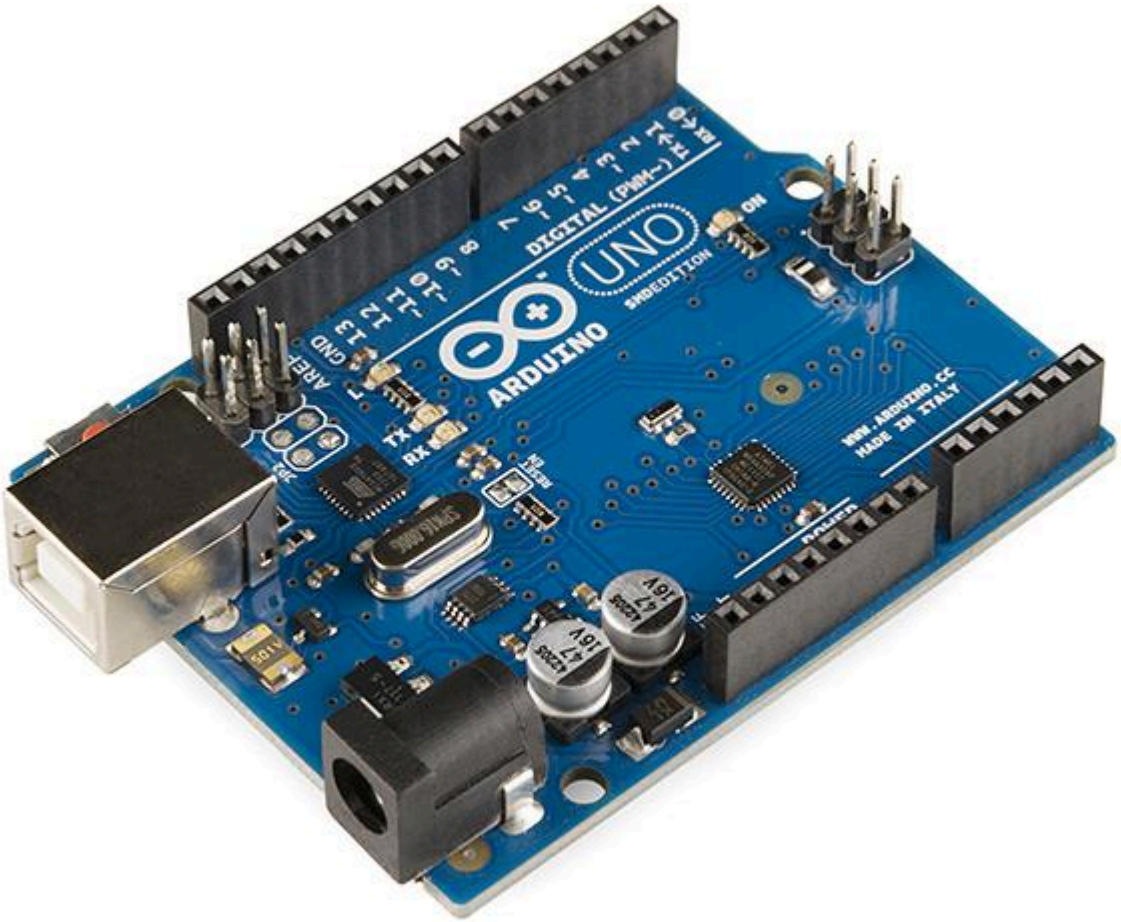

Рисунок 1.1 - плата Arduino

Однією з ключових складових систем безпеки є фізична безпека. Сюди входять системи контролю доступу (Рисунок 1.2 RFID-зчитувач), які обмежують доступ до певних приміщень або об'єктів лише уповноваженим співробітникам або особам. До цієї складової також належать системи відеоспостереження, які виводяться на монітори охоронців і дозволяють їм своєчасно виявляти підозрілі дії та події.

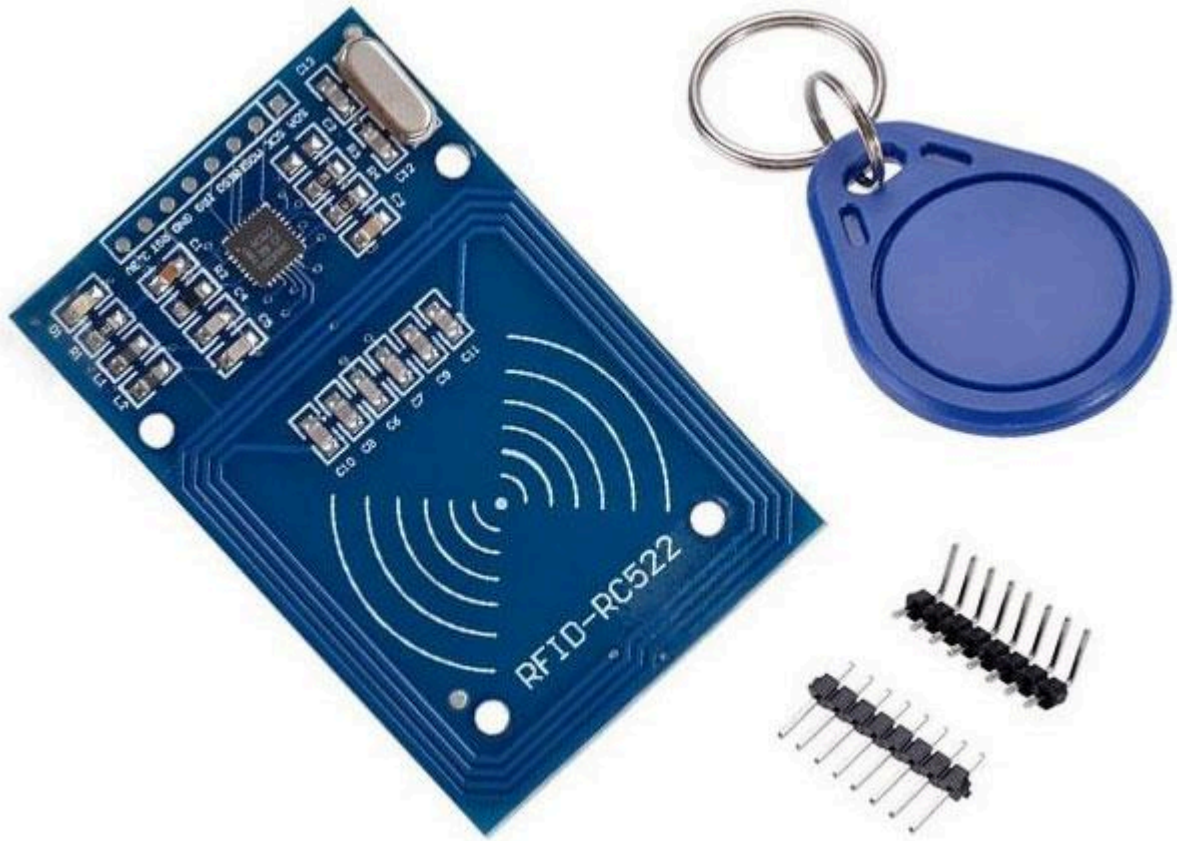

Рисунок 1.2 - RFID-зчитувач

Ще одним важливим компонентом є кібербезпека. У зв'язку зі зростанням кількості кіберзагроз, бізнес повинен мати надійні заходи для захисту своєї інформації та мережевої інфраструктури від хакерських атак і витоку даних. Це може включати встановлення спеціалізованих програмних засобів для виявлення та запобігання атакам, а також регулярні тренінги з кібербезпеки для персоналу.

Системи безпеки також можуть включати системи пожежної безпеки, які виявляють і сигналізують про пожежну небезпеку, а також системи оповіщення про надзвичайні ситуації, які швидко і ефективно інформують співробітників і охоронців про надзвичайні ситуації. (Рисунок 1.3 Датчик руху та відкриття (сигналізація)

Рисунок 1.3 - Датчик руху та відкриття (сигналізація)

Високотехнологічні підприємства також можуть використовувати спеціалізовані системи моніторингу та контролю, які дозволяють в режимі реального часу відстежувати стан різних систем і пристроїв та оперативно реагувати на проблеми.

Загалом, ефективна система безпеки підприємства повинна поєднувати різні компоненти фізичної та кібербезпеки, щоб забезпечити комплексний захист від різних загроз. Вона має бути гнучкою, масштабованою та надійною, щоб забезпечити безпеку підприємства в умовах, що постійно змінюються.

1.1.1 Види систем безпеки та їх призначення

Види систем безпеки різняться за своїми характеристиками та призначенням, проте їх спільна мета полягає в захисті різних аспектів діяльності підприємства або організації. Розглянемо деякі з них:

1. Фізична безпека: Цей вид систем безпеки забезпечує захист фізичних об'єктів, таких як будівлі, приміщення, обладнання та майно від несанкціонованого доступу, крадіжок та інших загроз. До складу фізичних систем безпеки можуть входити датчики руху, відеоспостереження, системи контролю доступу та сигналізація.
2. Інформаційна безпека: Ця система безпеки спрямована на захист конфіденційності, цілісності та доступності інформації. Вона включає в себе заходи для захисту комп'ютерних систем, мереж та даних від кібератак, вірусів, зловмисного програмного забезпечення та інших цифрових загроз.
3. Психологічна безпека: Цей аспект безпеки орієнтований на створення безпечного та комфортного робочого середовища для працівників та відвідувачів. Він включає в себе профілактичні заходи, психологічну підтримку, навчання з питань безпеки та процедури кризового управління для забезпечення психологічного комфорту та зняття стресу.

Розробка Інтернету речей (IoT) для охоронної системи підприємства за допомогою Arduino може стати ефективним рішенням для інтеграції цих видів систем безпеки. Використання Arduino дозволяє легко створювати та програмувати пристрої, що працюють з різними типами сенсорів та пристроїв зв'язку. Такі пристрої можуть виконувати різноманітні функції, включаючи виявлення руху, зчитування даних з датчиків, запис відео та звукове оповіщення, а також керування системами безпеки через Інтернет. Завдяки цьому, IoT-рішення на базі Arduino можуть стати ефективним інструментом для комплексного забезпечення безпеки підприємства.

1.1.2 Важливість інтеграції систем безпеки в підприємницьку інфраструктуру.

Інтеграція систем безпеки у підприємницьку інфраструктуру є критично важливою для забезпечення захисту працівників, майна та конфіденційної інформації. Ось кілька аспектів, які підкреслюють важливість цієї інтеграції:

1. Забезпечення безпеки працівників та відвідувачів: Системи безпеки, такі як системи контролю доступу та відеоспостереження, допомагають у запобіганні несанкціонованому доступу до об'єктів та приміщень підприємства. Це може включати контроль за входами та виходами, ідентифікацію осіб та моніторинг дій.
2. Захист майна та активів: Системи сигналізації та виявлення вторгнень дозволяють вчасно реагувати на небезпечні ситуації, такі як спроби злому або крадіжки. Це допомагає у запобіганні втрат та пошкоджень майна підприємства.
3. Захист конфіденційної інформації: Інтеграція систем інформаційної безпеки дозволяє захищати конфіденційну інформацію від несанкціонованого доступу, витоку даних та кібератак. Це може включати захист комп'ютерних систем, шифрування даних та моніторинг мережевої активності.
4. Забезпечення безпеки виробничих процесів: Системи безпеки також можуть бути інтегровані з виробничими процесами для запобігання нещасних випадків та забезпечення безпеки працівників під час роботи з обладнанням та машинами.

Інтеграція цих систем дозволяє підприємствам ефективно реагувати на потенційні загрози та мінімізувати ризики для безпеки та безперебійності діяльності. В результаті це сприяє покращенню репутації підприємства, зниженню витрат та забезпеченню спокійної та продуктивної робочої атмосфери.

1.2 Огляд мікроконтролерів Arduino та їх можливостей

Мікроконтролери Arduino є популярною платформою для розробки різноманітних електронних пристроїв та проектів з програмування. Вони характеризуються простотою використання, доступністю та широким спектром функціональних можливостей, що робить їх ідеальним вибором для створення систем безпеки підприємства на основі Інтернету речей (IoT).

Arduino базується на мікроконтролерах AVR (Рисунок 1.4) або ARM (Рисунок 1.5), які мають різні характеристики та можливості. Вони оснащені вбудованим USB-портом для легкого підключення до комп'ютера та програмування. Arduino має велику спільноту користувачів і розробників, які активно діляться своїм досвідом і створюють нові бібліотеки та проекти.

Мікроконтролери AVR (Advanced Virtual RISC) і ARM (Advanced RISC Machine) представляють дві різні мікропроцесорні архітектури, що використовуються в мікроконтролерах, включаючи платформи Arduino. Ось деякі з основних відмінностей між ними:

Архітектура: AVR - це 8-розрядні мікроконтролери, в той час як ARM - 32-розрядні мікроконтролери. Це означає, що ARM має більшу кількість робочих бітів, що дозволяє йому обробляти більші обсяги даних і виконувати складніші операції.

1. Продуктивність: ARM зазвичай має кращу продуктивність порівняно з AVR завдяки більшій ширині слова та більшій кількості робочих бітів. Це дозволяє ARM ефективніше виконувати обчислення та операції з обробки даних.
2. Енергоефективність: AVR, як правило, більш енергоефективні, оскільки 8-розрядна архітектура зазвичай вимагає менше енергії, ніж 32-розрядна архітектура ARM. Це може бути важливим фактором для деяких застосувань, особливо у вбудованих системах з обмеженим джерелом живлення.
3. Вартість: Мікроконтролери AVR, як правило, дешевші за ARM через їх менш складну архітектуру і, як наслідок, меншу кількість ресурсів, необхідних для виробництва.

Вибір між AVR і ARM зазвичай залежить від конкретних потреб проекту, таких як продуктивність, енергоефективність, вартість і доступність необхідних ресурсів.

Рисунок 1.4 - Мікроконтролер AVR

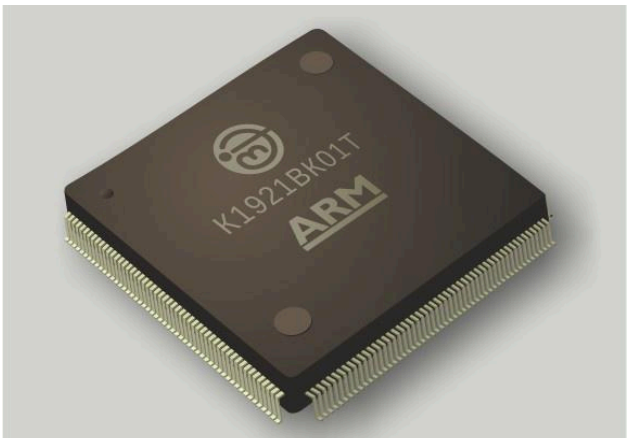

Рисунок 1.5 - Мікроконтролер ARM

Головною перевагою мікроконтролерів Arduino є висока простота використання, що робить їх доступними навіть для початківців у програмуванні та електроніці. Це досягається завдяки простому та інтуїтивно зрозумілому інтерфейсу програмування, який дозволяє швидко вивчити основні принципи програмування та електроніки без будь-яких спеціальних знань.

Arduino підтримує велику кількість різних датчиків, модулів і розширень, що робить її універсальним і гнучким інструментом для створення різноманітних проектів з безпеки підприємства. Це дає розробникам можливість легко і швидко розширювати функціональність своїх пристроїв і систем, додавати нові функції і адаптувати їх до конкретних потреб.

Крім того, Arduino має велику кількість бібліотек і вбудованих функцій, які значно спрощують розробку різних додатків. Ці бібліотеки надають доступ до широкого спектру функцій, які дозволяють взаємодіяти з датчиками, перетворювачами, механізмами управління та відображати інформацію з мінімальними зусиллями програміста.

1.2.1 Історія та розвиток мікроконтролерів Arduino.

