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

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Мікроконтролерна система контролю доступу на базі Atmega328P
Назва теми

КвРКІ 101061.21.01.11 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Виконав: студент III курсу, група КІ2с-21-1 _____ В. І. Подвисоцький
Підпис Ініціали, прізвище

Керівник _____ В. М. Грига
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ І.О. Засорнова
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Т.О. Говорущенко
Підпис Ініціали, прізвище

«13» червня 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"19" 01 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Подвисоцькому Владиславу Івановичу

Прізвище, ім'я, по батькові студента

1. **Тема проекту (роботи)** Мікроконтролерна система контролю доступу на базі Atmega328P

Керівник проекту (роботи) Грига В.М., , к.т.н., доцент

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

Затверджена наказом ректора університету від 15.02.2024 р. № 8

2. **Строк подання студентом проекту (роботи) на кафедру** 01.06.2024 р.

3. **Вихідні дані до проекту (роботи)** Завдання на кваліфікаційну роботу

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

Огляд та аналіз методів ідентифікації доступів

Проектування мікроконтролерної системи контролю доступу

Програмно-апаратна реалізація та тестування мікроконтролерної системи контролю доступу

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

Електрично-принципова схема мікроконтролерної системи контролю доступу на базі Atmega 328P

Логічна схема алгоритму та структурна схема мікроконтролерної системи контролю доступу на базі Atmega328P

Функціональна схема мікроконтролерної системи контролю доступу на базі Atmega328P

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Засорнова І.О., доцент кафедри КІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІС		

7. Дата видачі завдання «10» 01 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	10.01.2024	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2024	виконано
3	Робота над розділом 1 – огляд та аналіз методів ідентифікації доступів	01.03.2024	виконано
4	Робота над розділом 2 – вибір компонентів для проєктування та тестування мікроконтролерної системи контролю доступу	01.04.2024	виконано
5	Робота над розділом 3 – огляд реалізованого програмного забезпечення та функціонування пристрою контролю доступу	29.04.2024	виконано
6	Оформлення пояснювальної записки згідно вимог	25.05.2024	виконано
7	Попередній захист ВКР	30.05.2024	виконано
8	Захист ВКР на засіданні ЕК	Червень 2024 року	

Студент _____ В. І. Подвисоцький
Підпис Ініціали, прізвище

Керівник роботи _____ В. М. Грига
Підпис Ініціали, прізвище

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 101061.21.01.11 ПЗ	Пояснювальна записка	62		
			Графічні матеріали			
2		КвРКІ 101061.21.01.11 Е2	Електрично-принципова схема мікроконтролерної системи контролю доступу на базі Atmega 328P	1		
3		КвРКІ 101061.21.01.11 Е8	Логічна схема алгоритму та структурна схема мікроконтролерної системи контролю доступу на базі Atmega 328P	1		
4		КвРКІ 101061.21.01.11 Е8	Функціональна схема мікроконтролерної системи контролю доступу на базі Atmega 328P	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 101061.21.01.11 ВП			
Розробив		Подмасощький		13.06	Мікроконтролерна система контролю доступу на базі Atmega328P	Літера	Аркуш	Аркушів
Перевір.		Гриця В.М.		13.06		У	1	1
Н. контр.		Засорінова		13.06		ХНУ, КІ2с-21-1		
Затв.		Говорущенко		13.06				

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Мікроконтролерна система контролю доступу на базі Atmega328P».

Автор роботи: Подвисоцький Владислав Іванович.

Керівник роботи: Грига Володимир Михайлович

Пояснювальна записка: 62 с., 20 рисунок, 4 дод., 60 джерел.

Графічна частина: 3 креслення.

ATMEGA328P, КОНТРОЛЬ ДОСТУПУ, ПАРОЛЬНА ІДЕНТИФІКАЦІЯ, АПАРАТНА ІДЕНТИФІКАЦІЯ.

Мета дипломної роботи полягає у вивчені методів ідентифікації доступу,щоб знайти найбільш ефективний та безпечний в конкретних випадках використання

Об'єктом роботи є процес розробки та функціонування мікроконтролерної системи контролю доступу на базі мікроконтролера Atmega328P, що включає створення апаратної та програмної частини для забезпечення надійного контролю доступу до приміщень чи об'єктів, інтеграцію різних датчиків та виконавчих механізмів, обробку даних від них та прийняття рішень щодо надання або відмови в доступі.

Предметом дослідження є програмно-технічна реалізація системи контролю доступу на базі Atmega328P, що передбачає використання RFID зчитувача для ідентифікації користувачів, LCD дисплея для відображення інформації, клавіатури для введення PIN-кодів та електромагнітного замка для управління доступом.

Практичне значення полягає у дослідженні методу систематичного огляду літератури для вивчення і аналізу предметної області даного дослідження з текстових джерел інформації. Це дозволить визначити найкращі методи реалізації систем контролю доступу, які були враховані при розробці власної системи.

Підпис студента

03.06.2024

Дата

ЗМІСТ

ВСТУП

У світі, де цифрові технології проникають у всі сфери нашого життя, захист особистої інформації та конфіденційності даних стає однією з найбільш актуальних проблем. Захищений доступ до інформації в мережі Інтернет стає дедалі важливішим завданням для підприємств, організацій та користувачів. У цьому контексті огляд та аналіз методів ідентифікації доступу набуває особливого значення [1].

Методи ідентифікації доступу визначаються як набір процедур та технологій, що забезпечують контроль доступу до різних ресурсів та послуг. Вони відіграють критичну роль у захисті від несанкціонованого доступу та забезпеченні безпеки мереж та даних.

У ході дослідження буде проведемо огляд та ретельний аналіз різних методів ідентифікації доступу, вивчаючи їхні переваги, недоліки та виклики, що виникають у контексті сучасного цифрового середовища. Виокремлено ключові аспекти кожного методу та розглянемо їхні застосування в різних сферах, від бізнесу до особистого використання.

Мета дослідження полягає у тому, щоб зрозуміти, які методи ідентифікації доступу є найбільш ефективними та безпечними в конкретних випадках використання. Даний аналіз надасть узагальнену картину стану сучасних підходів до захисту доступу, допоможе виявити тенденції розвитку цієї галузі та запропонує рекомендації щодо вдосконалення систем ідентифікації доступу з метою забезпечення максимального рівня безпеки та захисту приватності.

Предметом дослідження є програмно-технічна реалізація системи контролю доступу на базі Atmega328P.

Об'єктом роботи є процес розробки та функціонування мікроконтролерної системи контролю доступу на базі мікроконтролера Atmega328P.

1 ОГЛЯД ТА АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ ДОСТУПУ

1.1 Актуальність тематики

Розроблення системи контролю доступу на базі мікроконтролера Atmega 328P може залишатися актуальним завданням у різних сферах, таких як будівельна безпека, офісні приміщення, склади тощо. Atmega 328P - це популярний мікроконтролер, який забезпечує достатній рівень функціональності та надійності для багатьох додатків. За наявності відповідних знань та навичок у програмуванні мікроконтролерів, розробка системи контролю доступу на його базі може бути ефективним рішенням [2]. Однак, завжди важливо враховувати нові технології та потреби ринку, щоб забезпечити відповідність розробленої системи сучасним вимогам і стандартам безпеки.

Системи контролю доступу використовуються для регулювання та обмеження доступу до певних об'єктів, приміщень або ресурсів. Їх використовують у різних сферах, включаючи комерційні, промислові, медичні, освітні та громадські установи. Основні компоненти систем контролю доступу включають:

– ідентифікаційні пристрої: це можуть бути картки доступу, ключ-карти, біометричні розпізнавальні системи (відбитки пальців, розпізнавання обличчя, сканування радужки ока тощо), PIN-коди або смартфони з додатками для контролю доступу;

– контролери доступу: вони відповідають за обробку інформації з ідентифікаційних пристроїв і прийняття рішення про надання або відмову у доступі. Можуть бути реалізовані на базі мікроконтролерів, як Atmega 328P, або на більш потужних пристроях;

– системи входів/виходів: двері, шлагбауми, турнікети або інші механізми фізичного доступу, які відкриваються або закриваються залежно від рішення контролера доступу;

– системи моніторингу та аналітики: ці системи відслідковують та реєструють події, пов'язані з контролем доступу, наприклад, час входу/виходу, спроби неуспішного доступу, тощо. Вони також можуть надавати аналітичні дані для звітності та аналізу;

– системи управління доступом: ці системи дозволяють адміністраторам налаштовувати права доступу для користувачів або груп користувачів, створювати розклади доступу, вести журнали подій тощо.

Широка функціональність і гнучкість систем контролю доступу робить їх важливими для забезпечення безпеки та ефективного управління доступом у будь-якому середовищі.

1.2 Класифікація систем контролю доступу

Системи контролю доступу – це технологічні рішення, які забезпечують контроль доступу до певних приміщень, об’єктів, інформації чи ресурсів. Головна мета такого охоронного обладнання – безпека та зниження ймовірності несанкціонованих дій. Системи контролю доступу можна класифікувати за різними критеріями:

а) за типом ідентифікації:

1) карткові системи [3]: використовуються картки або ключ-карти для ідентифікації;

2) біометричні системи [4]: використовують біологічні характеристики, такі як відбитки пальців, розпізнавання обличчя, сканування радужки ока тощо;

3) пін-кодові системи [5]: вимагають введення особистого ідентифікаційного номера (ПІН);

б) за способом фізичного доступу:

1) електронні системи: відкривають двері або ворота за допомогою електронних механізмів, таких як електромагнітні замки або електромеханічні шпингалети;

2) механічні системи: використовують механічні замки або ключі для фізичного доступу;

в) за масштабом впровадження:

1) одномісні системи: призначені для контролю доступу до одного об'єкту, наприклад, окремої кімнати або приміщення;

2) розподілені системи: використовуються для контролю доступу до кількох об'єктів або приміщень, можуть бути розташовані на різних місцях;

г) за способом авторизації:

1) статичні системи: параметри доступу, такі як карткові дані або біометричні характеристики, не змінюються з часом;

2) динамічні системи: параметри доступу можуть змінюватися з часом, наприклад, за допомогою тимчасових кодів або розкладів доступу;

д) за цілями використання:

1) комерційні системи: використовуються для контролю доступу до комерційних будівель, офісів, магазинів тощо;

2) промислові системи: використовуються для контролю доступу до промислових об'єктів, складів, виробничих ліній тощо;

3) громадські системи: використовуються для контролю доступу до громадських місць, таких як аеропорти, вокзали, спортивні комплекси тощо.

Класифікація систем контролю доступу допомагає краще розуміти їх функціональність та вибирати найбільш підходящий варіант для конкретних потреб.

1.3 Огляд та аналіз методів парольної ідентифікації

Методи парольної ідентифікації використовуються для перевірки та підтвердження ідентичності користувача на основі введення пароля або ПІН-коду. Найбільш поширені методи ідентифікації [6]:

– пароль: це набір символів, який встановлюється користувачем і використовується для автентифікації. Паролі можуть бути легко запам'ятати або

складні, включаючи комбінації букв, цифр та спеціальних символів. Однак вони також можуть бути вкрадені або вгадані;

– пін-коди: це числові коди, які використовуються для ідентифікації користувача. Вони зазвичай коротші за паролі і зазвичай використовуються в банківських та фінансових системах. ПІН-коди можуть бути менш зручними для запам'ятовування, але також можуть бути менш вразливими до вгадування;

– модель жестів: цей метод вимагає введення певної послідовності рухів на сенсорному екрані, таких як з'єднання точок або малювання певного символу. Це може бути менш підходящим для деяких сценаріїв використання та менш безпечним, оскільки залишає сліди рухів на екрані;

– методи геометричного вводу: ці методи використовують геометричні параметри, такі як форма обличчя або структура пальців, для ідентифікації. Вони зазвичай використовуються в біометричних системах і можуть забезпечити високий рівень безпеки, але вимагають спеціалізованого обладнання та обробки даних;

– парольні фрази: це довші послідовності символів або слів, які можуть бути більш надійними, ніж звичайні паролі. Вони можуть містити комбінації букв, цифр та спеціальних символів та бути складнішими для вгадування.

Аналізуючи ці методи, важливо враховувати їх відмінності в зручності використання, рівні безпеки та вартості впровадження. Кожен метод має свої переваги та обмеження, і вибір повинен бути здійснений з урахуванням конкретних потреб та вимог до безпеки системи.

1.4 Огляд та аналіз методів апаратної ідентифікації

Цей метод ідентифікації та аутентифікації базується на використанні предмета, такого як картка або токен, що перебуває в виключному володінні користувача. Два основних типи таких пристроїв - різноманітні карти (такі як проксіміті-карти, смарткарти, магнітні карти тощо) та токени, які можна підключити безпосередньо до порту комп'ютера.

Основною перевагою використання апаратної ідентифікації є висока надійність. Токени можуть зберігати ключі, які складно підібрати, і мають різноманітні захисні механізми. Крім того, вони можуть мати вбудований мікропроцесор, що дозволяє їм не лише брати участь у процесі ідентифікації користувача, але й виконувати інші корисні функції.

Найбільш серйозною небезпекою у випадку використання даного методу є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів.

1.4.1 Електронні ключі

Електронні ключі - це електронні пристрої або програмні рішення, які використовуються для автентифікації та контролю доступу до об'єктів або систем. Вони можуть бути фізичними пристроями, такими як картки, токени або ключі, або цифровими сертифікатами та ідентифікаторами, які зберігаються на електронних пристроях, наприклад, у мобільному телефоні чи смарт-карті.

Компоненти електронного ключа:

– ідентифікатор: унікальний код або ідентифікатор, який визначає конкретного користувача чи пристрій;

– ключ доступу: криптографічний ключ або пароль, який використовується для автентифікації та забезпечення доступу до системи чи об'єкта;

– програмне забезпечення автентифікації: спеціалізоване програмне забезпечення, яке використовується для перевірки ідентифікаторів та ключів доступу та прийняття рішення про надання доступу;

– криптографічні пристрої: деякі електронні ключі можуть включати в себе криптографічні пристрої для забезпечення безпеки, такі як смарт-карти з вбудованими мікросхемами або апаратні токени.

Електронні ключі знаходять застосування в різних сферах, таких як фізичний доступ до будівель і приміщень, комп'ютерні системи та мережі,

електронна комерція, банківські послуги, транспорт і багато інших. Вони дозволяють забезпечити безпеку та контроль доступу до цінних ресурсів і інформації, а також забезпечують зручність та ефективність управління правами доступу.

На рисунку 1.1 показано приклад застосування електронного ключа.

Рисунок 1.1 — Приклад застосування електронного ключа

1.4.2 Штрих-коди

Штрих-коди (рисунок 1.2) - це унікальні зображення, які складаються з чорних смуг і прогалин, що кодують інформацію. Їх можна роздруковувати на картках або екранах телефонів.

Штрих-коди є простими у використанні та виготовленні, але вони можуть бути підроблені або пошкоджені. Вони підходять для застосувань з невеликим обсягом даних та не вимагають дорогого обладнання для читання.

Рисунок 1.2 — Штрих-код

Штрих-коди складаються з таких компонентів:

– чорні та білі смуги: смуги складаються з чорних та білих смуг, які розташовані поруч одна з одною у певному порядку. Кожна комбінація смуг відповідає певному символу або цифрі, яка інтерпретується при зчитуванні штрих-коду;

– контрольні символи: деякі штрих-коди містять контрольні символи, які допомагають перевірити правильність зчитування інформації з штрих-коду та виявити помилки;

– кодові системи: існують різні види штрих-кодів, такі як EAN (European Article Number), UPC (Universal Product Code), Code 39, Code 128, QR-коди тощо. Кожен тип штрих-коду має свої характеристики, призначення та можливості;

– сканери штрих-кодів: для зчитування інформації з штрих-кодів використовуються спеціальні пристрої - сканери штрих-кодів. Вони можуть бути ручними, стаціонарними або вбудованими в різноманітні пристрої, такі як касові апарати, мобільні телефони тощо.

Штрих-коди дуже поширені у різних галузях, таких як роздрібна торгівля, логістика, виробництво, медицина, транспорт тощою. Вони дозволяють швидко та ефективно ідентифікувати товари, ведення обліку, відстеження їх руху та забезпечують точність введення даних. Крім того, їх можна легко створити та надрукувати на пакуваннях товарів, етикетках, касових чеках та інших носіях.

1.4.3 Технологія RFID

RFID (Radio Frequency Identification) (рисунок 1.3) - це бездротова технологія ідентифікації, яка використовує радіочастоти для передачі даних між тегом та читачем [7].

RFID забезпечує швидку та безконтактну ідентифікацію. Вона широко використовується у логістиці, управлінні запасами, контролі доступу та інших галузях.

Система RFID складається з наступних компонентів:

– rfid-теги (мітки): це невеликі електронні пристрої, які містять унікальний ідентифікатор (ID). Вони можуть бути активними (живлені власним джерелом живлення) або пасивними (живляться електромагнітним полем, яке надсилає считувач). RFID-теги можуть бути вбудовані в товари, бірки, картки доступу тощо;

– зчитувачі (читачі): це пристрої, які здійснюють зчитування інформації з RFID-тегів за допомогою радіочастотних сигналів. Вони можуть бути фіксованими або портативними і розміщатися на дверях, полицях в магазинах, автомобільних мостах і т. д;

– системне програмне забезпечення: для обробки даних, отриманих від считувачів, та виконання необхідних функцій, таких як ідентифікація об'єктів, ведення інвентаризації тощо, використовується спеціалізоване програмне забезпечення;

– живлення і зв'язок: активні RFID-теги мають вбудовані джерела живлення (батареї), тоді як пасивні теги живляться від радіочастотного поля считувача. Зв'язок між тегами та считувачами здійснюється через бездротовий канал радіочастотного зв'язку.

Основні переваги технології RFID полягають у її безконтактності, можливості одночасної ідентифікації багатьох об'єктів, високій швидкості зчитування та можливості автоматизації бізнес-процесів. Вона знаходить застосування в різних галузях, таких як логістика, виробництво, транспорт,

сховищення даних та інші. Однак, до недоліків можна віднести високу вартість імплементації та обмежений радіус дії системи.

Рисунок 1.3 — Приклад використання RFID

1.4.4 Технологія NFC

NFC (Near Field Communication) (рисунок 1.4) - це бездротова технологія, яка дозволяє обмінюватися даними між пристроями на невеликій відстані.

NFC забезпечує швидку та зручну ідентифікацію через смартфони та інші мобільні пристрої. Вона широко використовується в мобільних платежах, ідентифікації та контролі доступу.

Основні компоненти технології NFC включають:

– пристрої NFC: це пристрої, які мають вбудований NFC-чіп. Це можуть бути смартфони, планшети, платіжні картки, смарт-годинники, рідко - комп'ютери;

– точки доступу NFC: це пристрої, які можуть зчитувати і записувати дані на NFC-теги та інші пристрої. Це можуть бути платіжні термінали, банкомати, точки продажу, смарт-термінали тощо;

– nfc-теги: це невеликі електронні пристрої, які містять інформацію, яку можна зчитувати та записувати за допомогою пристроїв NFC. Вони можуть бути використані для різноманітних цілей, таких як ідентифікація, доступ до інформації, контактні дані тощо;

– програмне забезпечення NFC: для роботи з пристроями NFC потрібне відповідне програмне забезпечення, яке дозволяє зчитувати та записувати дані, а також виконувати різні дії, такі як оплата, обмін файлами тощо.

Основні переваги технології NFC включають швидкий обмін даними, простоту використання та високий рівень безпеки (оскільки вона працює на відстані до 10 см). Вона знаходить широке застосування у платіжних системах, рекламі, туризмі, контролі доступу та багатьох інших галузях. Однак, вона має обмежений радіус дії та не підтримує обмін даними на великі відстані.

Рисунок 1.4 — Технологія NFC

1.5 Огляд та аналіз методів біометричної ідентифікації

Біометрична ідентифікація — це передовий метод впізнавання особи, що базується на унікальних фізіологічних або поведінкових характеристиках [8]. Відбитки пальців, розпізнавання обличчя, структура раковини вуха, розпізнавання ірису – це лише деякі з біометричних ознак, які можуть бути використані для ідентифікації.

Що стосується безпеки, біометричні системи забезпечують вищий рівень захисту в порівнянні з традиційними методами аутентифікації, такими як паролі або PIN-коди. Це пояснюється тим, що біометричні характеристики складніше підробити чи використати без дозволу в порівнянні зі звичайними паролями, які можуть бути вкрадені або вгадані.

Однак, наразі існують питання щодо приватності та безпеки даних, пов'язаних з біометричними системами. Існує потенційна загроза, що біометричні дані можуть бути скомпрометовані або вкрадені, що може призвести до серйозних наслідків для особистої приватності та безпеки користувачів.

Незважаючи на ці ризики, сучасний розвиток біометричних технологій продовжує зростати. Індустрія вдосконалює і розширює спектр біометричних ознак, вдосконалює алгоритми впізнавання та забезпечує більші можливості для використання цих технологій в різних сферах, включаючи інформаційну безпеку, фінанси, медицину та інші.