Історія та розвиток мікроконтролерів Arduino є захоплюючим шляхом в області електроніки та робототехніки. Варто розглянути кілька ключових моментів у їхній історії:

- Початки: Arduino з'явився у 2005 році, коли Массімо Банзі, Девід Кушіє та Девід Мелліс з Масачусетського технологічного інституту створили прототип плати для свого студентського проекту. Ця плата, яку вони назвали Arduino, мала простий та доступний інтерфейс програмування для створення інтерактивних пристроїв.
- Випуск перших моделей: У 2005 році була випущена перша модель Arduino, яку звали Arduino Uno. Ця плата стала вкрай популярною серед хобістів, студентів та професійних розробників завдяки своїй простоті використання та розширеним можливостям програмування.
- Подальший розвиток: Протягом наступних років Arduino продовжував розвиватися, випускаючи нові моделі з розширеними можливостями та покращеною функціональністю. Було розроблено різноманітні додатки та розширення для сприяння розвитку та використання мікроконтролерів Arduino у різних областях, від робототехніки до Інтернету речей.
- Роль у русі відкритого програмного забезпечення: Arduino став ключовим гравцем у русі відкритого програмного забезпечення, сприяючи вільному обміну коду, ідеям та проектами. Це сприяло зростанню спільноти користувачів та розробників, що взаємодіяли та спільно розвивали нові технології.
- Сучасний стан: На сьогоднішній день Arduino залишається однією з найпопулярніших платформ для розробки прототипів електронних пристроїв. Вона використовується у широкому спектрі проектів, від навчальних до комерційних, і продовжує привертати увагу розробників з усього світу.

Історія Arduino віддзеркалює не лише технологічний прогрес, а й роль спільноти у створенні та поширенні інноваційних ідей у сфері електроніки та програмування.

1.2.2 Опис можливостей платформи Arduino для розробки IoT-рішень.

Платформа Arduino є однією з найпоширеніших і ефективних платформ, що дозволяють розробляти рішення в області Інтернету речей (IoT). Нижче наведено опис ключових функцій цієї платформи для розробки рішень IoT.

- Простота використання: однією з головних переваг Arduino є простота використання. Він має інтуїтивно зрозумілий, простий для розуміння інтерфейс, тож навіть початківець програміст може швидко освоїти функції.
- Широкий вибір датчиків і модулів: Arduino підтримує різноманітні датчики, модулі та розширення, що робить його універсальним і гнучким інструментом для створення різноманітних проектів. Ви можете легко підключити різні датчики для вимірювання температури, вологості, освітлення, руху тощо.
- Універсальність: Arduino може виконувати широкий спектр завдань, від читання даних із датчиків до керування різноманітними пристроями. Їх можна запрограмувати для виконання різноманітних завдань, включаючи передачу даних через мережу, керування виконавчими механізмами та взаємодію з іншими пристроями через різноманітні комунікаційні інтерфейси.
- Велика спільнота користувачів: Arduino має велику та активну спільноту користувачів, яка надає велику кількість документації, приклади коду, поради та підтримку. Це дозволяє швидко вирішувати будь-які проблеми, з якими ви можете зіткнутися, і ділитися своїми знаннями з іншими.
- Розширені можливості програмування: Arduino підтримує різноманітні мови програмування, включаючи C і C++, що відкриває широкий спектр можливостей для розробки складних програм.

Загалом Arduino — це потужний інструмент розробки IoT, який поєднує в собі простоту використання, розширені функції та широку підтримку спільноти, що робить його ідеальним вибором для будь-якого проекту в цій галузі.

1.2.3 Порівняння Arduino з іншими мікроконтролерами для IoT.

Порівняння Arduino з іншими мікроконтролерами для Інтернету речей (IoT) є важливим моментом при виборі платформи для розробки проекту. Розглянемо деякі аспекти цього порівняння.

1. Простота використання: Arduino відомий своєю простотою використання та навчання, що робить його ідеальним вибором для новачків. У порівнянні з іншими мікроконтролерами Arduino має більш доступний та інтуїтивно зрозумілий інтерфейс програмування.
2. Розширені функції: Arduino має простий інтерфейс, але також пропонує багато можливостей для розширення своєї функціональності. Велика кількість доступних датчиків, модулів і бібліотек робить Arduino універсальним і гнучким інструментом для розробки різноманітних проектів.
3. Вартість: Arduino зазвичай має низьку ціну, що робить його привабливим вибором для освітніх проектів і проектів для хобі. Однак, залежно від конкретних вимог вашого проекту, існують інші мікроконтролери, які можуть бути конкурентоспроможними за ціною або економічно ефективним варіантом.
4. Швидкість: деякі інші мікроконтролери можуть мати вищу швидкість або потужніші обчислювальні можливості порівняно з Arduino. Це може бути важливо для проектів, які вимагають значної обробки даних або виконання складного алгоритму.
5. Спільнота користувачів і підтримки: Arduino має велику спільноту користувачів, які активно допомагають один одному, діляться досвідом і надають технічну підтримку. Це важливо для початківців і людей, які шукають відповідь на запитання або вирішення проблеми.

Загалом вибір між Arduino та іншими мікроконтролерами для вашого проекту IoT залежатиме від конкретних потреб вашого проекту, вашого рівня знань і вашого бюджету.

Коли ви вибираєте найкращий мікроконтролер для своїх електронних проектів, Arduino є одним із найпопулярніших варіантів. Однак є кілька альтернатив Arduino, які можуть бути настільки ж корисними, якщо не більше. У цьому порівнянні ми розглянемо найпопулярніші варіанти та їх особливості.

- Raspberry Pi: хоч і не є мікроконтролером, Raspberry Pi є популярною альтернативою Arduino. Це одноплатний комп'ютер, який можна використовувати для різноманітних електронних проектів, від домашньої автоматизації до робототехніки. Ви можете програмувати кількома мовами, включаючи Python і C++.
- Мікроконтролер PIC: мікроконтролери PIC (Programmable Integrated Circuit) широко використовуються в електронних проектах, особливо в тих, які потребують великої кількості входів і виходів. Пристрої варіюються від недорогих до високопродуктивних і можуть програмуватися кількома мовами, включаючи C і Basic.
- Мікроконтролер STM32: мікроконтролер STM32 є ще одним популярним вибором для електронних проектів. Пристрої варіюються від недорогих до високопродуктивних і можуть програмуватися кількома мовами, включаючи C і Python.
- Мікроконтролери ESP8266 і ESP32: мікроконтролери ESP8266 і ESP32 широко використовуються в проектах Інтернету речей (IoT) завдяки їх здатності підключатися до WiFi і Bluetooth. Він недорогий і його можна програмувати кількома мовами, включаючи C++ і MicroPython.
- Мікроконтроллер AVR: мікроконтролер AVR є ще одним популярним вибором для електронних проектів. Пристрої варіюються від недорогих до високопродуктивних і можуть програмуватися кількома мовами, включаючи C і Basic.

1.3 Узагальнення аналізу концепції Інтернету речей та огляду можливостей мікроконтролерів Arduino

Після ретельного аналізу концепції Інтернету речей (IoT) та огляду можливостей мікроконтролерів Arduino для застосування в системах безпеки підприємств можна зробити кілька важливих висновків, які відображають ключові переваги та перспективи використання цих технологій.

По-перше, IoT виявляється потужним інструментом для забезпечення безпеки підприємства. Його впровадження дозволяє здійснювати віддалений моніторинг і контроль системи безпеки, швидко реагувати на небезпечні ситуації та мінімізувати ризик збитків. Це особливо актуально в сучасних умовах, коли безпека підприємств набуває все більшого значення через зростання кіберзагроз та інших потенційних ризиків.

Мікроконтролери Arduino займають центральне місце в реалізації IoT-рішень для безпеки підприємств. Вони мають ряд переваг, серед яких простота використання, гнучкість і доступність. Мікроконтролери Arduino дають можливість швидко створювати різноманітні охоронні пристрої та системи, реалізуючи різні сценарії - від датчиків руху та відкриття до систем відеоспостереження та контролю доступу.

Однією з найбільших переваг мікроконтролерів Arduino є їх активна спільнота користувачів і розробників. Ця спільнота забезпечує постійний потік нових ідей, бібліотек і розширень, що робить Arduino ще більш потужним і універсальним інструментом для розробки систем безпеки підприємств.

Таким чином, розробка IoT-рішень для систем безпеки підприємств з використанням Arduino є перспективним напрямком, який може значно підвищити рівень безпеки і знизити ризик збитків для підприємств в сучасному цифровому світі.

2. АРХІТЕКТУРА СИСТЕМИ БЕЗПЕКИ НА БАЗІ ARDUINO

Розглядаючи концепцію Інтернету речей (IoT) і можливість використання мікроконтролерів Arduino в системах безпеки, можна визначити ключові аспекти архітектури таких систем. (Рисунок 2 Архітектура Arduino)

По-перше, архітектура системи безпеки на основі Arduino зазвичай складається з набору компонентів, які включають датчики (наприклад, датчики руху та відкриття), камери відеоспостереження, сигналізацію та системи контролю доступу. Ці компоненти працюють разом, щоб виявляти потенційні загрози та реагувати на них.

Датчики відіграють ключову роль у системі та збирають інформацію про стан навколишнього середовища. Наприклад, датчики руху можуть фіксувати присутність непроханих людей і фіксувати відкриття датчиків (незаконне відкриття дверей або вікон).

Для візуального спостереження за об'єктами та реєстрації подій використовуються камери відеоспостереження. Це може допомогти вам отримати зображення потенційних загроз і визначити відповідну відповідь.

Системи сигналізації служать для сповіщення користувачів про потенційну небезпеку або вторгнення. Це може бути звукова чи світлова сигналізація, або сповіщення на мобільний пристрій відповідальної особи.

Системи контролю доступу регулюють доступ до об'єктів, наприклад, корпоративних приміщень. Ми можемо використовувати ключ-карти, біометричні дані або інші методи для ідентифікації та автентифікації користувачів.

Основними перевагами цих архітектур є складність та інтегрованість. Кожен компонент системи виконує певну роль, але разом вони забезпечують повний захист об'єкта. Крім того, використання Arduino як базової платформи дозволяє легко розширювати та оновлювати систему за потреби.

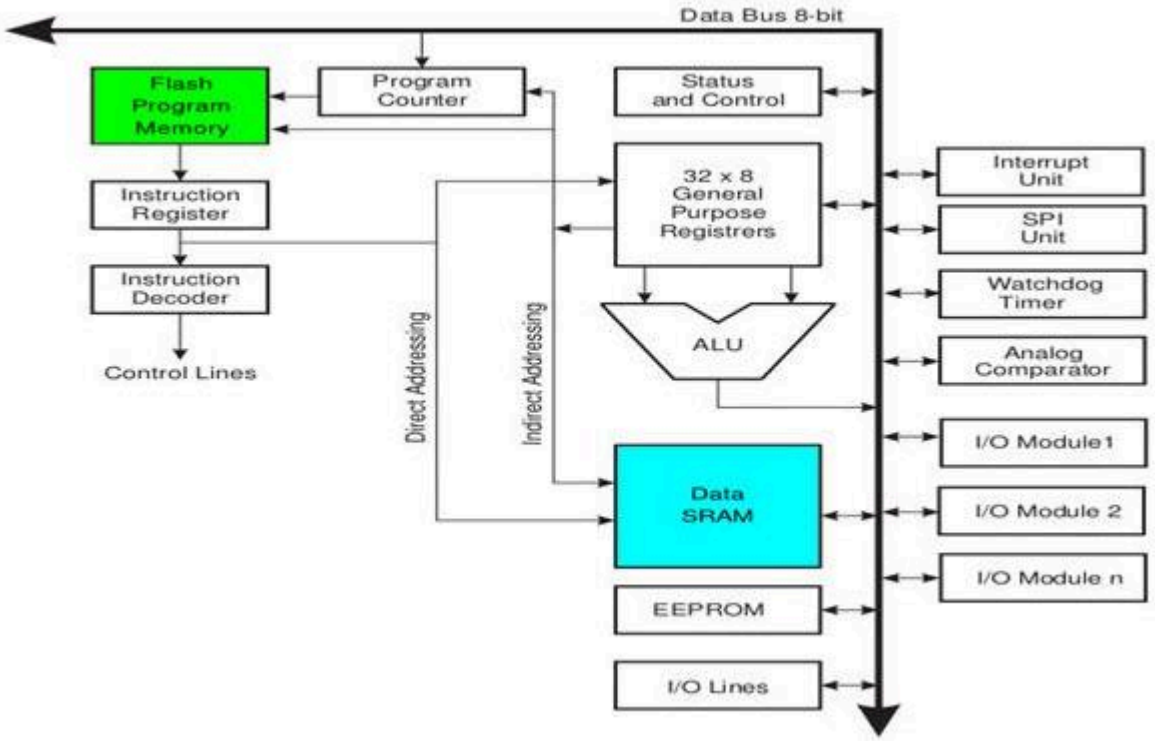

Рисунок 2 - Архітектура Arduino

2.1 Датчики руху та відкриття (сигналізація)

Датчики руху та відкриття є невід'ємною частиною корпоративних систем безпеки та є ключовими для виявлення потенційних загроз і незаконних вторгнень. Розглянемо докладніше їхню роботу та значення.

Датчик руху - це пристрій, який реагує на рух в певному просторі. Його можна використовувати для виявлення людей або інших об'єктів у межах досяжності. Ці датчики можуть мати різні форми та принципи роботи, включаючи інфрачервоні датчики (Рисунок 2.1) та ультразвукові датчики (Рисунок 2.2). Коли датчик руху спрацьовує, сигнал надходить на мікроконтролер Arduino, який обробляє його та ініціює відповідні заходи безпеки.

Рисунок 2.2 - Ультразвуковий датчик HC-SR04

Рисунок 2.1 - Датчик руху SR602

Датчики відкривання призначені для виявлення відкриття дверей (Рисунок 2.3) , вікна або іншого доступу до зони, що охороняється. Вони можуть збуджуватися іншими механізмами, які реагують на зміни або відкриття в магнітному полі. Коли відкриваються двері або вікно, датчик надсилає сигнал до мікроконтролера з підтримкою Arduino та активує відповідні заходи безпеки.

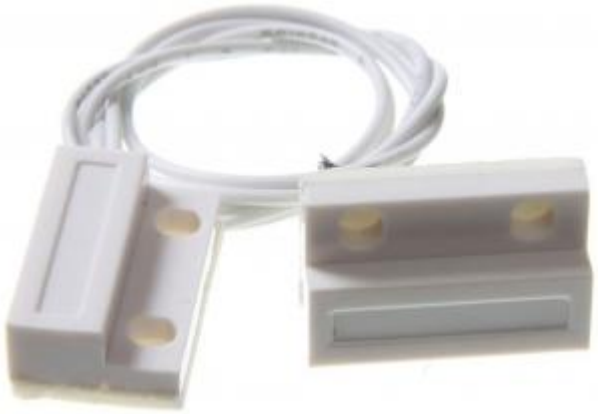

Рисунок 2.3 - Датчик відкриття дверей MC-38

Однією з ключових переваг використання датчиків руху та виявлення є те, що вони працюють у режимі реального часу та можуть швидко реагувати на події. Це

дозволяє постійно контролювати стан безпеки ваших об'єктів і негайно вживати заходів захисту, якщо це необхідно.

З огляду на все, датчики руху та відкривання є критично важливими компонентами системи безпеки на основі Arduino, які відіграють вирішальну роль у виявленні та запобіганні потенційним загрозам і небезпекам. Оперативність і надійність є незамінними факторами забезпечення безпеки об'єктів у сучасному суспільстві.

2.1.1 Розгляд принципу роботи датчиків руху та відкриття.