1.5.1 Статичні методи

Статичні методи біометричної ідентифікації ґрунтуються на аналізі фізіологічних або поведінкових характеристик людини, які залишаються сталими протягом тривалого періоду часу. Тут важливо відзначити, що ці характеристики не змінюються з часом або мають мінімальні зміни, які можна відслідкувати і врахувати.

Найпоширенішими статичними методами біометричної ідентифікації є:

– відбитки пальців: цей метод базується на аналізі унікальних деталей поверхні пальця, таких як візерунок та лінії. Біометричні системи сканують пальці користувача та зберігають унікальний шаблон, який може бути порівняний з під час наступної ідентифікації.

– розпізнавання обличчя: цей метод використовує унікальні особливості обличчя людини, такі як форма очей, носа, рота та інші деталі. Система зберігає шаблон обличчя та порівнює його з іншими шаблонами під час подальших ідентифікаційних процедур.

– розпізнавання раковини вуха: цей метод базується на унікальних особливостях раковини вуха, таких як форма та рельєф. Система сканує раковину вуха та порівнює її зі збереженими шаблонами.

– розпізнавання рітини очей: цей метод використовує унікальні особливості рітини очей, такі як венозний малюнок та пігментування. Система сканує рітину очей та зберігає унікальний шаблон для подальшого порівняння.

Статичні методи біометричної ідентифікації є надзвичайно ефективними та точними, оскільки вони базуються на унікальних характеристиках кожної людини. Вони застосовуються в різних сферах, від захисту особистих даних на мобільних пристроях до забезпечення безпеки в аеропортах та банківських установах.

1.5.2 Динамічні методи

Динамічні методи біометричної ідентифікації використовуються для аналізу та ідентифікації унікальних характеристик, що виникають у результаті рухів або дій користувача. Ці методи ґрунтуються на тому, що кожна людина має унікальний спосіб виконання певних дій або рухів, таких як письмо, мовлення або ходьба. Основні динамічні методи біометричної ідентифікації включають:

– розпізнавання рукопису: цей метод аналізує унікальні особливості рукопису користувача під час написання тексту. Система вимірює параметри, такі як швидкість письма, тиск на папір, кут нахилу ручки тощо, для створення унікального шаблону для ідентифікації;

– голосовий аналіз: цей метод базується на унікальних характеристиках голосу користувача, таких як тембр, частота голосу, інтонація тощо. Голосові зразки аналізуються і зберігаються для подальшого порівняння;

– динамічне розпізнавання письма на клавіатурі: Цей метод аналізує унікальний спосіб, яким користувач вводить текст на клавіатурі. Він враховує такі характеристики, як швидкість набору, час утримання клавіш, паузи між натисканням клавіш тощо;

– розпізнавання мовлення: Цей метод аналізує унікальні характеристики мовлення користувача, такі як інтонація, швидкість мовлення, акцент тощо. Голосові зразки аналізуються для створення унікального шаблону для ідентифікації.

Динамічні методи біометричної ідентифікації є надзвичайно ефективними, оскільки вони базуються на унікальних характеристиках, які важко підробити або підмінити. Ці методи застосовуються в різних сферах, від фінансових установ до контролю доступу до пристроїв та систем.

1.6 Огляд аналогічних систем контролю доступу

Існує багато відомих систем контролю доступу, які використовуються в різних сферах, від офісів до урядових установ і промислових об'єктів:

– salto system: це компанія, яка спеціалізується на електронних системах контролю доступу, таких як карткові чи мобільні ключі, електронні замки та системи контролю доступу для готелів, офісів та інших об'єктів;

– honeywell access control: Honeywell пропонує широкий спектр рішень з контролю доступу, включаючи системи карткового доступу, біометричні рішення, системи відеоспостереження та інші технології безпеки;

– kisi: це хмарна платформа для контролю доступу, яка пропонує рішення для офісів, спільних просторів та інших комерційних об'єктів. Kisi використовує сучасні технології, такі як мобільні додатки та хмарні зберігання, для забезпечення безпеки та зручності доступу;

– lenels2: ця компанія спеціалізується на інтегрованих системах безпеки, включаючи системи контролю доступу, відеоспостереження, а також системи безпеки на місцях роботи. LenelS2 пропонує рішення для різних типів об'єктів, від маленьких офісів до великих промислових комплексів;

– assa abloy: це велика корпорація, що володіє численними брендами в галузі безпеки, включаючи системи контролю доступу, замки та фурнітуру для дверей. ASSA ABLOY пропонує інноваційні рішення для різних вимог безпеки.

Ці системи контролю доступу використовуються для забезпечення безпеки об'єктів та обмеження доступу лише для авторизованих осіб. Вони можуть використовувати різні технології, включаючи картки доступу, біометричні

сканери, мобільні додатки та інші методи для забезпечення надійного контролю доступу.

1.7 Постановка завдання

Розробити надійну та ефективну систему контролю доступу, яка базуватиметься на мікроконтролері Atmega 328P, забезпечуючи контроль доступу до об'єктів з мінімальними витратами та високою надійністю.

Основні функції:

– зчитування та перевірка інформації для ідентифікації користувача (PIN-код, біометричні дані тощо);

– порівняння збереженої інформації з введеною для визначення правильності доступу;

– керування відкриттям або закриттям замка в залежності від результату перевірки.

Функціональні вимоги:

– можливість зберігання та керування базою даних доступу;

– підтримка різних методів ідентифікації (PIN-коди, біометричні дані, RFID-картки тощо);

– відстеження та журналювання подій доступу (успішні та неуспішні спроби входу).

Технічні вимоги:

– використання мікроконтролера Atmega 328P або сумісного мікроконтролера;

– підтримка необхідних сенсорів або модулів зв'язку для взаємодії з користувачем та замком;

– компактний та надійний дизайн системи.

План реалізації:

– проектування схеми системи та вибір необхідних компонентів;

– написання програмного забезпечення для мікроконтролера з використанням мови програмування C або Arduino;

– виконання зборки та тестування прототипу системи;

– вдосконалення та оптимізація системи на основі отриманих результатів тестування.

1.8 Висновки. Постановка задачі

У першому розділі було проведено аналіз методів ідентифікації доступу, а саме парольної ідентифікації та апаратної ідентифікації.

Парольна ідентифікація є найпоширенішим методом ідентифікації доступу, який використовує паролі або ПІН-коди для перевірки ідентичності користувача. Однак, цей метод має свої недоліки, такі як можливість вгадування або вкрадення пароля.

Апаратна ідентифікація є більш надійним методом ідентифікації доступу, який використовує фізичні пристрої, такі як електронні ключі, штрих-коди, RFID або NFC технології. Цей метод забезпечує високий рівень безпеки та зручності використання, але має свої обмеження, такі як можливість крадіжки або підробки фізичних пристроїв.

Також у першому розділі було розглянуто огляд відомих систем контролю доступу, які використовуються в різних сферах, таких як офіси, готелі, промислові підприємства та інші.

На основі проведеного аналізу, було визначено постановку завдання для розробки надійної та ефективної системи контролю доступу, яка базуватиметься на мікроконтролері Atmega 328P, забезпечуючи контроль доступу до об'єктів з мінімальними витратами та високою надійністю.

В цілому, перший розділ дозволив зробити висновок про необхідність розробки надійної та ефективної системи контролю доступу, яка забезпечить високий рівень безпеки та зручності використання.

2 ПРОЄКТУВАННЯ МІКРОКОНТРОЛЕРНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

2.1 Розроблення структури мікроконтролерної системи

Розроблення структури мікроконтролерної системи потребує ретельного планування. Метою є створення ефективної та функціональної системи, яка може взаємодіяти з різними електронними пристроями для виконання конкретних завдань.

– визначення вимог: першим кроком є визначення функціональних вимог до системи. Це включає визначення, які завдання система повинна виконувати, які сигнали вона повинна обробляти, і які дії вона повинна виконувати відповідно до цих сигналів;

– вибір мікроконтролера: після визначення вимог до системи необхідно вибрати мікроконтролер, який найкраще відповідає цим вимогам. Вибір мікроконтролера залежить від багатьох факторів, таких як потужність обчислення, кількість вхідних/вихідних портів, споживана потужність, вартість тощо.

– складання блок-схеми системи: потрібно створити блок-схему системи, що показує взаємозв'язок між різними компонентами системи, такими як мікроконтролер, сенсори, актуатори та інші електронні пристрої;

– планування вхідних/вихідних портів: визначити, які вхідні та вихідні порти мікроконтролера будуть використані для зв'язку зі сенсорами, актуаторами та іншими пристроями;

– розроблення програмного забезпечення: створити програмне забезпечення для мікроконтролера, яке відповідає вимогам системи. Це може включати написання коду для зчитування даних з сенсорів, обробки цих даних та керування актуаторами;

– тестування та налагодження: після написання програмного забезпечення виконати тестування системи, щоб переконатися, що вона працює

правильно. Виправити будь-які помилки та налагодити систему, якщо це необхідно;

– документування: необхідно документувати мікроконтролерну систему, включаючи схеми з'єднань, опис вхідних та вихідних сигналів, а також програмний код. Це допоможе іншим розробникам або нам у майбутньому розуміти та модифікувати систему.

На рисунок 2.1 представлено структурну схему мікроконтролерної системи.

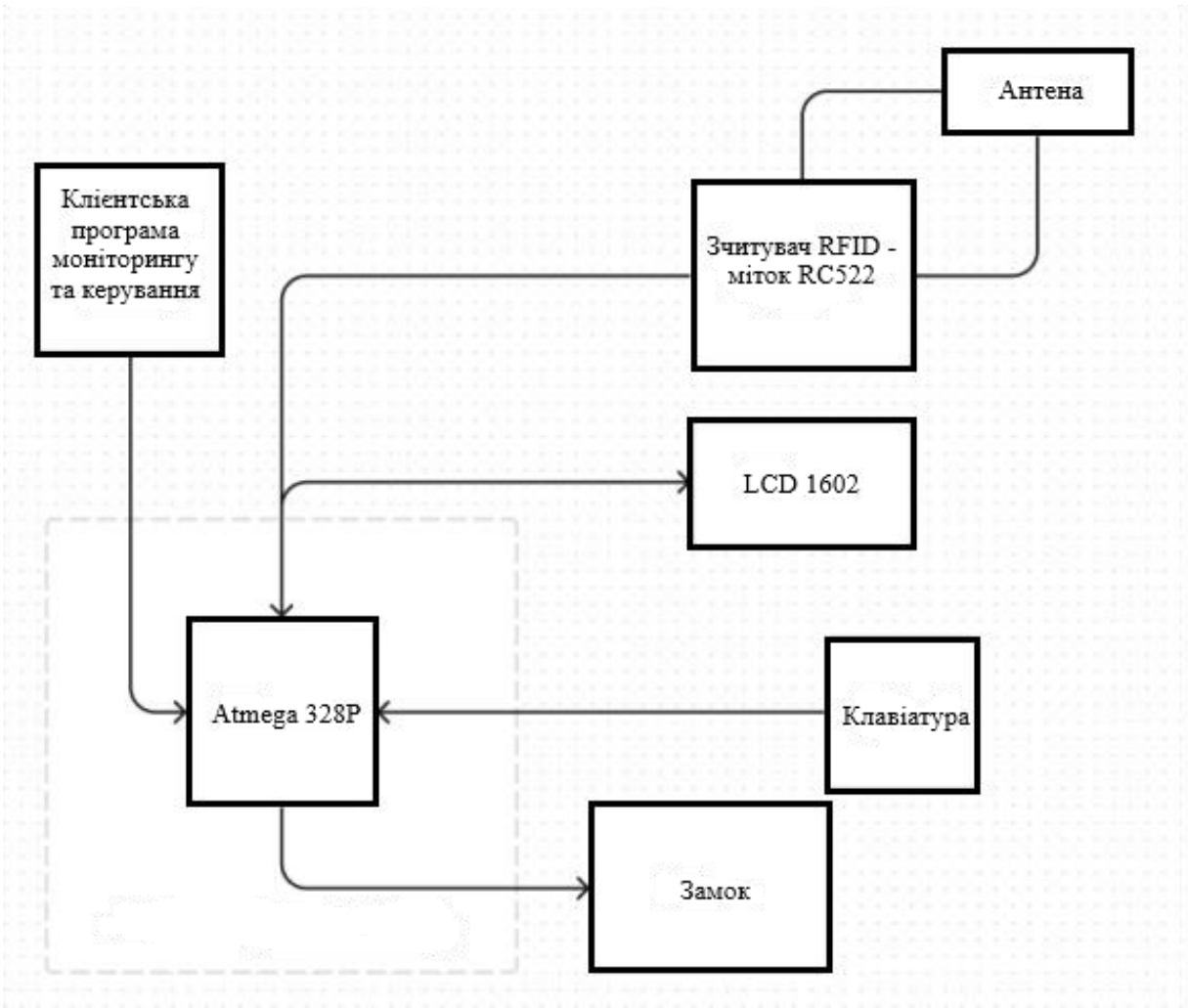


Рисунок 2.1 — Структурна схема мікроконтролерної системи

Структурна схема містить у собі основні компоненти, такі як: керуючий мікроконтролер, замок, клавіатура, зчитувач RFID-міток, антена, цифровий дисплей. Дана схема забезпечить інтегровану роботу всіх елементів для надійного контролю доступу.

2.2 Функціональне призначення основних модулів системи

В сучасному світі вбудовані системи стають все більш поширеними та важливими для нашого повсякденного життя. Вони знаходять застосування у різних галузях, від автомобілебудування до медичних пристроїв, від побутових пристроїв до індустріальних систем [9]. Розробка та впровадження таких систем потребує глибокого розуміння принципів їхньої роботи та структури:

а) мікроконтролерний модуль:

1) забезпечує керування та обробку даних усією системою;

2) виконує взаємодію зі сенсорами та актуаторами;

3) керує вхідними/вихідними портами для обміну даними з іншими модулями та пристроями;

б) сенсорний модуль:

1) отримує дані з датчиків (температури, вологості, тиску тощо;

2) передає ці дані мікроконтролерному модулю для подальшої обробки;

в) актуаторний модуль:

1) отримує команди від мікроконтролерного модуля для виконання певних дій (наприклад, включення/вимкнення пристроїв, регулювання параметрів тощо) ;

г) інтерфейсний модуль:

1) забезпечує зв'язок між системою та користувачем;

2) може включати сенсорний екран, кнопки, світлодіоди для відображення статусу тощо;

д) живлення та управління живленням:

1) забезпечує живлення всієї системи;

2) може містити блок живлення, акумулятор, систему управління енергоспоживанням;

е) комунікаційний модуль:

1) забезпечує зв'язок між системою та іншими пристроями чи мережами (наприклад, Wi-Fi, Bluetooth, Zigbee);

2) дозволяє передавати дані на віддалені сервери або приймати команди від зовнішніх джерел;

ж) модуль обробки даних:

1) виконує обробку отриманих від сенсорів даних для винесення рішень або аналізу;

2) може включати в себе алгоритми обробки сигналів, штучний інтелект тощо.

2.3 Вибір апаратних модулів мікроконтролерної системи

У розробці будь-якої мікроконтролерної системи вибір апаратних модулів є критичним етапом, що визначає можливості та функціональність системи. Кожен модуль повинен бути узгодженим з потребами проекту та забезпечувати необхідні можливості для виконання завдань.

Аналіз вимог системи.

Першим кроком є ретельний аналіз вимог до системи. Це включає визначення функціональних та технічних вимог, кількість та тип сенсорів, актуаторів, зв'язків та інтерфейсів.

Вибір мікроконтролера.

Один з найважливіших апаратних модулів - мікроконтролер. Вибір мікроконтролера залежить від потреб системи у потужності обчислення, кількості та типів вхідно-вихідних портів, енергоефективності та інших факторів.

Сенсори та актуатори.

На основі аналізу вимог обираються сенсори та актуатори, які найкраще підходять для системи. Наприклад, датчики температури, вологості, руху тощо.

Засоби зв'язку.

Для взаємодії з іншими пристроями чи мережами вибираються засоби зв'язку, такі як Wi-Fi, Bluetooth, Zigbee.

Живлення.

Обираються блоки живлення та системи управління енергоспоживанням, які забезпечать стабільну роботу системи та продовжать термін служби.

Інтерфейси.

Враховуючи потреби користувача, обираються зручні та ефективні інтерфейси для взаємодії з системою, такі як сенсорний екран, кнопки, світлодіоди тощо.

2.3.1. Вибір мікроконтролера Atmega 328P

Мікроконтролер Atmega328P (рисунок 2.2) має переваги над своїми аналогами, завдяки своїм зручним функціям та доступній ціні [10].

Рисунок 2.2 — Мікроконтролер Atmega328P

Основні характеристики мікроконтролера Atmega328P:

– широкий функціонал: Atmega328P має достатньо потужний набір функцій, який включає в себе велику кількість вхідних/вихідних портів, аналогові входи, таймери, засоби зв'язку і багато іншого. Це дозволяє реалізувати різноманітні завдання без необхідності використання додаткових пристроїв;

– підтримка широкого спектру пристроїв: Atmega328P є популярним мікроконтролером, який підтримується багатьма різними платформами та середовищами розробки, такими як Arduino IDE, PlatformIO, AVR Studio тощо. Це дозволяє легко розпочати роботу з ним та отримати підтримку від широкого співтовариства розробників;

– низька вартість та доступність: Atmega328P є досить дешевим мікроконтролером, який доступний для широкого кола розробників. Це робить його відмінним вибором для проектів з обмеженим бюджетом або для тих, хто тільки починає свій шлях у вбудованих системах;

– ефективність: Atmega328P має низьке споживання енергії, що робить його ідеальним вибором для проектів, які потребують довготривалого живлення від батареї або акумулятора.

Atmega328P завдяки своїй ціні, простоті використання та надійності у вбудованих системах є хорошим бюджетним варіантом.для проєктування мікроконтролерної системи контролю доступу.

2.3.2. Вибір модуля зчитувача RFID міток RC522

Модуль зчитувача RFID міток RC522 (рисунок 2.3) - це хороший вибір для мікроконтролерної системи доступу, що вимагає ідентифікації за допомогою RFID-технологій [11].

Рисунок 2.3 — Модуль зчитувача RFID міток RC522

Основні характеристики даного модуля:

– широкий функціонал: модуль RC522 може зчитувати та записувати дані на RFID-мітки з різними стандартами, включаючи мітки з частотою 13,56 МГц. Він підтримує різні типи міток, такі як MIFARE Classic, MIFARE Ultralight, NTAG і багато інших;

– простота використання: модуль RC522 має простий інтерфейс з підтримкою SPI, що робить його досить простим у підключенні та використанні з багатьма мікроконтролерами;

– доступність та вартість: цей модуль є досить доступним та широко доступним на ринку, що робить його відмінним вибором для проектів з обмеженим бюджетом або для початківців;

– підтримка спільноти розробників: модуль RC522 отримав значну підтримку від спільноти розробників, що означає наявність багатьох ресурсів, документації та прикладів коду, які можна знайти в Інтернеті;

– надійність та продуктивність: модуль RC522 відомий своєю надійністю та доброю продуктивністю, що робить його популярним вибором для різних застосувань, від контролю доступу до систем відстеження інвентарю.

Загалом, модуль зчитувача RFID міток RC522 є гарним вибором для мікроконтролерної системи контролю доступу, через його простоту використання, доступність та надійність роботи.

2.3.3. Вибір LCD-дисплею 1602A

LCD-дисплей 1602A (рисунок 2.4) - дисплей, що гарно себе зарекомендував під час роботи. Дозволяє провести швидке підключення до мікроконтролерної системи та відображати спеціальні користувацькі символи [12].

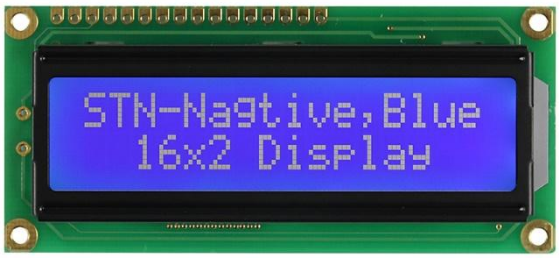


Рисунок 2.4 — LCD-дисплей 1602A

Переваги даного LCD-дисплею :

– розмір та роздільна здатність: дисплей 1602A має розмір 16 символів на 2 рядки, що забезпечує достатньо місця для відображення тексту. Його роздільна здатність дозволяє відображати достатньо інформації для більшості додатків;

– простота використання: LCD-дисплей 1602A має простий інтерфейс з підтримкою паралельного з'єднання з мікроконтролером. Це робить його легко підключити та використовувати в проектах;

– низька вартість: даний дисплей доступний за доступною ціною, що робить його відмінним вибором для проектів з обмеженим бюджетом;

– доступність ресурсів: багато документації, прикладів коду та бібліотек доступно для роботи з LCD-дисплеєм 1602A. Це дозволяє легко знайти необхідні ресурси для використання в проекті;

– надійність: LCD-дисплей 1602A відомий своєю надійністю та довговічністю, що робить його відмінним вибором для проектів, які потребують стабільного відображення інформації.