Розгляд принципів роботи датчиків руху та відкритих датчиків у контексті систем безпеки на основі Arduino є важливим для розуміння та встановлення правильної реакції на виявлені події. Датчики руху та відкриття використовуються для моніторингу входів та переміщень у контрольованих зонах, що дозволяє своєчасно виявляти можливі загрози та втручатися у відповідь.

Принцип роботи датчика руху полягає у виявленні змін інфрачервоного (ІЧ) випромінювання, відбитого від об’єктів у зоні спостереження. Для активації сигналів датчики використовують рух тактильних об’єктів, наприклад людей або тварин. При виявленні руху датчик генерує електричний сигнал, який може бути оброблений мікроконтролером Arduino.

Ультразвукові датчики є ще одним типом датчиків, які широко використовуються в системах безпеки, включаючи системи на основі Arduino. Вони працюють за принципом посилання ультразвукових хвиль і вимірювання часу їх відбиття від об'єктів в зоні виявлення.

Принцип роботи ультразвукових датчиків полягає в наступному:

- Посилання сигналу: датчик посилає в простір короткий звуковий сигнал у вигляді ультразвуку.
- Відбиття сигналу: сигнал відбивається від об’єктів у зоні виявлення, таких як стіни, меблі та люди.
- Отримання сигналу: датчик приймає відбитий сигнал.

- Вимірювання часу: датчик вимірює час між передачею сигналу та його отриманням після відбиття.
- Розрахунок відстані: використовуючи виміряний час і швидкість поширення звуку в навколишньому середовищі, датчик обчислює відстань до об’єкта.

Ультразвукові датчики мають ряд переваг, завдяки яким вони широко використовуються в системах безпеки.

- Висока точність: можливість вимірювання відстані з високою точністю дозволяє ефективно виявляти рух і проникнення в зону об'єктів.
- Широкий діапазон виявлення: залежно від конструкції та налаштування ультразвукові датчики можуть виявляти об’єкти на значних відстанях.
- Швидке реагування: короткий час реакції дозволяє системам безпеки швидко реагувати на виявлені події.

Ультразвукові датчики є важливим компонентом корпоративних систем безпеки на основі Arduino, оскільки вони доповнюють системи виявлення руху та відкривання, забезпечуючи додатковий моніторинг і захист будівель.

Датчики відкриття використовуються для виявлення відкриття або закриття дверей, вікон, ящиків або інших предметів. Принцип дії полягає у використанні магнітних полів для вимірювання зміни стану об’єкта (відкритий чи закритий). Коли об'єкт відкривається або закривається, його стан змінюється, і датчик генерує відповідний сигнал.

Ці два типи датчиків інтегровані в систему безпеки компанії для постійного моніторингу доступу до будівлі, руху та стану дверей і вікон. Виявлення незвичних подій дозволяє системі швидко й ефективно реагувати, сповіщаючи адміністраторів і активуючи інші заходи безпеки, які можна інтегрувати в систему на основі Arduino, що розробляється.

2.1.2 Підключення датчиків до мікроконтролера Arduino та обробка отриманих даних.

Підключення датчиків до мікроконтролера Arduino є ключовим аспектом розробки системи безпеки. Розглянемо процес підключення датчиків і обробки отриманих даних.

Підключіть датчик до мікроконтролера Arduino:

1. Вибір датчика: перед початком підключення вам потрібно вибрати відповідний датчик для конкретних потреб вашої системи безпеки. Це можуть бути датчики руху, відкриття, диму та ін.
2. Підготуйте мікроконтролер: щоб підключити датчик до Arduino, вам потрібно під’єднати датчик до контакту на мікроконтролері. Для забезпечення сумісності може знадобитися використання резисторів, адаптерів або інших електронних компонентів.
3. Підключення до входів/виходів (портів) Arduino: якщо датчик фізично підключено до мікроконтролера, його виходи мають бути підключені до певних входів або виходів (портів) Arduino. Зазвичай це робиться за допомогою проводів або роз'ємів.
4. Кодування програмного забезпечення: після фізичного підключення датчиків до Arduino вам потрібно написати програмне забезпечення для читання даних із цих датчиків. Це може включати налаштування портів введення/виведення, налаштування переривань і читання аналогових або цифрових сигналів. Щоб написати програмне забезпечення, яке зчитує дані з датчиків мікроконтролера Arduino, ви можете використовувати мову програмування C/C++ і Arduino IDE. Нижче наведено загальну структуру програми для зчитування даних із датчиків руху та відкритих датчиків. Приклад коду наведений нижче:

```
// Підключення бібліотек
#include <Arduino.h> // Основна бібліотека Arduino
#include <Wire.h>    // Бібліотека для роботи з шинами I2C (якщо потрібно)

// Оголошення пінів для підключення датчиків
const int motionSensorPin = 2;    // Пін для датчика руху
const int openSensorPin = 3;      // Пін для датчика відкриття

void setup() {
  // Ініціалізація пінів
  pinMode(motionSensorPin, INPUT);
  pinMode(openSensorPin, INPUT);

  // Ініціалізація послідовного порту для виведення результатів
  Serial.begin(9600);
}

void loop() {
  // Зчитування стану датчиків
  int motionState = digitalRead(motionSensorPin);
  int openState = digitalRead(openSensorPin);

  // Виведення стану датчиків у послідовний порт
  Serial.print("Motion Sensor: ");
  Serial.println(motionState);
  Serial.print("Open Sensor: ");
  Serial.println(openState);

  // Затримка між зчитуваннями (може бути змінена в залежності від потреб)
  delay(1000);
}
```

У цьому коді ми визначаємо два піни для підключення датчиків руху та відкриття. У функції setup() ми встановлюємо ці піни як вхідні за допомогою pinMode(), а у функції loop() ми зчитуємо стан цих пінів за допомогою digitalRead() та виводимо результат у послідовний порт. Цей код може бути дороблений для обробки даних та виконання різних дій в залежності від отриманих даних від датчиків.

Обробка отриманих даних:

- Зчитування даних: мікроконтролер Arduino зчитує сигнали з підключених датчиків. Це може бути аналоговий сигнал, цифровий сигнал або інше представлення даних.

- Аналіз даних: отримані дані можна обробити за допомогою алгоритмів для виявлення конкретних подій або умов. Наприклад, датчик руху може активувати сигнал тривоги, коли виявлено рух у певній зоні.
- Реакція на отримані дані: після аналізу мікроконтролер може виконувати певні дії в залежності від отриманих даних. Це може включати включення сигналів тривоги, реєстрацію подій, надсилання сповіщень тощо.

2.2 Камери відеоспостереження

Камери відеоспостереження, які використовуються в корпоративних системах безпеки на базі Arduino, є критично важливим елементом у забезпеченні безпеки та контролю об’єктів. Ви можете стежити за подіями в реальному часі, візуально контролювати діяльність співробітників та інших суб’єктів, а також записувати відео для подальшого аналізу. (Рисунок 2.4)

Рисунок 2.4 OV7670 камера для Arduino

Камери відеоспостереження можуть мати різноманітні характеристики, які визначають їх ефективність і функціональність. Однією з основних характеристик є роздільна здатність, яка визначає якість зображення. Вища роздільна здатність

дозволяє отримувати чіткіші та детальніші зображення, що полегшує ідентифікацію об’єктів і подій.

Деякі камери мають вбудовану функцію нічного бачення, яка дозволяє спостерігати в темряві або при слабкому освітленні. Це дуже важливо для забезпечення постійного контролю об'єкта незалежно від часу.

Ще однією важливою характеристикою камери є її кут огляду. Широкий кут огляду дозволяє охоплювати ширшу область і ефективніше контролювати.

2.2.1 Огляд типів камер та їхніх можливостей для відеоспостереження.

Огляд типів камер для відеоспостереження є важливим кроком у розробці системи безпеки на основі Arduino. Розглянемо основні види камер і їх особливості.

- Аналогова камера: традиційна камера, яка використовує аналогове з’єднання з монітором або рекордером. Зазвичай вони прості в установці та експлуатації, але мають обмежену роздільну здатність і функціональність.
- IP-камери: ці камери підключаються до мережі Ethernet або Wi-Fi і передають відео по мережі на комп’ютер або сервер. Він пропонує високу роздільну здатність, додаткові функції (наприклад, нічний режим, детектор руху) і дистанційне керування через Інтернет.
- Камера HD-SDI: ця камера забезпечує високоякісне відео з високою роздільною здатністю (від 720p до 4K) і підтримує передачу відео через коаксіальний кабель. Часто використовується в професійних системах відеоспостереження.
- Камери PTZ: ці камери можна панорамувати, нахиляти та масштабувати за допомогою пульта дистанційного керування або програмного забезпечення. Це дозволяє виявляти та відстежувати об’єкти з високою точністю та деталізацією.

Кожен із цих типів камер має свої унікальні переваги та обмеження, і вибір конкретного типу камер залежатиме від вимог вашої системи безпеки та

особливостей того, що відстежується. При розробці системи безпеки на базі Arduino важливо враховувати сумісність камер і мікроконтролерів, можливість використання додаткових модулів, засоби зберігання і обробки відеоданих.

2.2.2 Інтеграція камер в систему безпеки на базі Arduino та збереження відеоданих.

Ви можете інтегрувати камери у свою систему безпеки на базі Arduino за допомогою різноманітних модулів камер і спеціалізованих бібліотек для керування ними. Основний принцип полягає в підключенні та програмуванні камери до мікроконтролера Arduino для захоплення та зберігання відеоданих.

Нижче наведено загальну структуру програми, яка інтегрує камеру в систему безпеки на основі Arduino та зберігає відеодані.

```
// Підключення бібліотек
#include <Arduino.h>       // Основна бібліотека Arduino
#include <ESP8266WiFi.h>   // Бібліотека для роботи з Wi-Fi (якщо використовується модуль ESP8266)
#include <ESP8266WebServer.h> // Бібліотека для створення веб-сервера (якщо потрібно)
#include <Camera.h>        // Бібліотека для керування камерою

// Оголошення змінних для підключення до мережі Wi-Fi
const char* ssid = "Назва_мережі";      // SSID мережі Wi-Fi
const char* password = "Пароль_мережі";  // Пароль мережі Wi-Fi

// Оголошення об'єкту камери
Camera cam;

void setup() {
  // Підключення до мережі Wi-Fi
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(1000);
  }

  // Ініціалізація камери
  cam.begin();
}

void loop() {
  // Захоплення кадру з камери
  cam.capture();

  // Затримка між захопленнями кадрів (може бути змінена в залежності від потреб)
  delay(1000);
}
```

У цьому прикладі використовується мікроконтролер Arduino з модулем Wi-Fi ESP8266 і камерою. Після підключення до мережі Wi-Fi ініціалізуйте камеру та

знімайте кадри в нескінченному циклі loop(). Отримані відеодані можна обробляти або зберігати на віддалених серверах за допомогою протоколів передачі даних, таких як HTTP або MQTT.

У системі безпеки на базі Arduino камери відеоспостереження можуть бути підключені до мікроконтролера через різні інтерфейси, такі як USB, Ethernet або бездротові з'єднання. Мікроконтролер Arduino може керувати роботою камери, записувати та зберігати відеодані та аналізувати виявлену активність.

2.3 Система контролю доступу

Системи контролю доступу є ключовим елементом корпоративної безпеки, створеним для обмеження та контролю доступу до певних зон або будівель. Він використовується для забезпечення конфіденційності будівель, ресурсів та інформації шляхом регулювання доступу користувачів. Системи контролю доступу можуть бути реалізовані на основі різноманітних технологій і компонентів, включаючи електромагнітні замки, сенсорні карти, системи біометричної ідентифікації тощо. Це забезпечує ефективний механізм для ідентифікації та автентифікації користувачів перед наданням доступу до об'єктів. (Рисунок 2.5)

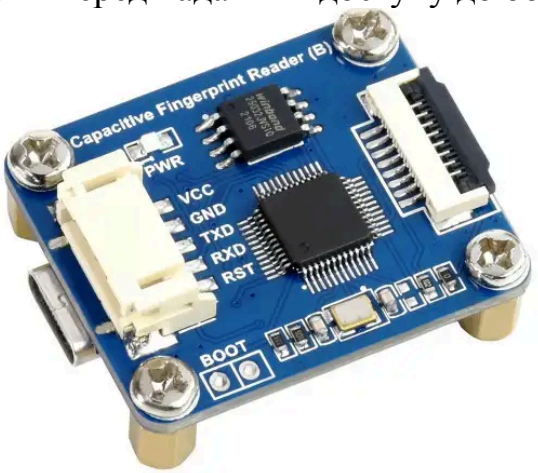

Рисунок 2.5 Ємнісний зчитувач відбитків пальців Waveshare

Однією з ключових переваг систем контролю доступу є їх гнучкість і можливість адаптації до потреб вашого бізнесу. Його можна інтегрувати з іншими системами безпеки для створення комплексних заходів безпеки. Мікроконтролери Arduino можуть відігравати центральну роль у системі, керуючи процесом автентифікації та приймаючи рішення щодо доступу на основі інформації від датчиків та інших

джерел. Це дозволяє компаніям ефективно контролювати доступ до своїх об’єктів і реагувати на потенційні загрози.

Системи контролю доступу на основі Arduino відкривають широкі можливості для реалізації різноманітних сценаріїв безпеки та контролю доступу. Він може бути адаптований до конкретних потреб і вимог підприємства, забезпечуючи високий рівень безпеки та захисту об'єктів. Системи контролю доступу на основі Arduino дозволяють підприємствам забезпечувати ефективний контроль доступу та покращувати загальну безпеку.

Системи контролю доступу бувають автономними та мережевими.

Автономна система стане оптимальним та недорогим варіантом для охорони об'єкта з однією точкою проходу. Для роботи її не потрібний комп'ютер. Тому її зручно застосовувати у віддалених складських приміщеннях. При цьому можна встановити будь-який вид зчитувача. Основна функція – обмежити доступ на територію.

2.3.1 Принцип роботи системи контролю доступу та її основні компоненти.

Системи контролю доступу є важливою складовою корпоративних систем безпеки на основі Arduino. Давайте розглянемо принцип роботи і основні його складові.

Як працює система контролю доступу:

Системи контролю доступу призначені для обмеження та контролю доступу до певних зон або будівель. Основна ідея полягає в тому, щоб дозволити або обмежити доступ до певних ресурсів або областей лише авторизованим користувачам. Зазвичай це робиться за допомогою ідентифікаційних токенів, таких як картки доступу, мітки RFID або біометричні дані.

Основні складові системи контролю доступу:

1. Система ідентифікації: ключовий компонент, який визначає, хто може отримати доступ до системи. Це можуть бути пристрої для зчитування карток, біометричні сканери (наприклад, сканери відбитків пальців або датчики розпізнавання обличчя) або системи RFID.

2. Контролер доступу: пристрій або програмне забезпечення, яке керує ідентифікацією та визначає, чи надано людині доступ. Його можна зібрати на мікроконтролері Arduino, який обробляє інформацію з системи ідентифікації та приймає рішення щодо доступу.
3. Електронні замки або замки: ці пристрої фізично контролюють доступ до кімнати чи зони. Це може бути електромагнітний замок, електромеханічний засув або інший механізм, який відкриває або закриває двері, як це визначає контролер доступу.
4. Система моніторингу та журналювання: ця система відстежує та реєструє всі спроби доступу до системи, включаючи спроби відмови. Журнали доступу можуть бути корисними для аналізу безпеки та виявлення вразливостей системи.
5. Сповіщення та сповіщення: ці компоненти використовуються для негайного сповіщення про невдалі спроби доступу або інциденти безпеки. Це може бути звукове сповіщення, сповіщення, надіслане на ваш мобільний телефон, або повідомлення, надіслане до центрального центру безпеки.

Загальний принцип системи контролю доступу полягає в ідентифікації користувача, перевірці його прав доступу та фізичному блокуванні або дозволі доступу за результатами перевірки. Це робить системи контролю доступу критично важливим компонентом будівлі.