Через свою простоту використання, доступність та надійність, LCD-дисплей 1602A є відмінним вибором для текстового відображення інформації.

2.3.4. Вибір електронного замка LY-4010

У світі, насиченому технологіями, забезпечення безпеки та контролю доступу стає дедалі важливішим завданням [13]. Електронні замки, такі як LY-

4010 (рисунок 2.5), стають невід'ємною частиною цього процесу, пропонуючи надійний та сучасний спосіб захисту приміщень, об'єктів та інформації.

Рисунок 2.5 — Електронний замок LY-4010

Ключові характеристики та переваги електронного замка LY-4010:

– безпека та надійність: електронний замок LY-4010 відомий своєю високою безпекою та надійністю. він забезпечує контроль доступу за допомогою електронних ключів або кодів, що робить його відмінним вибором для захисту важливих приміщень або об'єктів;

– простота установки: електронний замок LY-4010 має простий інтерфейс та може бути легко встановлений на двері або інші поверхні за допомогою стандартних інструментів;

– різноманітність методів відкривання: замок підтримує різні методи відкривання, такі як за допомогою електронних ключів RFID, біометричних сканерів відбитків пальців або кодів доступу. Це дозволяє вибрати найбільш зручний метод для конкретного проекту;

– додаткові функції безпеки: електронний замок LY-4010 може бути додатково обладнаний функціями безпеки, такими як автоматичне блокування після невдалих спроб відкриття або відслідковування історії відкривання;

– доступність та ціна: електронний замок LY-4010 доступний за доступною ціною, що робить його відмінним вибором для проектів з обмеженим бюджетом.

Безпека, простота встановлення та доступність роблять електронний замок LY-4010 популярним серед розробників та користувачів.

2.3.5. Вибір модулів звукової і світлової сигналізації

Коли вибираються модулі звукової та світлової сигналізації, спочатку звертається увага на вимоги проекту. Різні характеристики досліджуються з огляду на їх вплив на ефективність та функціональність модулів[14]. При цьому враховуються потреби користувачів та специфіка середовища, в якому система буде використовуватися.

Основна увага приділяється гучності та якості звуку. Пошук модулів, що можуть забезпечити достатньо високий рівень гучності без втрати якості звуку. Переконуються, що модулі підтримують різноманітність методів відтворення звуку для вибору найбільш підходящого для проекту.

Далі звертається увага на світлову потужність та видимість. Шукаються модулі, що забезпечують достатньо яскраве світло та широкий кут огляду, щоб вони були видимі з різних точок приміщення. Також вивчається можливість наявності різних кольорів світлодіодів або можливість миготіння для різних сигналів.

Під час вибору модулів зважається на їхню надійність та довговічність. Перевіряється якість матеріалів та конструкції, щоб переконатися, що вони здатні витримати тривале використання без поломок чи збоїв.

Не менш важлива є сумісність обраних модулів з іншими компонентами системи. Переконуються, що вони легко інтегруються з іншими елементами системи безпеки та аварійного сповіщення.

2.3.6. Вибір матричної клавіатури

При виборі матричної клавіатури враховуються кілька ключових аспектів, які визначають її сумісність, зручність використання та надійність у конкретному проекті [15].

Спочатку звертається увага на кількість кнопок, розмір і форму. Обираючи клавіатуру, розглядаються вимоги проекту щодо кількості кнопок та їх розмірів, які повинні відповідати габаритам та дизайну пристрою. Зокрема, для пристроїв з обмеженим простором важливо вибрати компактні клавіатури.

Після цього звертається увага на сумісність інтерфейсу клавіатури з мікроконтролером або іншим пристроєм. Перевіряють, чи підтримує обрана клавіатура необхідний інтерфейс, такий як аналоговий або цифровий, що використовується для зчитування даних.

Далі розглядається надійність та якість матеріалів клавіатури. Вибираються клавіатури від відомих виробників з доброю репутацією, які гарантують тривалу та безпроблемну роботу.

Також враховується ціна клавіатури та здійснюється пошук оптимального балансу між ціною та якістю. Уникаються занадто дешеві варіанти, які можуть мати низьку якість виготовлення та нестабільну роботу.

Нарешті, звертається увага на наявність додаткових функцій у клавіатурі, таких як вбудований LED-підсвітка, індикатори стану або мультимедійні кнопки, та їхню необхідність для конкретного проекту.

Клавіатура має 8 піновий конектор, який поділяє її на 4 стовпці та 4 радки, що дозволяє реалізувати модуль клавіатури із 16 клавішами. Спрацювання клавіш відбувається за рахунок замикання контакту певного стовпця та рядка. Принцип роботи модуля зображений на рисунку 2.6.

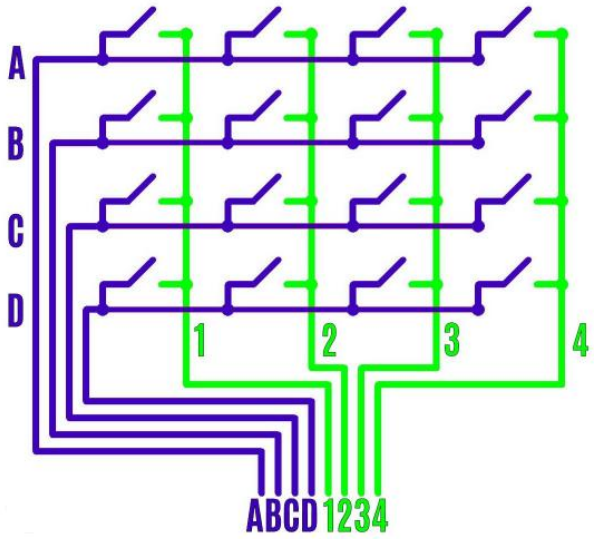


Рисунок 2.6 — Принцип роботи модуля клавіатури

Принцип роботи модуля клавіатури базується на електричній схемі, яка складається з матриці перемикачів, що з'єднують ряди і стовпці [16]. Коли користувач натискає клавішу, замикання контакту між певним рядом і стовпцем створює електричний сигнал. Контролер клавіатури, розташований всередині модуля, постійно сканує цю матрицю, виявляючи зміни в стані перемикачів. Сканування здійснюється з високою частотою для забезпечення миттєвої реакції на натискання клавіш. Коли контролер визначає, яка клавіша натиснута, він генерує відповідний код сканування, який надсилається до центрального процесора комп'ютера. Цей код обробляється програмним забезпеченням, яке інтерпретує його як певний символ або команду, що потім відображається на екрані або виконується системою. Таким чином, модуль клавіатури перетворює механічні дії користувача на електронні сигнали, які комп'ютер може розпізнати та обробити.

2.3.7. Вибір модуля реле

При виборі модуля реле, спершу звертається увага на тип реле, що відповідає конкретним потребам проекту [17]. Оцінюються різні варіанти, такі як

однополюсний, двополюсний чи потрійний, залежно від конфігурації схеми та вимог пристрою.

Далі аналізується струмова та напругова специфікація. Важливо визначити максимальні значення, які реле може витримати, і порівняти їх із потребами у вашому проекті, щоб уникнути перевантаження чи несправностей.

Також враховується тип керування. Обирають модуль, який сумісний зі сигналами вашого мікроконтролера або іншого пристрою. Це може бути цифрове або аналогове керування, залежно від характеристик використовуваного обладнання.

Надалі розглядається надійність і якість модуля. Перевіряється репутація виробника та його продукції, щоб забезпечити безперебійну роботу системи у вашому проекті.

Не менш важливим є аналіз ціни. Обирається модуль, який відповідає вашому бюджету, але при цьому має прийнятну якість і надійність.

Для управління виконавчим пристроєм можна використати 2-канальний модуль реле TONGLING (рисунок 2.7).

Рисунок 2.7 — Модуль реле TONGLING

2.4 Вибір інтегрованого середовища програмування Arduino IDE

При виборі інтегрованого середовища програмування Arduino IDE, акцент робиться на кількох ключових аспектах, які впливають на зручність та ефективність роботи з ним [18].

Спочатку важливо врахувати доступність та простоту використання середовища.

Обирається таке середовище, яке легко освоюється користувачами будь-якого рівня досвіду та одночасно має достатній функціонал для вирішення завдань різної складності.

Далі уважно розглядаються можливості та функціональність середовища. Обирається таке, яке відповідає потребам проекту та має необхідний набір інструментів для його реалізації.

При цьому важливо, щоб воно підтримувало різні типи мікроконтролерів Arduino, що дозволяє працювати з широким спектром обладнання.

Також враховується підтримка спільноти та наявність документації. Обирається середовище, яке користується популярністю серед розробників, що забезпечує доступність допомоги та ресурсів для вирішення потенційних проблем.

Завершальним етапом є розгляд сумісності середовища з операційною системою та апаратними можливостями.

Обирається програмне забезпечення, яке ефективно взаємодіє з доступним обладнанням та підтримується на різних платформах операційних систем.

Враховуючи ці аспекти, можна зробити обґрунтований вибір Arduino IDE, що найкраще відповідає нашим потребам та гарантує успішну реалізацію проекту

2.5 Вибір середовища розробки функціоналу системи Fritzing

При виборі середовища розробки для створення функціоналу системи, як Fritzing, акцент робиться на кількох ключових аспектах, які впливають на зручність, ефективність та якість роботи з ним [19].

Початково, звертається увага на інтерфейс та доступність.

Обирається середовище, яке має зрозумілий та легкий для освоєння інтерфейс, що сприяє швидкому розгортанню проектів навіть для новачків у сфері розробки електроніки.

Далі аналізується функціональність та можливості. Обирається середовище, яке надає широкий набір інструментів для моделювання схем, розробки плат та програмування мікроконтролерів, що забезпечує повний цикл розробки в одному інструменті.

Також враховується підтримка спільноти та наявність допомоги. Обирається середовище, яке користується популярністю серед розробників та має активну спільноту, яка готова надавати поради та допомогу у вирішенні технічних питань.

Завершальним етапом є розгляд сумісності інструменту з власними потребами та можливостями.

Обирається середовище, яке підтримує роботу з різними мікроконтролерами та елементами, необхідними для вашого проекту.

Враховуючи ці аспекти, можна зробити обґрунтований вибір середовища Fritzing.

При виборі компонентів та інструментів для розробки електронної системи ключовою було орієнтовано на досягнення успішного результату [20]. Кожен вибір був уважно обдуманим і здійснювався з урахуванням специфічних потреб та вимог проекту.

Зокрема, під час вибору мікроконтролера та інших компонентів було враховано їхню сумісність, функціональність та надійність. Вибір інтегрованого середовища розробки базувався на зручності використання, наявності необхідних інструментів та підтримці спільноти.

На рисунку 2.8 представлено вигляд інтерфейсу програми Fritzing.

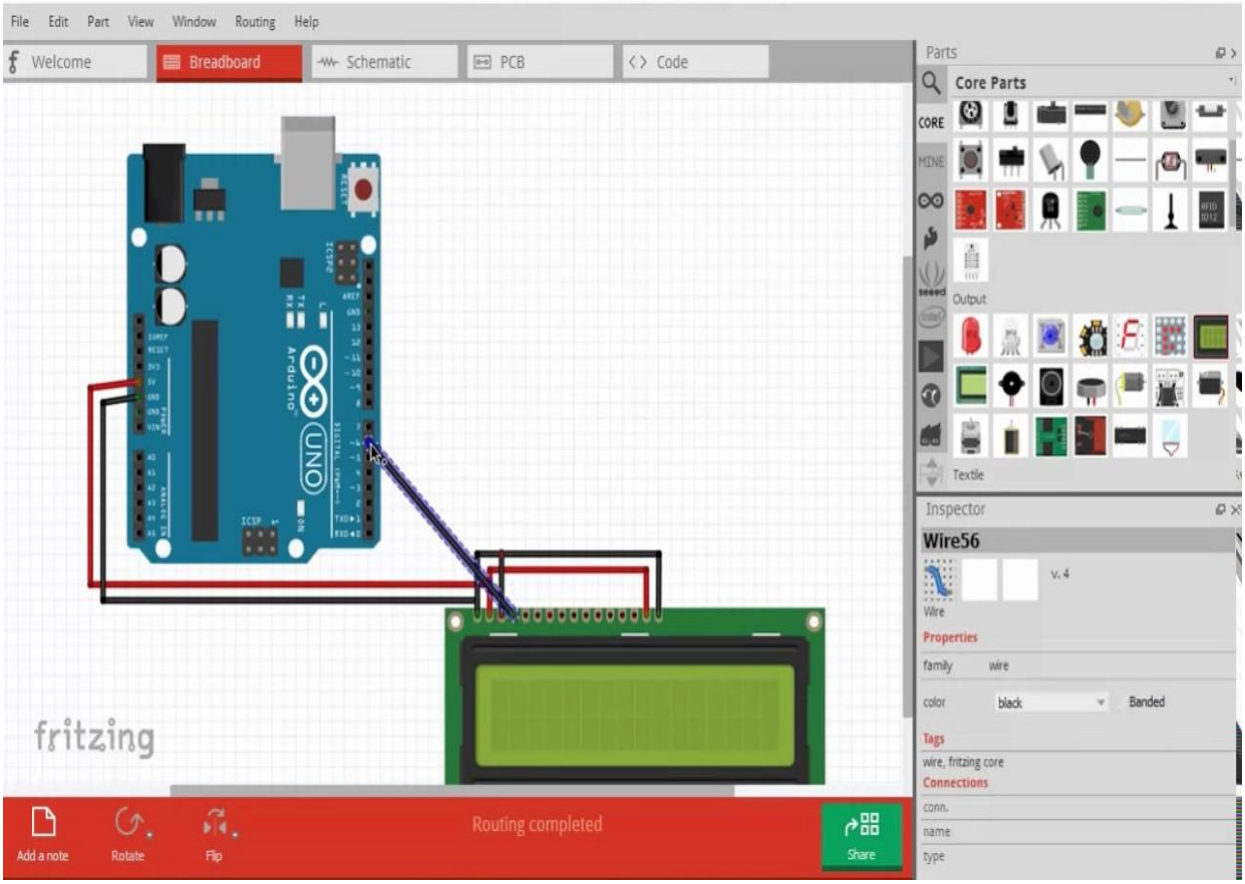


Рисунок 2.8 — Інтерфейс програми Fritzing

Вигляд програми включає кілька основних компонентів. Головне меню розташоване вгорі і містить основні команди для роботи з проектом, такі як створення нового, відкриття, збереження та експорт. Під головним меню знаходиться панель інструментів, яка забезпечує швидкий доступ до таких функцій, як вибір інструмента, з'єднання компонентів, редагування та масштабування. Центральна частина програми, або робоча область, поділена на три основні вкладки: Breadboard (макетна плата), Schematic (схема) та PCB (друкована плата). У вкладці Breadboard відображається візуальне представлення макетної плати, де можна розміщувати компоненти та проводити з'єднання. У вкладці Schematic користувачі можуть створювати графічні представлення електричних схем, малюючи з'єднання між компонентами у вигляді схеми. У вкладці PCB представлено вигляд друкованої плати, де можна проектувати та розташовувати компоненти на друкованій платі для подальшого виготовлення.

2.6 Висновки

Кожен компонент був обраний з урахуванням його можливостей та сумісності з іншими елементами системи, що забезпечило гармонійну роботу всього проекту.

Весь процес вибору компонентів та інструментів був спрямований на максимально ефективне та надійне втілення задуманої електронної системи.

І завдяки обґрунтованому підходу до кожного вибору, було досягнуто успішного результату в розробці системи, яка відповідає поставленим вимогам і задовольняє потреби користувачів.

Отже:

– вибір мікроконтролера та інших компонентів системи (таких як модулі RFID, LCD-дисплеї, електронні замки тощо) здійснювався з урахуванням їх функціональності та сумісності з проектом;

– вибір інтегрованого середовища розробки (наприклад, Arduino IDE або Fritzing) проводився з урахуванням доступності, зручності та функціональності для реалізації поставлених завдань;

– при виборі кожного компонента або інструменту враховувалися такі аспекти, як надійність, підтримка спільноти, документація та сумісність з іншими елементами системи.

У цілому, кожен вибір був обґрунтованим та спрямованим на досягнення успішного результату в розробці електронної системи.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ МІКРОКОНТРОЛЕРНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1. Розроблення функціональної схеми мікроконтролерної системи

Функціональна схема мікроконтролерної системи є ключовим елементом у процесі розробки. Вона допомагає визначити взаємозв'язки між різними компонентами та підсистемами, а також забезпечує базову структуру для подальшого розвитку системи. Нижче наведено розширений опис кроків для розробки функціональної схеми мікроконтролерної системи контролю доступу:

– визначення вхідних та вихідних сигналів: першим кроком є детальний аналіз вхідних та вихідних сигналів, які будуть оброблятися мікроконтролером [21]. У нашому випадку, вхідними сигналами є дані з RFID-читача, клавіатури та датчика руху, а вихідними сигналами є керування електронним замком, індикатором стану та звуковим сигналом. Крім того, слід враховувати додаткові сигнали, такі як живлення, сигнали синхронізації та інші;

– визначення підсистем: наступним кроком є визначення підсистем, які будуть складатися з різних компонентів та виконувати певні функції [22]. У нашому випадку, підсистеми включають RFID-читач, клавіатуру, датчик руху, електронний замок, індикатор стану та звуковий сигнал. Однак, можуть бути визначені додаткові підсистеми, такі як підсистема живлення, підсистема зв'язку та інші, в залежності від конкретних вимог проекту;

– розробка блок-схеми: після визначення вхідних/вихідних сигналів та підсистем, можна розпочати розробку блок-схеми [23]. Блок-схема є графічним представленням функціональної схеми, яке показує взаємозв'язки між підсистемами та мікроконтролером. У блок-схемі повинні бути вказані всі підсистеми, їхні входи/виходи та з'єднання з мікроконтролером. Крім того, слід враховувати додаткові елементи, такі як джерела живлення, фільтри, підсилювачі та інші, необхідні для коректної роботи системи;

– розробка діаграми станів: діаграма станів є графічним представленням поведінки системи в різних станах [24]. У нашому випадку, система може знаходитися в станах "очікування", "ідентифікація", "відкриття двері" та "закриття двері". Діаграма станів допомагає визначити, які дії повинні виконуватися в кожному стані та як переходити між станами. Крім того, слід враховувати додаткові стани, такі як "аварійне закриття", "несанкціонований доступ" та інші, в залежності від конкретних вимог проекту;

– розробка алгоритмів: після розробки діаграми станів, можна розпочати розробку алгоритмів для кожної з підсистем [25]. Алгоритми повинні враховувати входи/виходи підсистем та дії, які повинні виконуватися в кожному стані. Крім того, слід враховувати додаткові алгоритми, такі як алгоритми фільтрації сигналів, алгоритми шифрування даних та інші, необхідні для коректної роботи системи;

– тестування та відлагодження: після розробки функціональної схеми, необхідно провести тестування та відлагодження для виявлення та виправлення помилок [26]. Тестування може включати в себе перевірку роботи кожної з підсистем, перевірку взаємодії між підсистемами та перевірку роботи системи в різних станах. Крім того, слід провести тестування на стійкість до зовнішніх впливів, таких як електромагнітні поля, температурні коливання та інші.

Після завершення розробки функціональної схеми, можна перейти до наступного етапу - розробки електричної схеми та програмування мікроконтролера.

На рисунку 3.1 представлено функціональну схему мікроконтролерної системи.