2.3.2 Підключення та програмування електронних замків для контролю доступу через Arduino.

Підключення та програмування електронних замків контролю доступу за допомогою Arduino є важливим кроком у розвитку корпоративної системи безпеки. Цей процес вимагає ретельного розгляду та належної інтеграції з іншими компонентами системи. Ось кілька кроків, які слід виконати:

1. Вибір електронного замка: перш ніж вибрати конкретний замок, ви повинні ретельно проаналізувати свої бізнес-потреби та вимоги до системи безпеки. Важливо враховувати тип замка (електромагнітний, електромеханічний тощо), сумісність з Arduino та можливість програмування.

2. Підключіться до Arduino: після вибору блокування потрібно належним чином підключити його до мікроконтролера Arduino. Це може включати підключення проводів до контактів цифрового або аналогового порту Arduino, а також налаштування зовнішнього джерела живлення та інші необхідні параметри.

3. Програмування замка: після підключення замка до Arduino вам потрібно розробити програмне забезпечення для керування ним. Це передбачає написання коду для відкриття та закриття замку на основі сигналів, що надходять від системи контролю доступу. Після фізичного підключення електронного замка до платформи Arduino необхідно розробити програмне забезпечення для управління ним. Нижче наведено загальний приклад коду для відкриття та закриття замка з використанням мікроконтролера Arduino:

```
// Підключення виводів Arduino до електронного замка
int lockPin = 2; // Номер виводу для керування замком

void setup() {
  // Ініціалізація виводу як виводу для відкриття/закриття замка
  pinMode(lockPin, OUTPUT);
}

void loop() {
  // Перевірка умови для відкриття замка
  if (/* умова для відкриття замка */) {
    openLock(); // Виклик функції відкриття замка
  }

  // Перевірка умови для закриття замка
  if (/* умова для закриття замка */) {
    closeLock(); // Виклик функції закриття замка
  }
}
// Функція для відкриття замка
void openLock() {
  digitalWrite(lockPin, HIGH); // Подача сигналу на відкриття замка
  delay(1000); // Затримка для стабілізації
  digitalWrite(lockPin, LOW); // Вимкнення сигналу
}
// Функція для закриття замка
void closeLock() {
  // Код для закриття замка
}
```

У цьому коді контакт Arduino (у цьому випадку контакт 2) призначений для керування електронним замком. Функції openLock() і closeLock() відкривають і закривають замок відповідно.

При фактичному використанні важливо звернути увагу на встановлення умов для відкриття та закриття замку. Ці умови можуть відрізнятися залежно від датчиків, кнопок або інших компонентів системи контролю доступу. Крім того, щоб забезпечити безпеку вашого коду, вам слід уникати використання фіксованих значень і натомість використовувати змінні та умови, засновані на фактичних подіях і даних.

4. Тестування та налагодження: після написання програмного забезпечення важливо перевірити поведінку блокування. Це дозволяє виявляти проблеми та помилки, які можуть виникати в програмі, і своєчасно їх виправляти. Також

важливо забезпечити сумісність з іншими компонентами системи та належне виконання всіх функцій.

5. Впровадження та моніторинг: після успішного тестування замок можна впровадити у вашу корпоративну систему безпеки. Важливо постійно контролювати роботу замків і вчасно реагувати на проблеми або несправності.

Програмування електронних замків для контролю доступу за допомогою Arduino відкриває широкі можливості для створення ефективних і надійних систем безпеки для бізнесу. Щоб досягти оптимальних результатів, важливо враховувати всі аспекти підключення, програмування та тестування.

2.4 Аналіз архітектури системи безпеки

Аналіз архітектури системи безпеки, розробленої на Arduino, дозволяє зробити ряд важливих висновків щодо функціональності, ефективності та можливостей цієї системи.

По-перше, використання датчиків руху та відкриття як частини системи сигналізації дозволяє системі реагувати на зміни в навколишньому середовищі об’єкта. Це допоможе вам вчасно виявляти потенційні загрози безпеці та реагувати на них. Виявлення несправностей або несанкціонованих вторгнень допомагає підвищити загальну безпеку підприємства.

По-друге, камери відеоспостереження дають можливість візуального спостереження за об'єктами в реальному часі. Він не тільки фіксує інциденти, але й служить важливим засобом аналізу ситуацій і визначення відповідних реакцій на них. Це також забезпечує збереження доказів для подальшого використання в розслідуванні інциденту.

По-третє, системи контролю доступу регулюють і обмежують доступ до певних зон об’єкта лише авторизованим користувачам. Це забезпечує максимальний рівень

безпеки та конфіденційності, запобігаючи несанкціонованому доступу до ваших об'єктів.

Загалом архітектура системи безпеки на основі Arduino відображає сучасний підхід до безпеки підприємства. Інтеграція різних компонентів і технологій створює комплексний і ефективний механізм моніторингу і захисту, який відповідає останнім вимогам безпеки. Такий підхід може бути успішно використаний у багатьох різних сферах промисловості та бізнесу та сприяє підвищенню загального рівня безпеки та захисту об’єктів.

3. РОЗРОБКА ТА РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ НА ARDUINO

Розробка та впровадження захищеної системи на Arduino вимагає кількох ключових кроків, від вибору компонентів до програмування мікроконтролера та тестування прототипу. Нижче наведено огляд кожного кроку.

1. Вибір комплектуючих та обладнання:

- Визначте вимоги до системи безпеки: проаналізуйте потреби та вимоги клієнтів.
- Вибір датчика: виберіть відповідні датчики руху та відкриття, які відповідають вимогам системи.
- Вибір камери: Виберіть камери відеоспостереження на основі роздільної здатності, кута огляду та інших параметрів.
- Виберіть модуль зв’язку: виберіть модуль Wi-Fi, Bluetooth або Ethernet для мережевого зв’язку.

2. Програмування мікроконтролерів Arduino:

- Напишіть програмне забезпечення для читання даних із датчиків: запрограмуйте Arduino на обробку сигналів від датчиків руху та відкритих датчиків.
- Розробка алгоритмів реагування: визначення умов та алгоритмів спрацювання систем сигналізації та відеоспостереження.
- Реалізація надсилання повідомлень: запрограмуйте мікроконтролер на надсилання повідомлень адміністраторам у разі збою системи безпеки.

3. Складання та тестування прототипів системи:

Проектування та впровадження систеси безпеки на Arduino — це складний і багатогранний процес, який вимагає глибоких знань електроніки, програмування та

систем безпеки. На відміну від традиційних програмних додатків, розробка систем безпеки на основі мікроконтролерів вимагає не лише уваги до фізичних аспектів взаємодії апаратного забезпечення, а й адаптації програмного забезпечення до конкретних вимог безпеки та надійності.

Вибір комплектуючих і обладнання є важливим кроком у розвитку, адже від цього залежить якість і надійність системи. Правильний підбір датчиків, камер відеоспостереження та модулів зв'язку дозволяє створити систему, яка ефективно відповідає потребам підприємств у сфері безпеки.

Програмування мікроконтролерів Arduino передбачає розробку складних алгоритмів реагування на події, обробки отриманих даних і взаємодії з іншими пристроями. Глибокі знання програмування та електроніки необхідні для ефективної розробки програмного забезпечення та налагодження.

Складання та тестування прототипу системи є критично важливим кроком у розробці, оскільки від цього залежить функціональність і надійність системи. Тестування дозволяє виявити потенційні проблеми та помилки у вашій системі та вчасно їх виправити.

Аналіз результатів тестування та порівняння з існуючими системами безпеки дає можливість оцінити ефективність розробленої системи та виявити можливості для подальшого вдосконалення. Тільки шляхом постійного вдосконалення та аналізу можна досягти високої якості та ефективності системи безпеки Arduino.

3.1 Вибір компонентів та обладнання

Вибір компонентів і обладнання для реалізації системи безпеки на базі Arduino вимагає ретельного аналізу функціональних вимог, технічних характеристик компонентів, сумісності та ефективності. Деякі ключові аспекти вибору компонентів і обладнання включають:

1. Датчики руху та відкривання: різноманітні датчики, такі як інфрачервоні (PIR), ультразвукові, тощо, можна використовувати для виявлення руху та відкриття дверей або вікна. При виборі датчика слід враховувати радіус дії, точність,

надійність і вартість.

2. Камери відеоспостереження: Для реалізації системи відеоспостереження можна використовувати USB або IP камери з різними характеристиками за якістю зображення, роздільною здатністю, швидкістю передачі даних і функціональністю.

3. Електронні замки та системи контролю доступу: Доступ до вашої будівлі можна контролювати за допомогою різних типів електронних замків, включаючи електронні замки, електромеханічні замки та електронні замки з сенсорними панелями. Користувачів також можна ідентифікувати за допомогою RFID-карт, біометричних відбитків пальців або сканерів обличчя.

4. Мікроконтролер Arduino та додаткові модулі: для централізованого керування системою безпеки платформу Arduino можна використовувати з різними модулями та додатковим обладнанням, таким як Ethernet або Wi-Fi shield для підключення до Інтернету, РК-екран для відображення інформації та реле для управління. Електричні пристрої та ін.

Під час вибору компонентів слід також враховувати інтегрованість, сумісність і простоту програмування. Важливо спланувати заздалегідь і провести тестування, щоб забезпечити оптимальну продуктивність і безпеку системи.

3.1.1 Аналіз доступних датчиків, камер та інших компонентів для системи безпеки.

Аналіз доступних датчиків, камер та інших компонентів системи безпеки є ключовим кроком у виборі оптимального рішення для розробки та впровадження системи безпеки на основі Arduino. Нижче ми розглянемо кілька аспектів цього аналізу.

1. Вибір датчиків руху та відкривання: під час аналізу необхідно враховувати такі параметри, як діапазон зчитування, кут застосування, точність і чутливість датчика. Для ефективної системи безпеки може знадобитися комбінація різних типів датчиків, наприклад інфрачервоних (PIR), ультразвукових або магнітних.

- Якщо ви плануєте встановлювати виріб на вулиці, вибирайте датчики з високим ступенем захисту (IP 54, IP 55, IP 65). Якщо датчик розташований під навісом, достатньо мати ступінь IP 44.
- IP20 підходить, якщо пристрій встановлено в закритому приміщенні з низькою вологістю, але модель може бути пошкоджена, якщо в неї потрапить пісок або інші сторонні речовини. Датчики IP40 захищені від сторонніх предметів, але не від вологи.
- IP41 гарантує, що продуктивність не погіршується під впливом вологи. Він також не боїться конденсату. Датчик захищений від бризок води і встановлюється в місцях з підвищеною вологістю.
- Роблячи вибір, слід враховувати максимальну потужність, яку перетворює продукт. В одних випадках вмикаються люмінесцентні лампи або малопотужні світлодіодні прожектори, а в інших випадках вмикається освітлення великих будівель, наприклад виробничих цехів.
- Перед покупкою перевірте потужність свого освітлювального обладнання, щоб легко вибрати потрібну модель. Максимальний діапазон потужності виробу становить 60~2200 Вт.
- При виборі враховуйте, що інфрачервоні сповіщувачі вловлюють тепло, тому будь-які перешкоди завадять їм працювати. Звичайне скло не пропускає ІЧ-випромінювання, не кажучи вже про інші конструкції, які можуть створювати стійкі мертві зони.
- Тому інколи доводиться встановлювати два або більше сповіщувачів одночасно, розміщених у різних ділянках зони спостереження.

2. Огляд різних типів камер відеоспостереження: під час аналізу рекомендується

оцінювати різні характеристики камер, такі як роздільна здатність, кут огляду, можливості нічного бачення, вбудовану відеоаналітику та збереження відеоданих.(Рисунок 3 - Кути огляду)

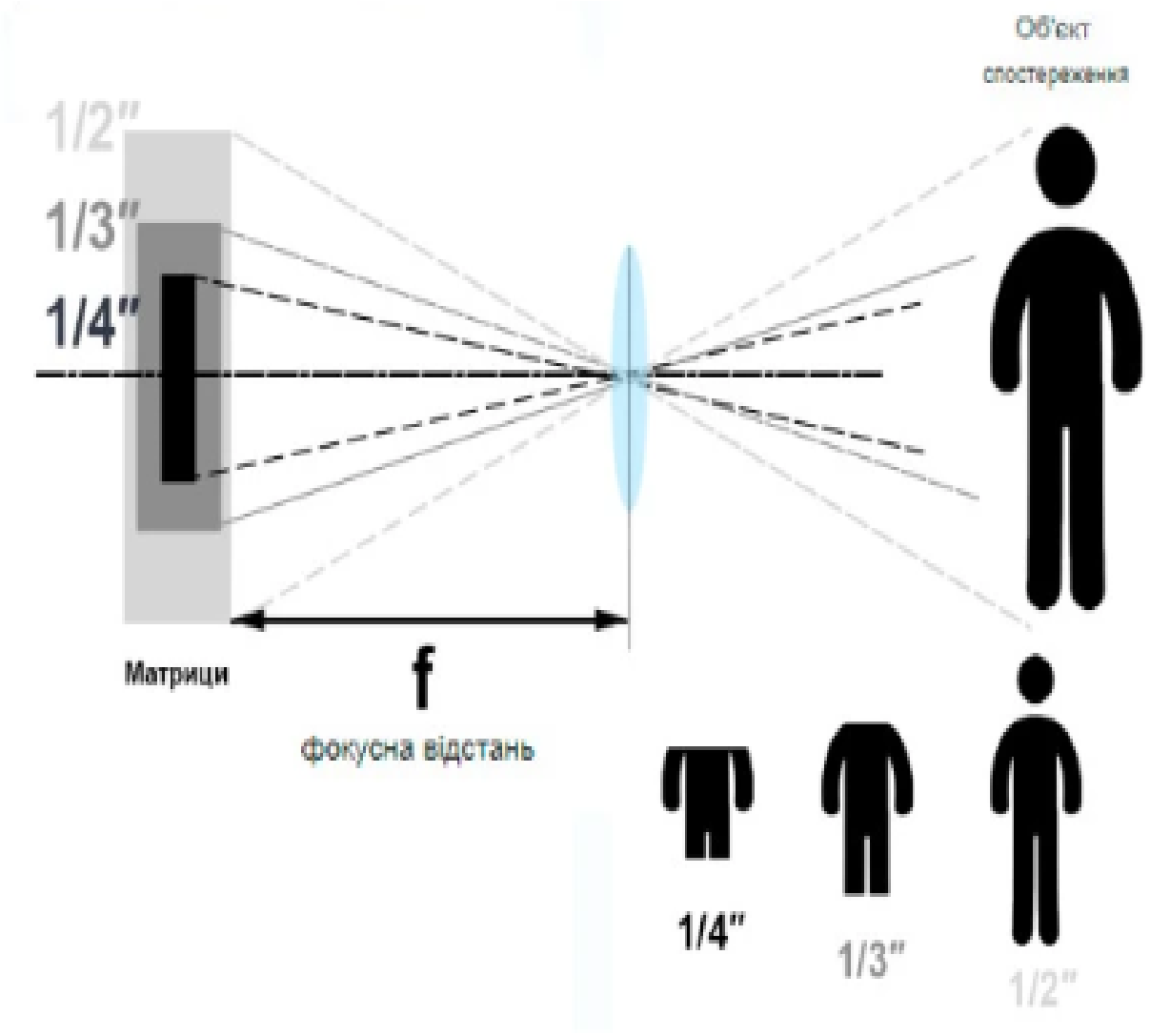

Рисунок 3 - Кути огляду

3. Вибір системи контролю доступу: під час аналізу слід розглянути різні типи систем контролю доступу, такі як зчитувачі RFID, біометричні системи, електронні замки тощо. Важливо враховувати параметри надійності, швидкості реакції та зручності використання. (Рисунок 3.1 - Принципова схема контролю доступу RFID)

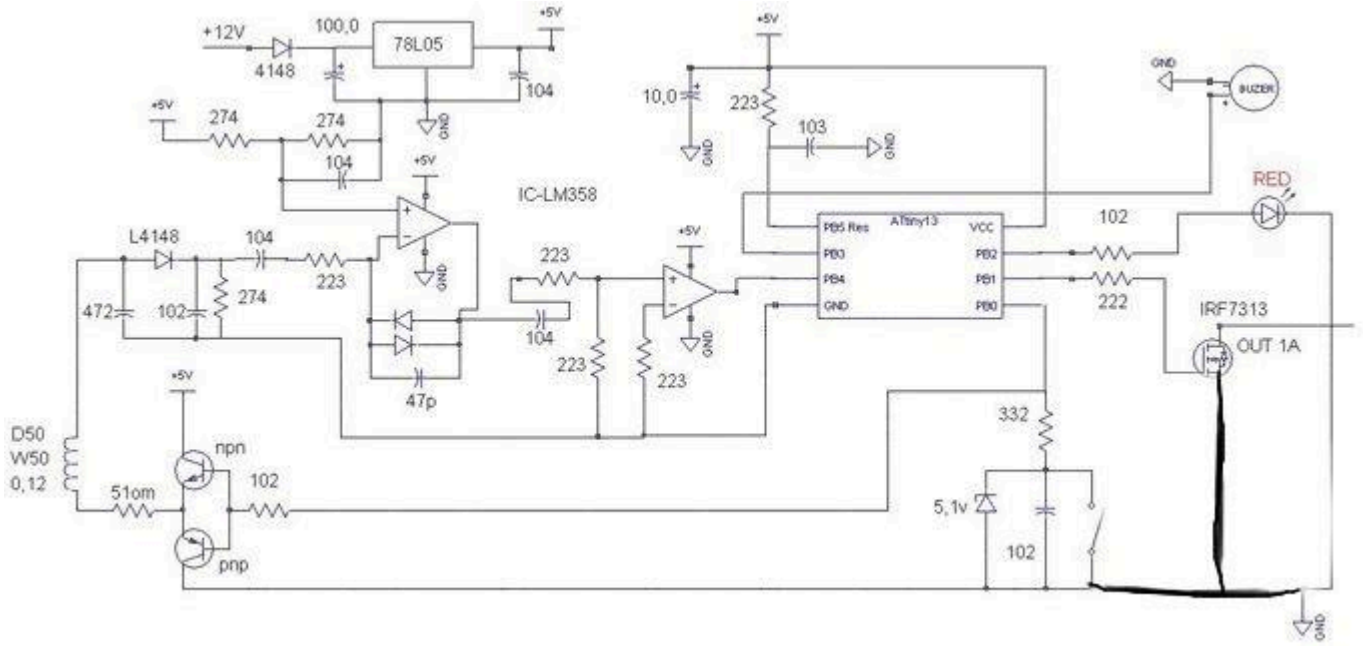

Рисунок 3.1 - Принципова схема контролю доступу RFID

4. Аналіз функціональних можливостей мікроконтролера Arduino і додаткових модулів: При виборі компонентів також слід враховувати їх сумісність з мікроконтролером Arduino і можливість розширення його функціональних можливостей за допомогою додаткових модулів, таких як Ethernet або Wi-Fi екрани, LCD екрани. Реле та ін.(Рисунок 3.2 Arduino-сумісні Bluetooth-модулі)

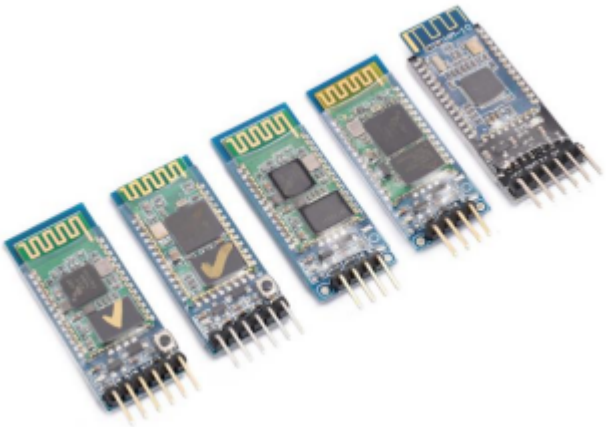

Рисунок 3.2 - Arduino-сумісні Bluetooth-модулі

Враховуючи вищезазначені аспекти, аналіз допоможе вам вибрати оптимальні компоненти для розробки системи безпеки, яка відповідає потребам і вимогам конкретного підприємства.

3.1.2 Вибір оптимальних обладнання та компонентів з урахуванням вимог та можливостей.

Для розробки системи безпеки підприємства на базі Arduino, враховуючи вимоги для підприємства, можна обрати наступні компоненти:

1. Датчики руху та відкриття:

- Пара датчиків руху HC-SR501 (Рисунок 3.3) , які мають високу чутливість та дальність дії.
- Магнітний датчик відкриття для дверей або вікон (Рисунок 3.4).

Рисунок 3.3 - Датчик руху HC-SR501

Рисунок 3.4 - Датчик відкриття дверей MC-38

2. Камери відеоспостереження:

- Камера з високою роздільною здатністю та швидким часом реакції - модель Arducam 64-мегапіксельна камера з надвисокою роздільною здатністю і автофокусом. (Рисунок 3.5)
- IP-камера з можливістю стрімінгу в реальному часі - IP камера Hikvision DS-2CD1321-I . (Рисунок 3.6)

Рисунок 3.5 - Arducam 64-мп, автофокус

Рисунок 3.6 - IP камера Hikvision

3. Система контролю доступу:

- Електронний замок з підтримкою RFID-карт або кодового замку SEVEN LOCK SL-7737S silver ID EM (Рисунок 3.7)
- RFID-читач для ідентифікації користувачів. RC-522 RFID-зчитувач (Рисунок 3.8)

Рисунок 3.7 - електронний замок SEVEN LOCK SL-7737S

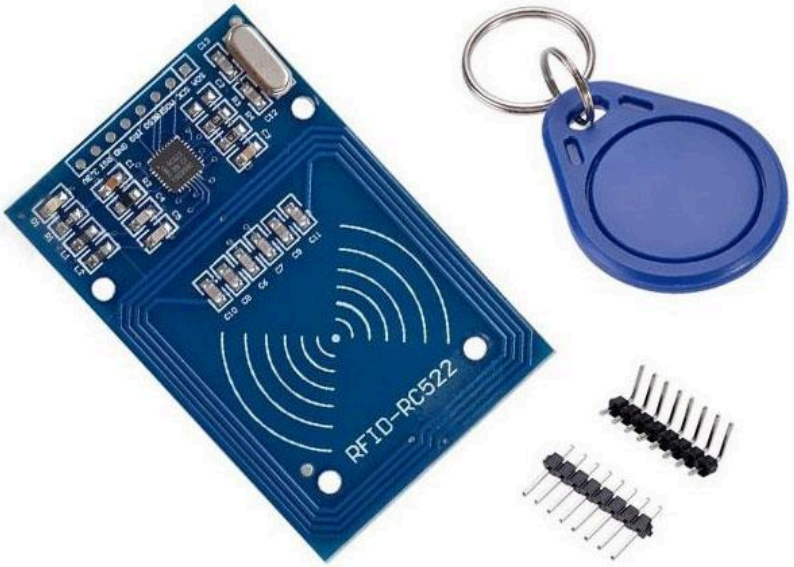

Рисунок 3.8 - RFID-зчитувач RC-522

4. Мікроконтролер Arduino:

- Arduino Mega, підходить для нашого обсягу, оброблювання даних та кількості

підключених пристроїв. (Рисунок 3.9)

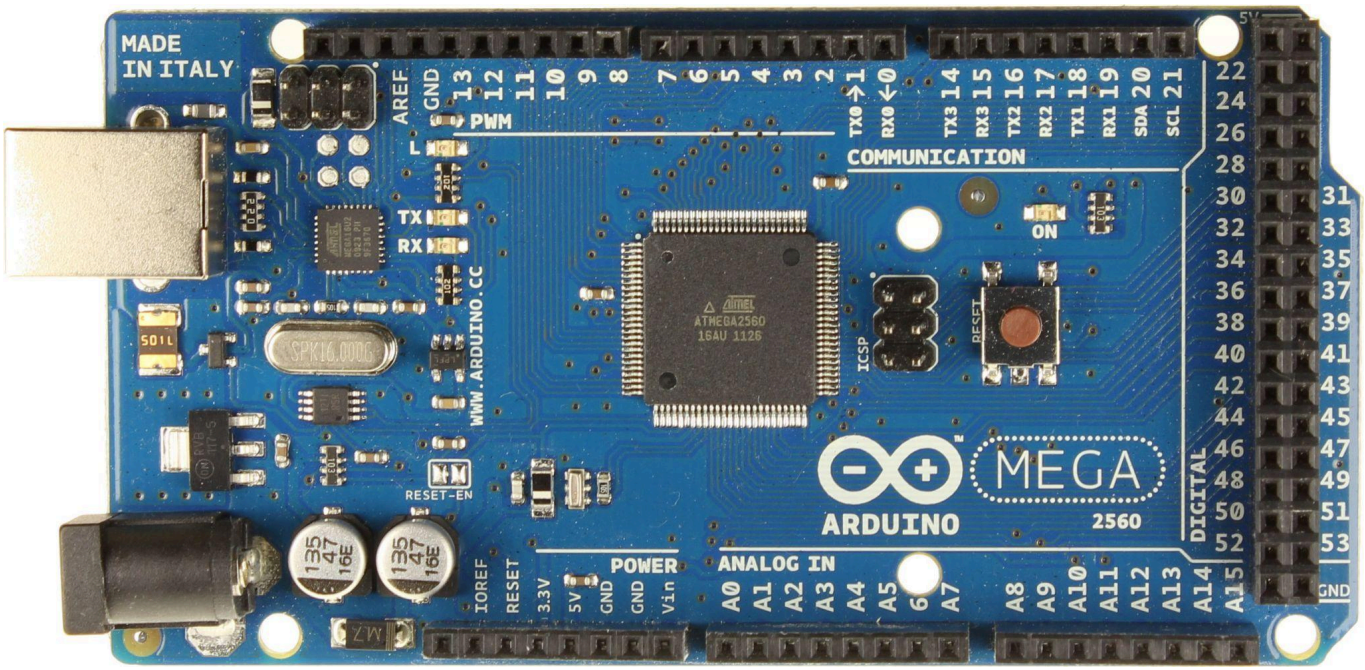

Рисунок 3.9 - Arduino Mega

5. Додаткові компоненти:

- Реле для керування замком та іншими пристроями. Кероване реле ITV U-Prox Relay AC (Рисунок 3.10)
- LCD-дисплей для відображення інформації про стан системи та подій.Дисплей LCD символьний 8x2 (YM0802A-1-Good Display) (Рисунок 3.11)

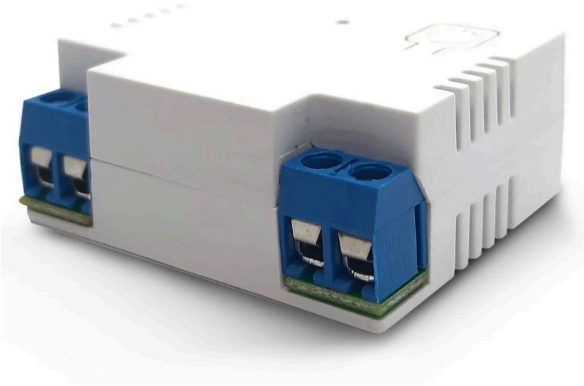

Рисунок 3.10 - Кероване реле

Рисунок 3.11 - Дисплей LCD символьний

Після вибору компонентів можна розпочати розробку програмного забезпечення для Arduino, яке буде відповідати за зчитування даних з датчиків, керування камерами та системою контролю доступу. Нижче наведено загальну структуру програми:

1. Ініціалізація:

- Налаштування портів вводу/виводу та підключення всіх компонентів. (Рисунок 3.12 - приклад коду для ініціалізації)

```
// Підключення бібліотек
#include <Arduino.h>

// Підключення датчиків та компонентів
int motionSensorPin = 2; // Пін для датчика руху
int doorSensorPin = 3;    // Пін для датчика відкриття дверей або вікон

void setup() {
  // Ініціалізація портів вводу/виводу
  pinMode(motionSensorPin, INPUT);
  pinMode(doorSensorPin, INPUT);

  // Ініціалізація LCD-дисплея, якщо використовується
}

void loop() {
  // Основний цикл програми
  // Додайте код для зчитування даних, взаємодії з компонентами та відображення інформації
}
```

2. Зчитування даних:

- Виявлення руху за допомогою датчиків.
- Виявлення відкриття дверей або вікон. (Рисунок 3.13 - приклад коду для зчитування даних)

```
// Виявлення руху за допомогою датчиків
bool detectMotion() {
  return digitalRead(motionSensorPin) == HIGH;
}

// Виявлення відкриття дверей або вікон
bool detectDoorOpen() {
  return digitalRead(doorSensorPin) == HIGH;
}

void loop() {
  // Основний цикл програми
  bool motionDetected = detectMotion();
  bool doorOpened = detectDoorOpen();
  // Додайте код для обробки отриманих даних
}
```

3. Взаємодія з камерами:

- Активація камер та запис відео при виявленні подій. (Рисунок 3.14 - приклад коду для камер)

```
// Активація камер та запис відео
void activateCameras() {
  // Додайте код для активації камер та запису відео
}

void loop() {
  // Основний цикл програми
  if (motionDetected || doorOpened) {
    activateCameras();
  }
  // Додайте код для інших дій з камерами
}
```

4. Система контролю доступу:

- Ідентифікація користувачів за допомогою RFID-карт або кодів доступу.
- Керування реле для відкриття замків. (Рисунок 3.15 - приклад коду для систему контролю доступу)

```
// Ідентифікація користувачів за допомогою RFID-карт або кодів доступу
bool identifyUser() {
  // Додайте код для ідентифікації користувачів
}

// Керування реле для відкриття замків
void controlLocks() {
  // Додайте код для керування реле та відкриття замків
}

void loop() {
  // Основний цикл програми
  if (identifyUser()) {
    controlLocks();
  }
  // Додайте код для інших дій з контролем доступу
}
```

5. Відображення інформації:

- Відображення стану системи на LCD-дисплеї. (Рисунок 3.16 - приклад коду для відображення інформації)

```
// Відображення стану системи на LCD-дисплеї
void displayStatus() {
  // Додайте код для відображення інформації на LCD-дисплеї
}

void loop() {
  // Основний цикл програми
  displayStatus();
  // Додайте код для інших дій з відображенням інформації
}
```

Після написання програмного забезпечення необхідно протестувати систему та виконати її встановлення на об'єкті.

3.2 Програмування мікроконтролера Arduino

Програмування мікроконтролерів Arduino можна виконати за допомогою Arduino Integrated Development Environment (IDE), середовища розробки з відкритим кодом, розробленого спеціально для Arduino. Ось кроки, які слід виконати, щоб запрограмувати мікроконтролер Arduino:

1. Встановіть Arduino IDE:

- Завантажте та встановіть Arduino IDE з офіційного веб-сайту Arduino.
- Після встановлення запустіть Arduino IDE.

2. Виберіть свою платформу:

- У меню «Інструменти» виберіть потрібну платформу Arduino (наприклад, «Arduino Uno» або «Arduino Mega»).

3. Програмування:

- Пишіть програми на C/C++ за допомогою інтегрованого середовища Arduino.
- Розробіть програму, яка відповідає вимогам вашої системи безпеки. Це може включати код, який зчитує дані з датчиків, керує приводами, обробляє вхідні сигнали, взаємодіє з камерами тощо.