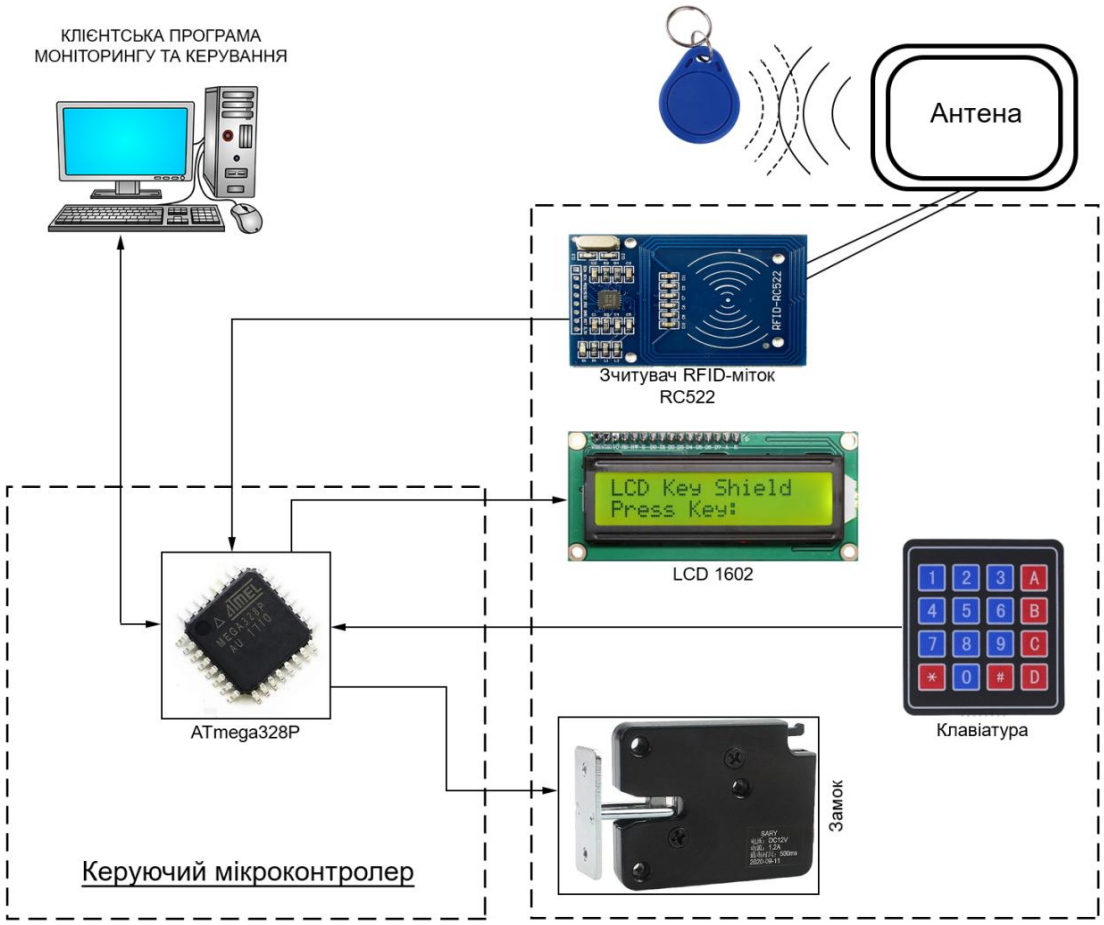


Рисунок 3.1 — Функціональна схема мікроконтролерної системи

Функціональна схема мікроконтролерної системи контролю доступу включає кілька основних компонентів, що взаємодіють для забезпечення надійної роботи системи. Центральним елементом є мікроконтролер, який керує всіма іншими компонентами. RFID-модуль здійснює зчитування даних з RFID-карт для ідентифікації користувача [27]. Матрична клавіатура дозволяє вводити PIN-коди або інші дані для додаткової аутентифікації. Дані, зчитані RFID-модулем та введені через клавіатуру, обробляються мікроконтролером, який порівнює їх з інформацією в базі даних. Результати аутентифікації відображаються на LCD-дисплеї, що дозволяє користувачам бачити статус доступу.

Якщо аутентифікація успішна, мікроконтролер активує модуль реле, який, у свою чергу, розблоковує електронний замок, дозволяючи доступ. Для підвищення

рівня безпеки та інформативності система оснащена модулями звукової та світлової сигналізації, які повідомляють про успішну або невдалу спробу доступу. Усі компоненти системи живляться від централізованого блоку живлення, що забезпечує стабільну роботу всієї системи. Така функціональна схема забезпечує комплексний підхід до контролю доступу, поєднуючи різні методи аутентифікації та зворотного зв'язку з користувачем.

3.2. Розроблення електричної-принципової схеми мікроконтролерної системи

Після розроблення функціональної схеми, необхідно розробити електричну-принципову схему мікроконтролерної системи контролю доступу [28]. Електрична схема допомагає визначити, як будуть підключені всі компоненти та пристрої до мікроконтролера, а також як буде живитися система.

Електрична схема повинна включати всі необхідні компоненти, такі як:

– мікроконтролер;
– rfid-модуль;
– електронний замок;
– lcd-дисплей;
– модулі звукової та світлової сигналізації;
– модуль реле;
– живлення;
– з'єднання між компонентами.

Для розробки електричної схеми необхідно:

– вибрати відповідні компоненти та пристрої для підключення до мікроконтролера;
– визначити, як будуть підключені компоненти до мікроконтролера. Для цього необхідно визначити, які порти мікроконтролера будуть використовуватися для з'єднання з кожним компонентом;

– визначити, як буде живитися система. Для цього необхідно вибрати джерело живлення та визначити, як воно буде підключене до системи [29];

– створити схему з'єднань між компонентами. Схема повинна включати всі необхідні деталі, такі як тип з'єднання, напрямок сигналу та інші важливі параметри;

– перевірити схему на наявність помилок та неточностей. Для цього необхідно перевірити, чи всі компоненти підключені вірно та чи відповідають вони вимогам функціональної схеми [30];

– схему необхідно протестувати на практиці, під'єднавши всі компоненти відповідно до схеми та перевіривши їх роботу.

При розробці електричної схеми необхідно дотримуватися всіх вимог безпеки та правил електротехніки. Також необхідно враховувати особливості роботи мікроконтролера та підключених до нього компонентів.

На рисунку 3.2 представлено електрично-принципову схему мікроконтролерної системи контролю доступу.

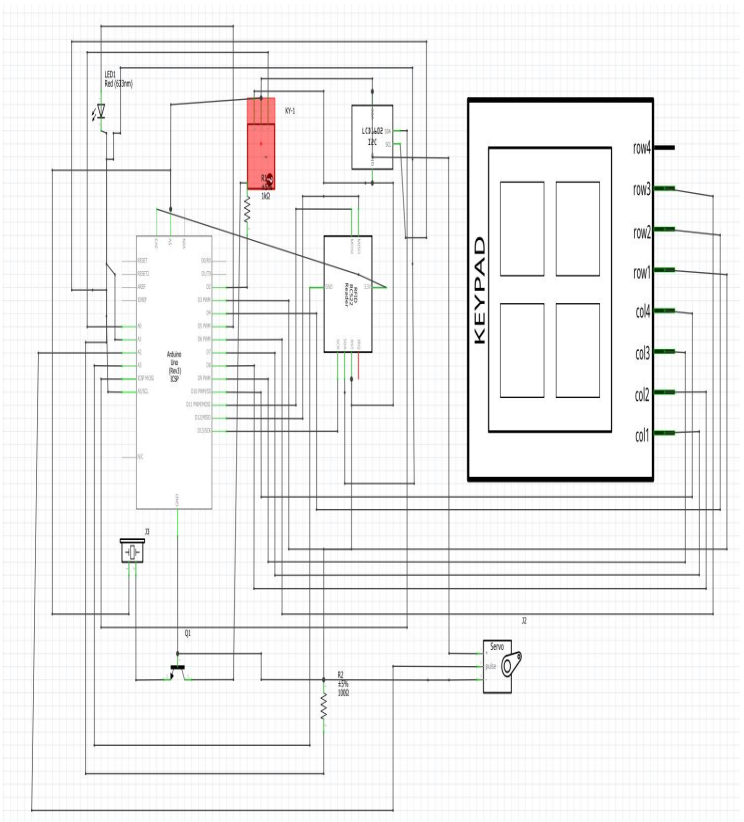


Рисунок 3.2 — Електрично-принципова схема мікроконтролерної системи контролю доступу

Після розробки та перевірки електричної схеми, можна перейти до наступного етапу - розробки програмного забезпечення для мікроконтролера.

3.2.1. Під’єднання до мікроконтролерної плати RFID-модуля

RFID-модуль є одним з ключових компонентів системи контролю доступу, оскільки він дозволяє ідентифікувати користувачів за допомогою RFID-карт.

Спочатку потрібно визначити тип RFID-модуля та його специфікації, оскільки існують різні типи модулів, такі як RC522, PN532 тощо, які можуть мати різні інтерфейси та методи підключення [31].

Потім необхідно підключити модуль до мікроконтролера. Зазвичай для цього використовуються SPI (Serial Peripheral Interface) або I2C (Inter-Integrated Circuit) інтерфейси. Для підключення по SPI зазвичай використовуються піни для передачі даних (MISO, MOSI), клоку (SCK), а також піни SS (Slave Select) та RST (Reset). Для підключення по I2C використовуються піни SDA (Serial Data) та SCL (Serial Clock).

Після підключення модуля до мікроконтролера необхідно встановити відповідний драйвер або бібліотеку для взаємодії з RFID-модулем. Для Arduino це може бути бібліотека MFRC522 для модуля RC522 або Adafruit PN532 для модуля PN532. Після встановлення бібліотеки необхідно ініціалізувати модуль та налаштувати його параметри за допомогою відповідних функцій чи методів [32].

Останнім етапом є написання програмного коду для обробки інформації, отриманої від RFID-модуля. Це може включати зчитування та ідентифікацію RFID тегів, перевірку їхньої валідності та виконання відповідних дій, наприклад, відкриття дверей або виконання інших функцій контролю доступу.

Отже, для підключення RFID-модуля до мікроконтролерної плати необхідно виконати наступні кроки:

– визначити тип RFID-модуля, який буде використовуватися в системі;

– перевірити, чи відповідає RFID-модуль вимогам системи контролю доступу;

– з'єднати RFID-модуль з мікроконтролерною платою за допомогою відповідних проводів;

– перевірити правильність підключення RFID-модуля до мікроконтролерної плати;

– налаштувати RFID-модуль для роботи з мікроконтролером;

– перевірити працездатність RFID-модуля;

– після завершення підключення виконати налаштування програмного забезпечення мікроконтролера для коректної взаємодії з RFID-модулем. Це може включати ініціалізацію портів вводу-виводу, налаштування протоколів передачі даних та реалізацію функцій для зчитування та обробки даних з RFID-міток;

– при налаштуванні програмного забезпечення врахувати особливості використовуваного RFID-модуля, такі як підтримувані типи міток, формат даних, швидкість передачі тощо [33].