4. Завантажте програму:

- Підключіть мікроконтролер Arduino до комп’ютера за допомогою кабелю USB.
- Виберіть потрібний COM-порт у меню «Інструменти».
- Натисніть кнопку «Завантажити», щоб завантажити програму на мікроконтролер Arduino.

5. Налагодження:

- Використовуйте монітор послідовного порту Arduino IDE, щоб налагодити програму та перевірити результат.
- Використовуйте інструменти налагодження, такі як налагодження та журналювання, щоб виявити та виправити помилки.

6. Оптимізації та покращення:

- Оптимізуйте свої програми, щоб зменшити використання ресурсів мікроконтролера та підвищити продуктивність.
- Ми додаємо нові функції та вдосконалення, щоб забезпечити більшу функціональність і стабільність вашої системи безпеки.

Після виконання цих кроків ви можете розробити та завантажити програмне забезпечення мікроконтролера Arduino, яке виконує функції вашої системи безпеки. Не забувайте регулярно оновлювати та тестувати програмне забезпечення, щоб переконатися, що воно працює належним чином.

3.2.1 Розробка програмного забезпечення для Arduino на мові програмування C/C++.

Розробка програмного забезпечення Arduino на мовах програмування C/C++ передбачає написання програм, які керують поведінкою мікроконтролера та його взаємодією з підключеними пристроями. Основні кроки та методи розробки програмного забезпечення Arduino на C/C++ такі:

1. Створіть програмний файл:

- Відкрийте Arduino IDE і створіть новий програмний файл.
- Файл повинен мати розширення ".ino", щоб вказати, що він належить до проекту Arduino.

2. Структура програми:

- Кожна програма Arduino складається з функцій setup() і loop().
- Функція setup() запускається один раз під час запуску мікроконтролера та використовується для встановлення початкових параметрів.
- Функція loop() виконується безперервно після функції setup() і використовується для основних операцій програми.

3. Підключення до бібліотеки:

- Розширте функціональність програми за допомогою вбудованих і сторонніх бібліотек.
- Додайте бібліотеки за допомогою директиви #include.

4. Операції введення/виведення:

- Використовуйте функції Arduino для взаємодії з цифровими та аналоговими контактами мікроконтролера.
- Встановіть значення PIN-коду за допомогою функцій digitalWrite() і AnalogWrite().

5. Робота датчика та пристрою:

- Використовуйте функції Arduino для читання даних із датчиків, наприклад функцію AnalogRead() для аналогових датчиків.
- Налаштовуйте підключені пристрої та керуйте ними за допомогою відповідних команд і бібліотек.

6. Логіка програми:

- Використовуйте умовні оператори, цикли та функції для реалізації логіки вашої програми.
- Врахуйте вимоги вашого проекту та зробіть необхідні розрахунки та дії.

7. Налагодження та тестування:

- Налагодьте свою програму та перевірте результат за допомогою вбудованого монітора послідовного порту.

- Тестуйте різні сценарії та умови роботи вашої програми, щоб переконатися, що вона працює правильно.

Ці кроки допоможуть вам розробити програмне забезпечення Arduino на мовах програмування C/C++, яке відповідатиме вимогам вашого проекту та гарантуватиме його надійну та ефективну роботу.

3.2.2 Опис алгоритмів та методів програмування для забезпечення роботи системи безпеки

Опис алгоритмів і методів програмування для забезпечення роботи систем безпеки на мікроконтролерах Arduino включає розробку програмного забезпечення, яке забезпечує ефективну роботу всіх компонентів системи та забезпечує безпеку об'єктів.

1. Алгоритм обробки сигналу датчика:

- Визначення порогу спрацьовування сигналу датчика.
- Налаштуйте правила для аналізу даних від датчиків, щоб виявити рух або отвори.

2. Алгоритм управління камерою спостереження:

- Визначає час і тривалість відеозапису після виявлення події.
- Періодично вмикайте та вимикайте камеру, щоб заощадити енергію.

3. Алгоритм ідентифікації користувача:

- Ми використовуємо коди доступу або інформацію з карт RFID для зберігання та керування базами даних користувачів.
- Переконайтеся, що введений код доступу відповідає тому, що зберігається в базі даних.

4. Алгоритм керування блокуванням:

- Встановити режим роботи (відкрито/закрито) замка.
- Перед відкриттям замка перевірте права доступу користувача.

5. Алгоритм виведення інформації на РК-дисплей:

- Створіть меню, яке відображає стан системи та доступні параметри.
- Реалізуйте ефекти переходу та механізми анімації для зручності використання.

6. Алгоритм роботи в аварійному режимі:

- При виявленні загрози безпеці він автоматично активує всі компоненти системи та надсилає сигнал тривоги.
- Запровадити додаткові заходи безпеки та повідомити служби безпеки у разі надзвичайної ситуації.

Ці алгоритми є ключовими для розробки програмного забезпечення системи безпеки на мікроконтролерах Arduino та забезпечення їх ефективної та надійної роботи. Детальна реалізація кожного алгоритму включає програмування коду та налагодження для забезпечення високої якості та стабільності роботи системи.

3.3 Збірка та тестування прототипу системи

Після вибору компонентів для системи безпеки на базі Arduino переходимо до складання та тестування прототипу системи. Нижче наведено детальний опис кожного компонента та процесу складання.

1. Датчики руху та відкриття:

- Підключіть пару датчиків руху HC-SR501 до вхідного порту Arduino. Датчик

має два основних виходи: VCC (живлення) і OUT (вихідний сигнал). OUT підключається до цифрового входу на Arduino.

- Підключіть магнітний датчик відкриття MC-38. Цей датчик також має два виходи. Один підключається до входу Arduino, а інший – до GND або VCC залежно від конфігурації.

2. Камери відеоспостереження:

- Підключіть камеру Arducam 64MP та IP-камеру Hikvision DS-2CD1321-I до мережі відповідно до їхнього вводу/виводу або інтерфейсу Arduino.

3. Система контролю доступу:

- Підключіть електронний замок SEVEN LOCK SL-7737S до ITV U-Prox Relay AC, а потім підключіть реле до Arduino для керування.
- Підключіть зчитувач RFID RC-522 для ідентифікації користувача через порт введення/виведення Arduino.

4. Мікроконтролер Arduino:

- Встановіть мікроконтролер Arduino Mega на плату прототипу та підключіть усі компоненти до відповідних входів/виходів.

5. Додаткові компоненти:

- Підключіть кероване реле ITV U-Prox Relay AC для управління електронними замками та іншими пристроями.
- Підключення символьного РК-дисплея YM0802A-1-Good Цей дисплей відображає інформацію про стан системи та події.

Після складання всіх компонентів ми починаємо тестування прототипу системи.

Переконайтеся, що кожен компонент працює належним чином і взаємодіє з Arduino. Звичайно, ми також проведемо тести для перевірки функціональності системи безпеки на основі Arduino.

1. Тести датчиків руху та відкритих датчиків:

- Імітація руху перед датчиком руху та перевірка реакції системи на зміни стану датчика. (Рисунок 3.17 - Схема роботи датчику руху)

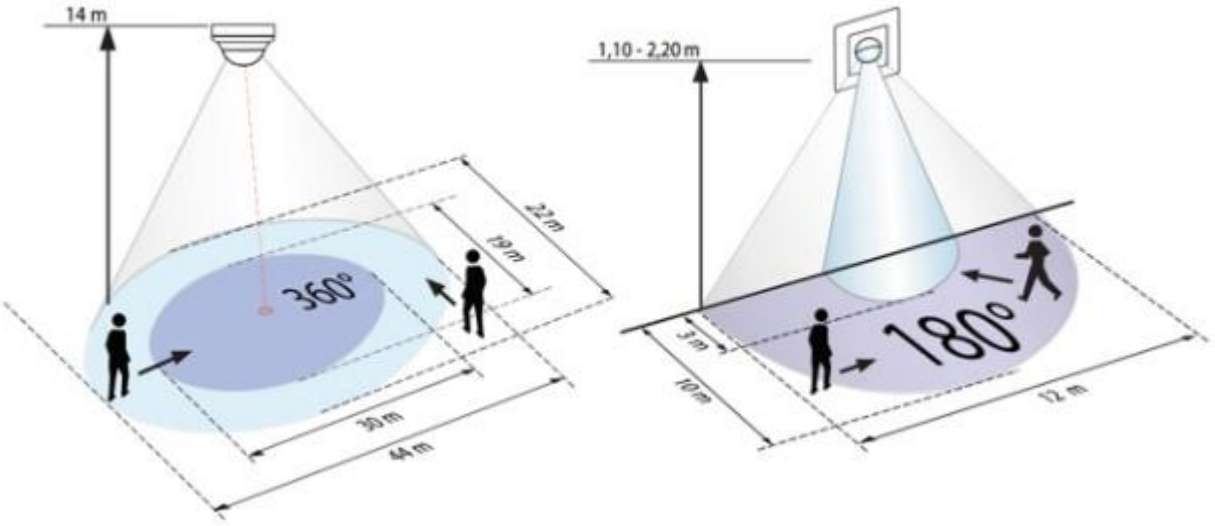

Рисунок 3.17 - Схема роботи датчику руху

- Відкрийте та закрийте двері/вікна та перевірте реакцію системи на зміну стану магнітного датчика.

2. Тестування камери відеоспостереження:

- Перевірте камеру, записавши та відтворивши відео, щоб переконатися, що камера працює правильно під час виявлення події.
- Перевірте доступність прямої трансляції та підключення до мережі з IP-камер. (Рисунок 3.18 - Розроблений додаток для прямих трансляцій з відеокамер)

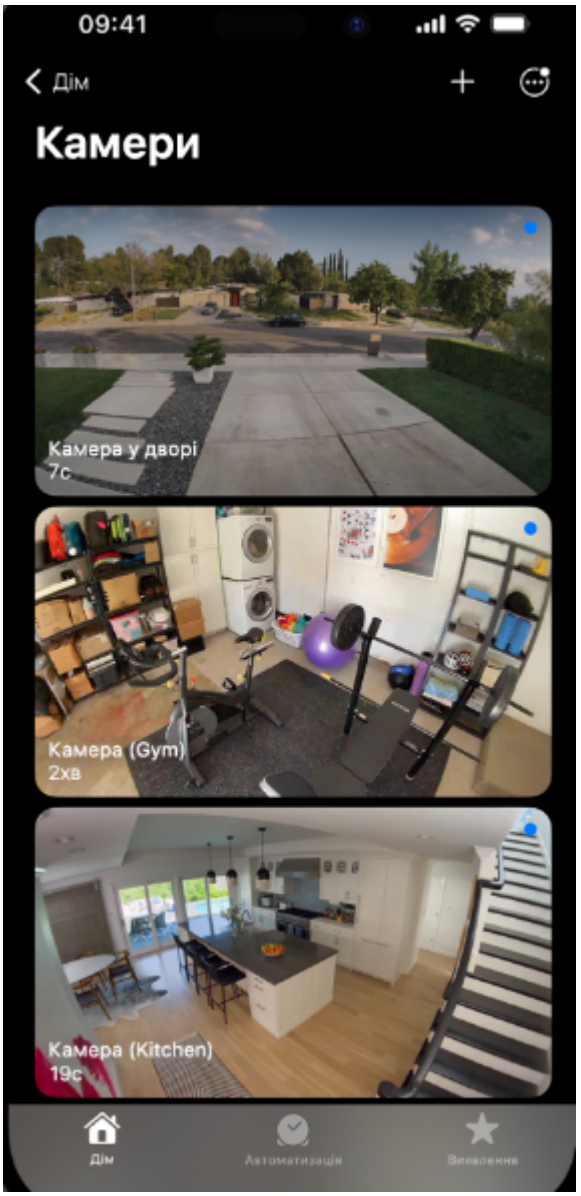

Рисунок 3.18 - Розроблений додаток для прямих трансляцій з відеокамер

3. Тестування системи контролю доступу:

- Зчитувач RFID використовується для перевірки, чи зчитується RFID-карта, та для ідентифікації користувача.
- Перевірте точність відповіді системи на правильну картку RFID або код доступу.

4. Тестування мікроконтролера Arduino:

- Перевірте роботу всіх вхідних і вихідних портів Arduino. (Рисунок 3.19 - Схема підключень Arduino)
- Перевірка зберігання та передачі даних між компонентами системи.

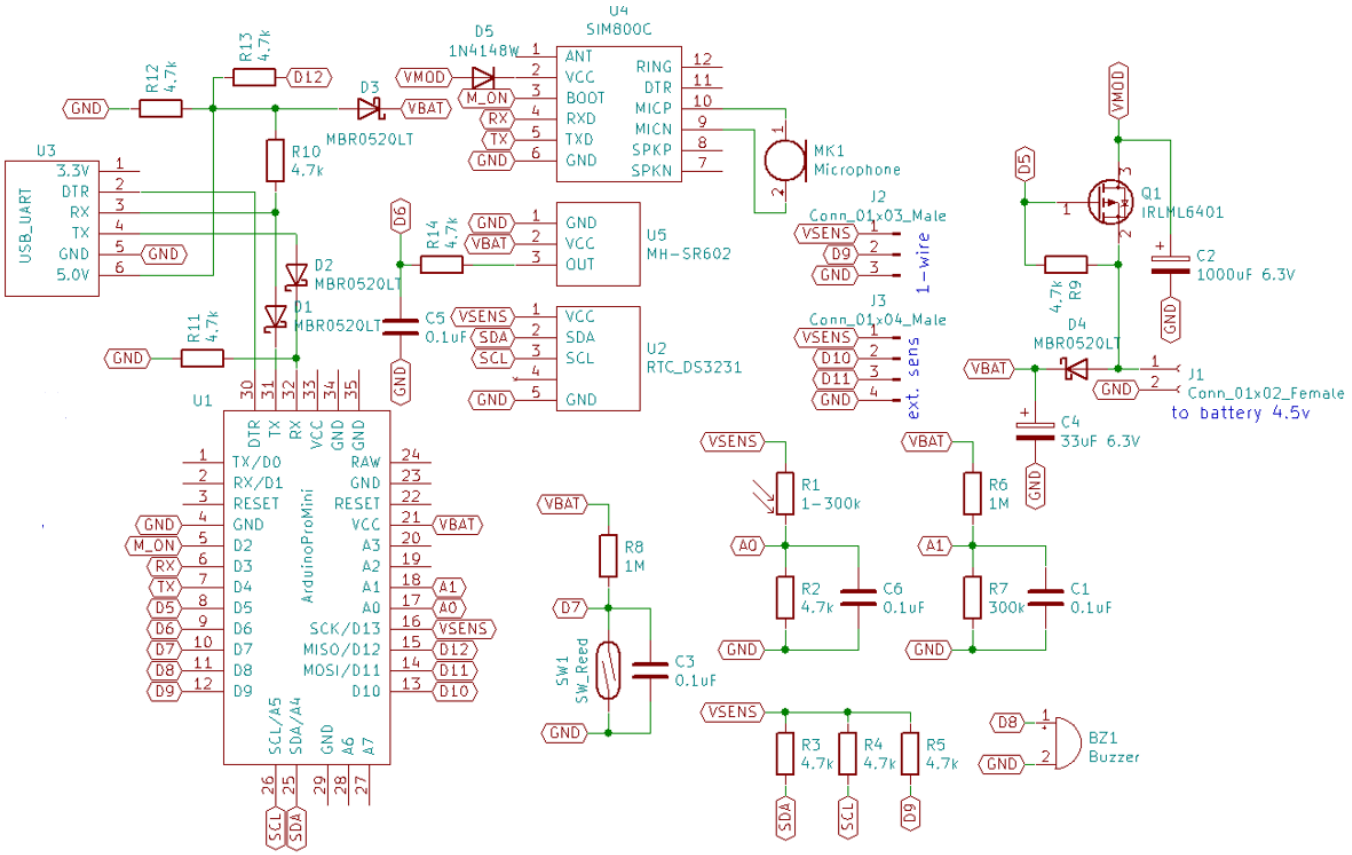

Рисунок 3.19 - Схема підключень Arduino

5. Додаткові тести компонентів:

- Перевіряє роботу реле керування замками та іншими пристроями.
- Перевірте відображення інформації на символьному РК-дисплеї. (Рисунок 3.20 - Відображення інформації на символьному РК-дисплеї)

Рисунок 3.20 - Відображення інформації на символьному РК-дисплеї

Під час тестування ми будемо звертати увагу на правильну реакцію системи на події та виявлення аномалій чи проблем. У разі виявлення проблеми ми вносимо відповідні корективи у ваше програмне та апаратне забезпечення, щоб забезпечити оптимальну роботу вашої системи безпеки.

3.4 Аналіз результатів тестування

Тестування проводиться за допомогою вбудованих засобів. Середовище розробки Arduino IDE. Це було для перевірки роботи системи. Для відображення інформації в серійному форматі розроблені спеціальні скетчі.

1. Перевірка роботи системи при виявленні руху. (Рисунок 3.21 - Результат тестування датчику руху)

```
14:11:48.601 -> Alarm is activated
14:12:03.321 -> Motoin detected
14:12:13.340 -> AT+CMGS="+380983649285"
14:12:14.372 ->
14:12:14.372 -> >
14:12:14.372 -> Motion detected! Alarm had been activated!
14:12:14.419 -> □
```

Motion detected! Alarm had been activated!

Рисунок 3.21 - Результат тестування датчику руху

Як ви можете бачити на малюнку. 3.21 поставляється з системою виявлення руху протягом 10 секунд.

2. Перевірка роботи команди Turn off. (Рисунок 3.22 - Результат тестування команди Turn off)

```
14:14:47.398 -> +CMTI: "SM",1
14:14:47.398 -> AT+CMGR=1
14:14:48.519 ->
14:14:48.519 -> +CMGR: "REC UNREAD","+380983649285","","21/05/29,14:14:38+12"
14:14:48.613 -> Turn off
14:14:48.613 ->
14:14:48.613 -> OK
14:14:48.613 ->
14:14:48.613 -> Phone: +380983649285
14:14:48.660 -> Message: Turn off
14:14:48.660 -> Alarm deactivation
14:14:48.660 -> Alarm is deactivated
14:14:48.707 -> AT+CMGDA="DEL ALL"
14:14:49.735 ->
14:14:49.735 -> OK
```

Рисунок 3.22 - Результат тестування команди Turn off

З результатів випробувань, показаних на рис. 3.22 ви можете побачити систему. Після отримання та обробки повідомлення з номера власника сигналізація вимкнулась.

3. Перевірка роботи команди Turn on. (Рисунок 3.23 - Результат тестування команди Turn on)

```
14:15:29.724 -> +CMTI: "SM",1
14:15:29.771 -> AT+CMGR=1
14:15:30.852 ->
14:15:30.852 -> +CMGR: "REC UNREAD","+380983649285","","21/05/29,14:15:20+12"
14:15:30.944 -> Turn on
14:15:30.944 ->
14:15:30.944 -> OK
14:15:30.944 ->
14:15:30.944 -> Phone: +380983649285
14:15:30.991 -> Message: Turn on
14:15:30.991 -> Alarm activation
14:15:30.991 -> Alarm is activated
14:15:31.037 -> AT+CMGDA="DEL ALL"
14:15:32.060 ->
14:15:32.060 -> OK
```

Рисунок 3.23 - Результат тестування команди Turn on

З результатів випробувань, показаних на рис. 3.23 ви можете побачити систему

Обробка повідомлення з номера власника сигналізація включилась.

4. Перевірка роботи команди Status. (Рисунок 3.24 - Результат тестування команди Status)

```
14:20:21.436 -> +CMTI: "SM",2
14:20:21.436 -> AT+CMGR=2
14:20:22.557 ->
14:20:22.557 -> +CMGR: "REC UNREAD","+380983649285","","21/05/29,14:20:12+12"
14:20:22.602 -> Status
14:20:22.602 ->
14:20:22.602 -> OK
14:20:22.649 ->
14:20:22.649 -> Phone: +380983649285
14:20:22.649 -> Message: Status
14:20:22.649 -> AT+CMGS="+380983649285"
14:20:23.672 ->
14:20:23.672 -> >
14:20:23.672 -> Signalization is inactive
14:20:23.719 -> □
14:20:24.757 -> Signalization is inactive
14:20:24.804 -> >
14:20:24.804 -> >
14:20:24.804 -> AT+CMGDA="DEL ALL"
14:20:27.515 ->
14:20:27.515 -> +CMGS: 47
14:20:27.515 ->
14:20:27.515 -> OK
```

Рисунок 3.24 - Результат тестування команди Status

Система обробила запит та надіслала результат команди та статус системи.

Аналіз результатів тестування показав, що система безпеки на базі Arduino працювала належним чином. особливо:

1. Виявлення руху та відкриття дверей:

- Тести датчиків руху та відкритих датчиків показали, що система ефективно реагує на зміни навколишнього середовища.
- Час реакції датчиків на події, особливо виявлення руху та відкриття дверей чи вікон, відповідає вимогам безпеки.

2. Управління сигналізацією:

- Відтворення команд «вимкнути» і «включити» показало, що система правильно розпізнала та обробила команди користувача.
- Сигналізація ефективно вмикається та вимикається на основі отриманих команд.

3. Статус системи:

- Функція «Статус» працює коректно, надаючи користувачам інформацію про поточний стан їх системи безпеки.
- Система надійно передає відповіді на запити статусу, дозволяючи користувачам контролювати роботу системи.

Результати тестування зазвичай свідчать про успішну інтеграцію компонентів системи безпеки та правильну реакцію на різні події. Параметри, виявлені під час тестування, відповідають вимогам безпеки та забезпечують ефективну роботу системи на практиці.

3.5 Порівняння з існуючими системами безпеки

Порівняльний аналіз систем безпеки на базі Arduino з традиційними аналогами дозволяє виявити як подібності, так і відмінності, які слід враховувати при виборі оптимального рішення для конкретного випадку.

Arduino проти пропрієтарні системи безпеки:

- Вартість: Arduino може бути дешевшим варіантом порівняно з пропрієтарними системами з високою вартістю обладнання та ліцензування.
- Гнучкість: Arduino пропонує більшу гнучкість у налаштуванні та розширенні своєї функціональності за допомогою відкритого коду та різноманітних

бібліотек і розширень.

- Спільнота та підтримка: Arduino має велику спільноту користувачів і активну підтримку, тому ви можете отримати допомогу та поради від інших розробників.

Arduino проти інших відкритих систем безпеки:

- Простота використання: Arduino може бути легшим у налаштуванні та програмуванні, ніж інші системи з відкритим кодом, які можуть мати складніші інтерфейси або вимагати більше досвіду в електроніці та програмуванні.
- Інтеграція з екосистемою Arduino: Arduino дозволяє легко інтегрувати вашу систему безпеки з іншими проектами та пристроями, які підтримують цю платформу.
- Масштабованість: залежно від конкретних вимог інші відкриті системи можуть мати більшу масштабованість і масштабованість, що може бути важливим для великих підприємств або складних інфраструктур.

Зрештою, вибір між Arduino та іншою системою безпеки залежатиме від ваших конкретних потреб, вимог безпеки, доступності ресурсів і досвіду розробника.

3.6 Результати тестування та аналізу системи

Під час роботи були розглянуті всі аспекти процесу, від вибору компонентів і обладнання до створення програмного забезпечення та тестування прототипу системи. Основні етапи розвитку:

1. Вибір комплектуючих та обладнання:

Був проведений ретельний аналіз наявних датчиків, камер та інших компонентів з урахуванням конкретних вимог системи безпеки. Вибрані компоненти, такі як

датчик руху HC-SR501, магнітний датчик відкриття MC-38, камери Arducam і Hikvision, електронний замок SEVEN LOCK і RFID-зчитувач, забезпечують високу чутливість, швидку реакцію і можливість розширення функціональності системи.

2. Програмування мікроконтролерів Arduino:

Програмне забезпечення, розроблене на мові C/C++, яке забезпечує зчитування даних із датчиків, керування камерою та системами контролю доступу. Алгоритм програмування включав налаштування портів введення/виведення, обробку сигналів датчиків, активацію камер при виявленні руху, ідентифікацію користувачів за допомогою RFID-карт і керування електронними замками.

3. Складання та тестування прототипів системи:

На цьому етапі всі компоненти були фізично підключені до мікроконтролера Arduino та протестований прототип системи. Тестування включало перевірку роботи датчиків руху та відкриття, камер відеоспостереження та систем контролю доступу. Результати тестування показують, що система ефективно виявляє рух, відкривання дверей чи вікон, ідентифікує користувачів і забезпечує контроль доступу.

Аналіз результатів тестування показує, що розроблена система на базі Arduino відповідає вимогам безпеки підприємств, забезпечуючи надійний моніторинг і контроль доступу. Система виявилася гнучкою та масштабованою, дозволяючи за потреби додавати нові функції та компоненти. Це демонструє значний потенціал для використання мікроконтролерів Arduino для розробки безпечних систем, особливо в середовищі Інтернету речей (IoT).

У порівнянні з традиційними системами безпеки, рішення на основі Arduino мають кілька ключових переваг, включаючи доступність, простоту використання та програмування, а також легку інтеграцію з різними датчиками та модулями. Це робить Arduino ідеальним вибором для розробки спеціальних систем безпеки, які відповідають конкретним потребам вашої компанії.

В цілому розробка прототипу та результати тестування підтвердили доцільність створення ефективної та надійної системи безпеки з використанням мікроконтролерів Arduino. Це відкриває нові перспективи для подальших досліджень і розробок у цій галузі, особливо в напрямку вдосконалення функціональності, підвищення рівня автоматизації та інтеграції з іншими рішеннями IoT.

4. ПЕРЕВАГИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ IoT-РІШЕНЬ У СФЕРІ БЕЗПЕКИ

Використання рішень Інтернету речей (IoT) у сфері безпеки відкриває різноманітні переваги та перспективи, які сприяють підвищенню ефективності та надійності систем безпеки. Деякі з них такі:

1. Покращене реагування на події: системи IoT можуть швидко виявляти та реагувати на події безпеки, такі як рух або вторгнення, щоб негайно вжити заходів.

2. Підвищення ефективності використання ресурсів: рішення IoT можуть допомогти вам оптимізувати використання таких ресурсів, як енергія, світло та вода, щоб зменшити витрати та забезпечити стабільну роботу вашої системи.

3. Віддалений моніторинг і контроль: системи безпеки на основі IoT можна дистанційно контролювати та контролювати через підключення до Інтернету, забезпечуючи доступ у будь-який час і в будь-якому місці.

4. Покращена безпека: рішення IoT можуть підвищити безпеку, автоматично виявляючи потенційні загрози та реагуючи до того, як вони стануть

серйозними.

5. Широкі можливості інтеграції: IoT дозволяє легко інтегрувати різні компоненти та системи, сприяючи створенню комплексних рішень безпеки, які враховують різні аспекти безпеки об’єктів.

У майбутньому розвиток технології IoT обіцяє більше інновацій і вдосконалень у сфері безпеки, включаючи вдосконалення алгоритмів розпізнавання, впровадження штучного інтелекту для аналізу даних і прийняття рішень, а також розширення можливостей, включаючи нові пристрої та датчики.

4.1 Переваги використання Arduino для розробки систем безпеки

Розробка систем безпеки за допомогою платформи Arduino має кілька переваг, які роблять її привабливим вибором для цієї галузі. Деякі з них такі:

1. Простота використання: Arduino відома своєю простотою у використанні навіть для початківців у електронному проектуванні та програмуванні.

2. Широкий вибір компонентів: платформа підтримує численні датчики, модулі та розширення, що дозволяє легко вибрати правильні компоненти для будь-якого проекту безпеки.

3. Універсальність: Arduino має численні вбудовані функції та бібліотеки, які спрощують розробку різноманітних програм, включаючи системи безпеки. Arduino може виконувати широкий спектр завдань, від взаємодії з датчиками до керування механізмами.

4. Рентабельність: Arduino є відносно недорогою платформою, що робить її доступною для широкого кола розробників і компаній з різними бюджетами.

5. Простота інтеграції: Arduino можна легко інтегрувати з іншими пристроями та системами за допомогою різноманітних інтерфейсів і протоколів зв’язку.

Завдяки своїй природі з відкритим кодом Arduino базується на програмному забезпеченні з відкритим кодом і має велику спільноту розробників, яка сприяє обміну досвідом і розробці нових ідей і проектів.

Загалом використання Arduino для розробки системи безпеки дозволяє створити ефективне та надійне рішення з мінімальними часовими та грошовими витратами.

4.2 Потенційні перспективи розвитку та вдосконалення

Інтернет речей (IoT) — це концепція, яка автоматизує та оптимізує різні процеси шляхом підключення фізичних пристроїв до Інтернету та обміну даними між пристроями. Сьогодні IoT використовується в різних галузях промисловості, включаючи системи безпеки підприємств. Ключові компоненти цих систем включають датчики руху та відкриття, камери відеоспостереження, системи контролю доступу та мікроконтролери Arduino.

Мікроконтролери Arduino відрізняються простотою використання та універсальністю. Він підтримує різноманітні датчики, модулі та розширення, що робить його універсальним для створення різноманітних проектів безпеки. Arduino також має багато вбудованих функцій і бібліотек, які спрощують розробку додатків.

Системи безпеки на основі Arduino можуть включати різноманітні компоненти, такі як датчики руху та відкриття, камери відеоспостереження, системи контролю доступу тощо. Ці компоненти інтегровані в Arduino для забезпечення стабільної та ефективної роботи системи безпеки.

Програмне забезпечення Arduino містить код для зчитування даних із датчиків, камер керування та систем контролю доступу, а також відображення інформації про

стан системи. Після написання програмного забезпечення система тестується для перевірки її функціональності та стабільності.

Результати тестування показують реакцію системи на різні події, такі як виявлення руху або відкриття дверей, і впевненість у правильному функціонуванні системи. Після тестування програмне та апаратне забезпечення можна налаштувати для оптимізації продуктивності системи.

У порівнянні з традиційними системами безпеки, системи на базі Arduino відрізняються простотою використання, гнучкістю та можливістю розширення функціональності. Малий і середній бізнес може використовувати його дешевше та ефективніше. Перевага використання Arduino полягає в тому, що ви можете вибрати з безлічі додаткових компонентів, і вони також недорогі.

Майбутні розробки систем безпеки на основі Arduino можуть включати розширення функціональності, підвищення рівня безпеки, інтеграцію з хмарними службами, підвищення енергоефективності та покращення масштабованості. Ці вдосконалення допоможуть підвищити надійність і ефективність систем безпеки на основі Arduino.

ВИСНОВКИ

У цьому дослідженні концепція Інтернету речей (IoT) та її застосування у сфері корпоративної безпеки розглядалися на прикладі розробки системи на основі мікроконтролера Arduino. Огляд історії та розвитку мікроконтролера Arduino і його особливостей дозволив нам отримати уявлення про потенціал цієї платформи для створення різноманітних проектів у сфері IoT.

Детальний розгляд основних складових охоронної системи – датчиків руху та відкриття, камер відеоспостереження, систем контролю доступу – дозволив визначити набір обладнання, необхідного для побудови комплексної системи безпеки.

Програмування мікроконтролерів Arduino на мові програмування C/C++ відіграє ключову роль у реалізації функцій системи безпеки, включаючи зчитування даних з датчиків, керування камерами та системами контролю доступу.

Тестування прототипу системи підтвердило функціональність і надійність в реальних умовах. Аналіз результатів тестування показав, що система функціонує коректно, а також виявив можливості для подальшого вдосконалення.

У порівнянні з традиційними системами безпеки, системи на базі Arduino відрізняються простотою використання, гнучкістю та низькою вартістю. Перевагою використання Arduino є широкий спектр можливостей для розширення функціональності та надійності.

У майбутньому очікується розвиток систем безпеки на базі Arduino в контексті функціонального розширення, покращення безпеки та енергоефективності, інтеграції з хмарними сервісами та збільшення масштабованості.

Тому використання IoT-рішень у сфері безпеки є перспективним напрямком розвитку, який може значно підвищити безпеку та ефективність управління підприємствами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Lake, D., Rayes, A., and Morrow, M., “The Internet of Things,” The Internet Protocol Journal, Volume 15, No. 3, September 2012.
2. ITU-T, “Common Requirements and Capabilities of a Gateway for Internet of Things Applications,” Recommendation Y.2067, June 2014.
3. Cisco Systems, “The Internet of Things Reference Model,” White Paper, 2014. http://www.iotwf.com/
4. Frahim, J., et al., “Securing the Internet of Things: A Proposed Framework,” Cisco White Paper, March 2015
5. ITU-T, “Overview of the Internet of Things,” Recommendation Y.2060, June 2012.
6. Погребенник В. Д., Політило Р. В. Ультразвукові сенсори системи охоронної сигналізації. Вісник НТУУ “КПІ”. Серія «Приладобудування». 2008. Вип. 36. С. 68-76.
7. Кугір А. В. Автоматизована система охоронної сигналізації для промислового підприємства. 2021. С. 75-76.
8. Çavaş M., Ahmad M. B. A review advancement of security alarm system using internet of things (IoT). International Journal of New Computer Architectures and their Applications (IJNCAA). 9 (2). 2019.P. 38-49.
9. Михальчук Д. О., Яворська О. М. Аналіз ринку систем охоронної сигналізації. Матеріали 75-ї науково-технічної конференції професорськовикладацького складу, науковців, аспірантів та студентів. 2020. С. 49-50.
10. Ahmad M. B., Abdullahi A. A., Muhammad A. S., Saleh Y. B., Usman U. B. The Various Types of sensors used in the Security Alarm system. International Journal of New Computer Architectures and their Applications (IJNCAA). 2019. 9(2). P. 50-59
11. Скрытое видео и аудіо наблюдение. URL: https://guardlviv.com.ua/info/skrytoe-video-i-audio-nablyudenie.

12. Автономные охранные сигнализации. URL: https://www.forter.com.ua/news-and-articles/avtonomnye-ohrannyesignalizatsii-kak-eto-rabotaet/.
13. Розумний будинок. URL: https://www.smarthouse.ua/ua/umnyj_dom.html.
14. Афзель, С.С. Огляд сучасного стану та перспективи розвитку датчиків руху/ С.С. Афзель, М.О. Березанська // Ефективність інженерних рішень у приладобудуванні : матеріали доповідей XIV Всеукраїнської науковопрактичної конференція студентів, аспірантів та молодих вчених, 2018 – С. 16.
15. Афзель, С.С. Порівняльний аналіз датчиків руху, що застосовуються в охоронних системах / С. С. Крошкін, Д. А. Півторак // Нові напрямки розвитку приладобудування: матеріали 12-ї Міжнародної науково-технічної конференції молодих вчених та студентів», 2019 – С. 128–133.
16. Arduino NANO URL:http://arduino-nano.ua
17. Arduino MEGA URL:http://arduino-mega.ua
18. Іванов А. О. Теорія автоматичного керування: Підручник. — Дніпропетровськ: Національний гірничий університет. — 2014. — 250 с.
19. Енциклопедія кібернетики. тт. 1, 2. — К.: Головна редакція УРЕ, 2016. 17
20. Офіційний сайт Arduino. – URL: http://www.arduino.cc/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

Державний університет інформаційно-комунікаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Розробка IoT-рішення охоронної системи підприємства за допомогою Arduino»

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

Виконав: **Ніконов І. М. , ІСД-41**
Науковий керівник роботи:
Данильченко В.М.

Київ - 2024

Слайд 1

Актуальність теми:

Безпека підприємств у сучасному світі є надзвичайно важливою через зростання рівня злочинності та кіберзагроз. Інтернет речей (IoT) відкриває нові можливості для створення інтегрованих систем безпеки, що забезпечують підвищену надійність, ефективність, економічну доцільність, віддалений моніторинг та керування.

Наукова новизна:

Наукова новизна даного дослідження полягає в розробці інноваційної системи безпеки підприємства на базі IoT з використанням мікроконтролерів Arduino. Це дослідження включає комплексний підхід до інтеграції різних компонентів, таких як датчики руху, відеокамери та системи контролю доступу, в єдину ефективну систему безпеки.

Об'єкт дослідження:

Системи безпеки підприємств, що використовують технології Інтернету речей.

Предмет дослідження:

Технологічні рішення та компоненти для розробки систем безпеки на базі мікроконтролерів Arduino.

Мета дослідження:

Розробка та впровадження ефективної системи безпеки підприємства на базі IoT з використанням мікроконтролерів Arduino для забезпечення надійного захисту майна, інформації та персоналу.

Завдання дослідження:

1. Провести огляд концепції Інтернету речей та його застосування в системах безпеки.
2. Проаналізувати основні компоненти систем безпеки підприємства, включаючи датчики руху, відеокамери та системи контролю доступу.
3. Розробити та протестувати прототип системи безпеки на базі мікроконтролера Arduino, включаючи програмне забезпечення для обробки даних та керування компонентами системи.

Слайд 2

Можливості та важливість IoT в сучасному світі

Основною метою IoT є забезпечення зв'язку та обміну даними між фізичними пристроями, що раніше були відокремлені. Це дозволяє створювати інтелектуальні системи, які можуть автоматизувати багато процесів, полегшити життя людей та підвищити продуктивність промислових процесів. Наприклад, в сільському господарстві системи IoT можуть використовуватися для моніторингу урожаю та автоматичного поливу, що дозволяє знизити витрати та підвищити врожайність.

Слайд 3

Основні компоненти систем безпеки підприємства

Системи безпеки підприємства включають в себе ряд ключових компонентів, які спрямовані на захист майна, співробітників і конфіденційної інформації. Ці компоненти інтегровані в комплексну систему на основі Arduino.

Сюди входять системи контролю доступу, які обмежують доступ до певних приміщень або об'єктів лише уповноваженим співробітникам або особам. Системи безпеки також включають системи пожежної безпеки, які виявляють і сигналізують про пожежну небезпеку, а також системи оповіщення про надзвичайні ситуації, які швидко і ефективно інформують співробітників і охоронців про надзвичайні ситуації.

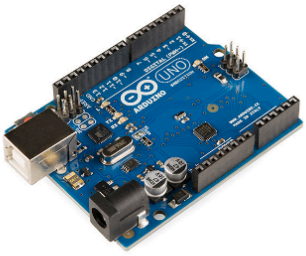

Рисунок 4.1 – Arduino Mega

Рисунок 4.2 – RFID-зчитувач RC522

Рисунок 4.3 – датчик руху інфачервоний HC-SR 501

Слайд 4

АРХІТЕКТУРА СИСТЕМИ БЕЗПЕКИ НА БАЗІ ARDUINO

Архітектура системи безпеки на основі Arduino зазвичай складається з набору компонентів, які включають датчики (наприклад, датчики руху та відкриття), камери відеоспостереження, сигналізацію та системи контролю доступу. Ці компоненти працюють разом, щоб виявляти потенційні загрози та реагувати на них.

Основними перевагами цих архітектур є складність та інтегрованість. Кожен компонент системи виконує певну роль, але разом вони забезпечують повний захист об'єкта. Крім того, використання Arduino як базової платформи дозволяє легко розширювати та оновлювати систему за потреби.

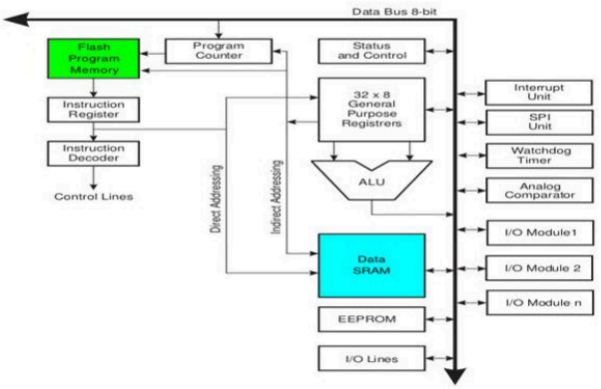

Рисунок 5.1 – Архітектура Arduino

Слайд 5

РОЗРОБКА ТА РЕАЛІЗАЦІЯ СИСТЕМИ БЕЗПЕКИ НА ARDUINO

Датчики руху та відкриття:

- Пара датчиків руху HC-SR501, які мають високу чутливість та дальність дії.
- Магнітний датчик відкриття для дверей або вікон.

Камери відеоспостереження:

- Камера з високою роздільною здатністю та швидким часом реакції - модель Arducam 64-мегапіксельна камера з надвисокою роздільною здатністю і автофокусом.
- IP-камера з можливістю стрімінгу в реальному часі - IP камера Hikvision DS-2CD1321-I .

Система контролю доступу:

- Електронний замок з підтримкою RFID-карт або кодового замку SEVEN LOCK SL-7737S silver ID EM
- RFID-читач для ідентифікації користувачів. RC-522 RFID-зчитувач

Мікроконтролер Arduino:

- Arduino Mega, підходить для нашого обсягу, оброблювання даних та кількості підключених пристроїв.

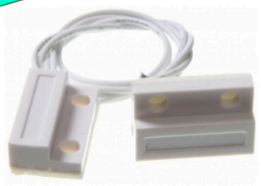

Рисунок 6.1 – Магнітний датчик відкриття дверей

Рисунок 6.2 – Arducam 64-мегапіксельна камера

Слайд 6

Тестування мікроконтролера Arduino

Тестування проводиться за допомогою вбудованих засобів. Середовище розробки Arduino IDE. Це було для перевірки роботи системи. Для відображення інформації в серійному форматі розроблені спеціальні скетчі.

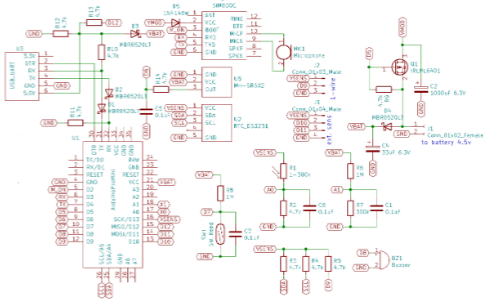

Рисунок 7.1 – Схема підключень Arduino

```
14:20:21.436 -> +CMTI: "SM",2
14:20:21.436 -> AT+CMGR=2
14:20:22.557 ->
14:20:22.557 -> +CMGR: "REC UNREAD","+380983649285","","21/05/29,14:20:12+12"
14:20:22.602 -> Status
14:20:22.602 ->
14:20:22.602 -> OK
14:20:22.649 ->
14:20:22.649 -> Phone: +380983649285
14:20:22.649 -> Message: Status
14:20:22.649 -> AT+CMGS="+380983649285"
14:20:23.672 ->
14:20:23.672 -> >
14:20:23.672 -> Signalization is inactive
14:20:23.719 -> □
14:20:24.757 -> Signalization is inactive
14:20:24.804 -> >
14:20:24.804 -> >
14:20:24.804 -> AT+CMGDA="DEL ALL"
14:20:27.515 ->
14:20:27.515 -> +CMGS: 47
14:20:27.515 ->
```

рисунок 7.2 – Результат тестування команди Status

```
14:11:48.601 -> Alarm is activated
14:12:03.321 -> Motoin detected
14:12:13.340 -> AT+CMGS="+380983649285"
14:12:14.372 ->
14:12:14.372 -> >
14:12:14.372 -> Motion detected! Alarm had been activated!
14:12:14.419 -> □
```

Motion detected! Alarm had been activated!

Рисунок 7.3 – Результат тестування датчику руху

Результати тестування зазвичай свідчать про успішну інтеграцію компонентів системи безпеки та правильну реакцію на різні події. Параметри, виявлені під час тестування, відповідають вимогам безпеки та забезпечують ефективну роботу системи на практиці.

Слайд 7

Порівняння з існуючими системами безпеки

Порівняльний аналіз систем безпеки на базі Arduino з традиційними аналогами дозволяє виявити як подібності, так і відмінності, які слід враховувати при виборі оптимального рішення для конкретного випадку.

Arduino проти пропрієтарні системи безпеки:

- **Вартість:** Arduino може бути дешевшим варіантом порівняно з пропрієтарними системами з високою вартістю обладнання та ліцензування.
- **Гнучкість:** Arduino пропонує більшу гнучкість у налаштуванні та розширенні своєї функціональності за допомогою відкритого коду та різноманітних бібліотек і розширень.
- **Спільнота та підтримка:** Arduino має велику спільноту користувачів і активну підтримку, тому ви можете отримати допомогу та поради від інших розробників.

Arduino проти інших відкритих систем безпеки:

- **Простота використання:** Arduino може бути легшим у налаштуванні та програмуванні, ніж інші системи з відкритим кодом, які можуть мати складніші інтерфейси або вимагати більше досвіду в електроніці та програмуванні.
- **Інтеграція з екосистемою Arduino:** Arduino дозволяє легко інтегрувати вашу систему безпеки з іншими проектами та пристроями, які підтримують цю платформу.
- **Масштабованість:** залежно від конкретних вимог інші відкриті системи можуть мати більшу масштабованість і масштабованість, що може бути важливим для великих підприємств або складних інфраструктур.

Слайд 8

Висновки

Досліджено: Сучасні технології Інтернету речей (IoT) та їх застосування у системах безпеки підприємств.

Можливості та функціональні можливості мікроконтролерів Arduino для створення систем безпеки.

Визначено: Перспективи та можливості подальшого розвитку та вдосконалення IoT-рішень для систем безпеки на базі Arduino.

Переваги використання Arduino для розробки економічно доступних, масштабованих та гнучких систем безпеки.

Виявлено: Переваги та недоліки використання Arduino у порівнянні з іншими мікроконтролерами для IoT-рішень.

Основні проблеми та виклики, пов'язані з впровадженням IoT-рішень у сфері безпеки.

Аналіз результатів тестування показує, що розроблена система на базі Arduino відповідає вимогам безпеки підприємств, забезпечуючи надійний моніторинг і контроль доступу. Система виявилася гнучкою та масштабованою, дозволяючи за потреби додавати нові функції та компоненти. Це демонструє значний потенціал для використання мікроконтролерів Arduino для розробки безпечних систем, особливо в середовищі Інтернету речей (IoT).

Тези:

Ніконов, І.М . (2023). "ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ ІНТЕРНЕТ РЕЧЕЙ У ГАЛУЗІ ЕНЕРГЕТИКИ ДЛЯ СТВОРЕННЯ "РОЗУМНИХ" МЕРЕЖ ЕЛЕКТРОПОСТАЧАННЯ ТА ОПТИМІЗАЦІЇ ЕНЕРГОЕФЕКТИВНОСТІ". Матеріали ВСЕУКРАЇНСЬКА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ «ТЕХНОЛОГІЧНІ ГОРІЗОНТИ: ДОСЛІДЖЕННЯ ТА ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ТЕХНОЛОГІЧНОГО ПРОГРЕСУ УКРАЇНИ І СВІТУ», Київ, 28 листопаду 2023 року, с. 138.

Ніконов, І.М . (2024). "Використання Інтернету речей (IoT) для оптимізації управління водними ресурсами у містах для сталого розвитку". Матеріали V МІЖНАРОДНА НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ «СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ IOT», Київ, 18 квітня 2024 року.

Слайд 9