На рисунку 3.3 зображене з’єднання RFID-модуля із платою Arduino UNO. Також для успішного підключення модуля необхідно попередньо підключити бібліотеку MFRC522.h, після чого, за допомогою директиви #define, перед компіляцією, присвоїти ім’я RST_PIN константі 9 та SS_PIN константі 10, це означає, що лінія скидання підключена до 9 контакту на платі Arduino, а вибір веденого до 10. Тобто, будь-яка згадка RST_PIN в коді буде замінена константою 9 під час компіляції. Це буде мати наступний вигляд:

```
#define RST_PIN 9
#define SS_PIN 10
```

Далі за допомогою бібліотеки MFRC522.h створюється екземпляр об’єкту MFRC522:

```
MFRC522 mfrc522(SS_PIN, RST_PIN);
```

Після чого у функції void setup() виконується ініціалізація MFRC522 командами:

```
SPI.begin();
mfrc522.PCD_Init();
```

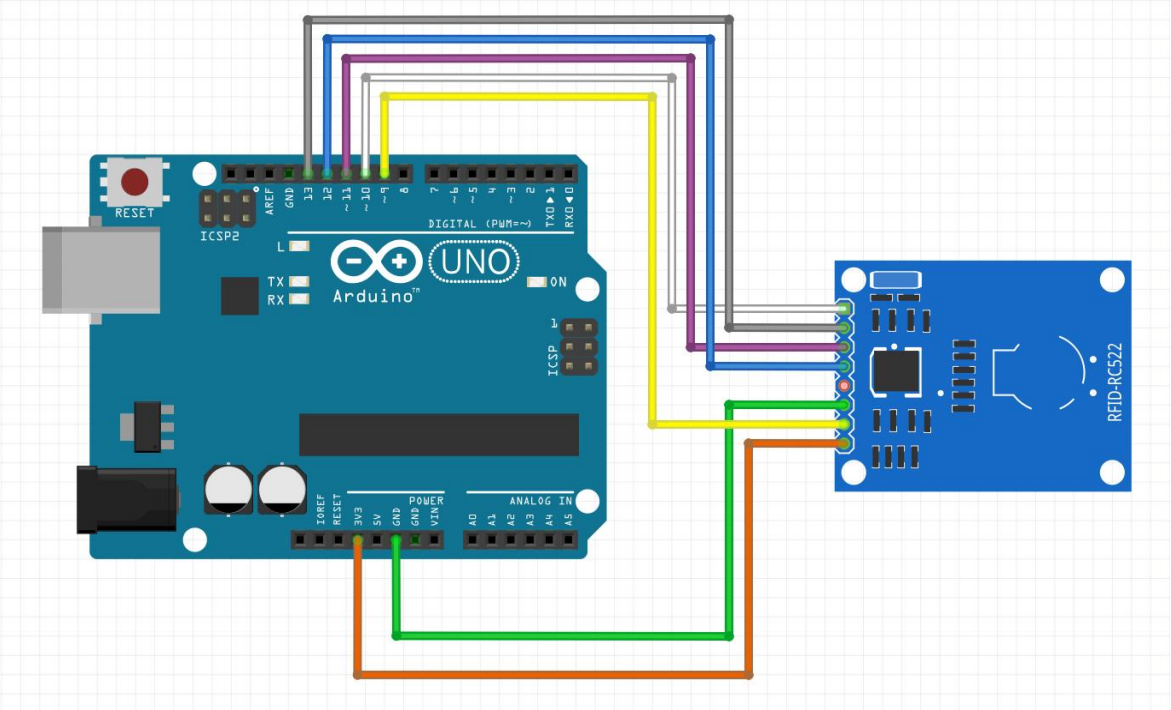


Рисунок 3.3 — Підключення RFID-модуля до плати

3.2.2. Під’єднання до мікроконтролерної плати електронного замка

Електронний замок є ще одним важливим компонентом системи контролю доступу [34]. Для підключення електронного замка до мікроконтролерної плати необхідно виконати наступні кроки:

– визначити тип електронного замка, який буде використовуватися в системі;

– перевірити, чи відповідає електронний замок вимогам системи контролю доступу;

– з'єднати електронний замок з мікроконтролерною платою за допомогою відповідних проводів;

– перевірити правильність підключення електронного замка до мікроконтролерної плати;

– налаштувати електронний замок для роботи з мікроконтролером;

– перевірити працездатність електронного замка;

– залежно від типу електронного замка, може знадобитися додаткове підключення сигналів керування або живлення. Наприклад, для електромагнітних замків потрібно врахувати достатню потужність джерела живлення;

– у програмному забезпеченні передбачити функції для активації/деактивації замка, враховуючи час спрацьовування та безпечне керування.

Процес підключення електронного замка до мікроконтролерної плати Arduino, є досить простим, особливо якщо замок працює з низькими напругами (наприклад, 5V).

Спершу необхідно визначити тип електронного замка, який використовується. Це може бути сольно-механічний замок з електричним управлінням або повноцінний електронний замок [35].

Потім потрібно встановити джерело живлення для замка. Більшість електронних замків працюють з напругою 5V або 12V. Важливо переконатися, що напруга, яку використовує замок, сумісна з мікроконтролером.

Наступним кроком є підключення замка до мікроконтролера. Це може варіюватися в залежності від типу замка, але загальна ідея полягає в тому, щоб мікроконтролер міг вмикати і вимикати замок. Для цього зазвичай використовуються два провідники: один для живлення (позначений червоним або "+"), інший для заземлення (позначений чорним або "-").

Коли мікроконтролер отримує команду відкрити або закрити замок, він вмикає або вимикає потік електричного струму до замка.

На рисунку 3.4 зображене з’єднання RFID-модуля із платою Arduino UNO.

Для успішного підключення модуля небхідно попередньо підключити бібліотеку SolenoidLock.h., після чого, за допомогою директиви #define, перед компіляцією, присвоїти ім’я PIN_GND константі 2.Далі за допомогою бібліотеки SolenoidLock.h створюється екземпляр об’єкту, який має наступний вигляд:

```
#define SOLENOIDLOCK_PIN_GND       2
SolenoidLock solenoidLock(SOLENOIDLOCK_PIN_GND);
```

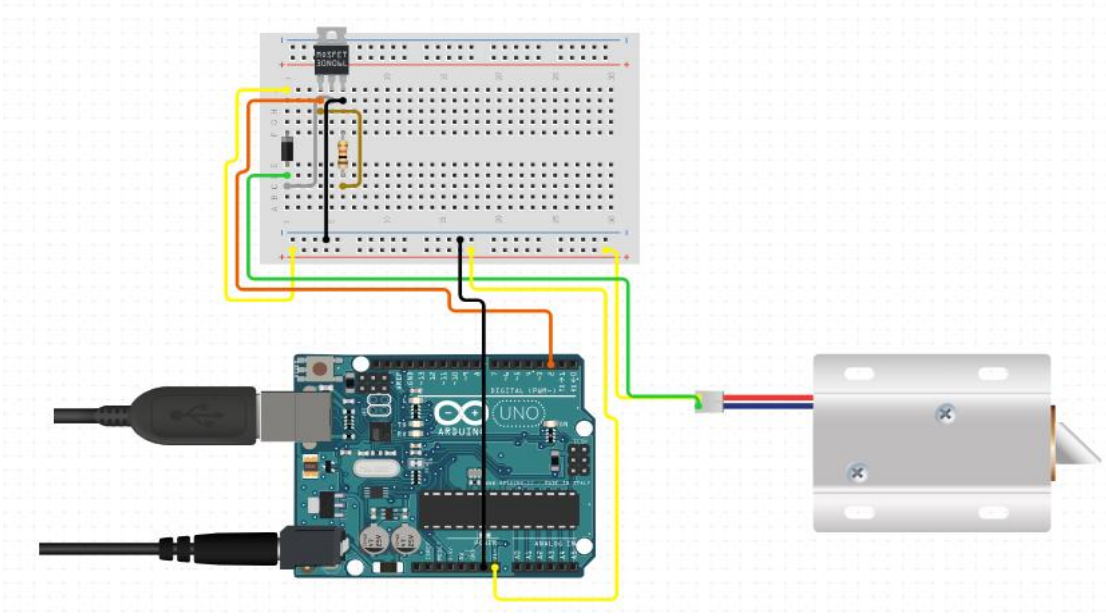


Рисунок 3.4 — Підключення електронного замка до плати

3.2.3. Під’єднання до мікроконтролерної плати LCD-дисплею

LCD-дисплей використовується для відображення інформації про стан системи контролю доступу.

По-перше, потрібно визначити тип LCD-дисплею та його параметри. Зазвичай використовуються дисплеї з розміром 16x2 символи, які мають дві лінії по 16 символів кожна [36].

По-друге, необхідно підключити дисплей до мікроконтролера. Для цього зазвичай використовуються вісім провідників: для живлення, заземлення, керування режимом роботи (RS), зчитування/запису даних (RW), підтвердження (E), та чотири для передачі даних (D4-D7). Всі ці провідники повинні бути підключені до відповідних пінів мікроконтролера.

По-третє, підключення дисплею необхідно встановити відповідну бібліотеку. Для Arduino це може бути бібліотека LiquidCrystal.h. Її необхідно встановити через Arduino IDE.

Останнім етапом є написання програмного коду для відображення інформації на дисплеї. Це включає ініціалізацію дисплею, встановлення режимів роботи, виведення тексту, символів, та інших графічних елементів.

Отже, для підключення LCD-дисплею до мікроконтролерної плати необхідно виконати наступні кроки:

– визначити тип LCD-дисплею, який буде використовуватися в системі [37];

– перевірити, чи відповідає LCD-дисплей вимогам системи контролю доступу;

– з'єднати LCD-дисплей з мікроконтролерною платою за допомогою відповідних проводів [38];

– перевірити правильність підключення LCD-дисплею до мікроконтролерної плати;

– налаштувати LCD-дисплей для роботи з мікроконтролером [39];

– перевірити працездатність LCD-дисплею;

– залежно від розміру та роздільної здатності LCD, може знадобитися оптимізація відображення даних на екрані, використання шрифтів різного розміру або розбиття інформації на декілька екранів;

– передбачити у програмному забезпеченні функції для ініціалізації LCD, виведення тексту, символів та можливо графічних елементів при необхідності.

На рисунку 3.5 зображене з’єднання LCD-дисплею із платою Arduino UNO

Також для успішного підключення модуля необхідно попередньо підключити бібліотеку LiquidCrystal_PCF8574.h після чого, за допомогою директиви #define, перед компіляцією, визначаємо характеристики LCD:

```
#define LCD_ADDRESS 0x3F
#define LCD_ROWS 2
#define LCD_COLUMNS 16
#define SCROLL_DELAY 150
#define BACKLIGHT 255
```

Далі за допомогою бібліотеки проводиться ініціалізація об’єкта

```
LiquidCrystal_PCF8574 lcdI2C;
```

Визначаємо змінні для текстового меню:

```
const int timeout = 10000;
char menuOption = 0;
long time0;
```

Після чого у функції void setup() виконується ініціалізація LiquidCrystal_PCF8574

```
lcdI2C.begin(LCD_COLUMNS, LCD_ROWS, LCD_ADDRESS, BACKLIGHT);
```

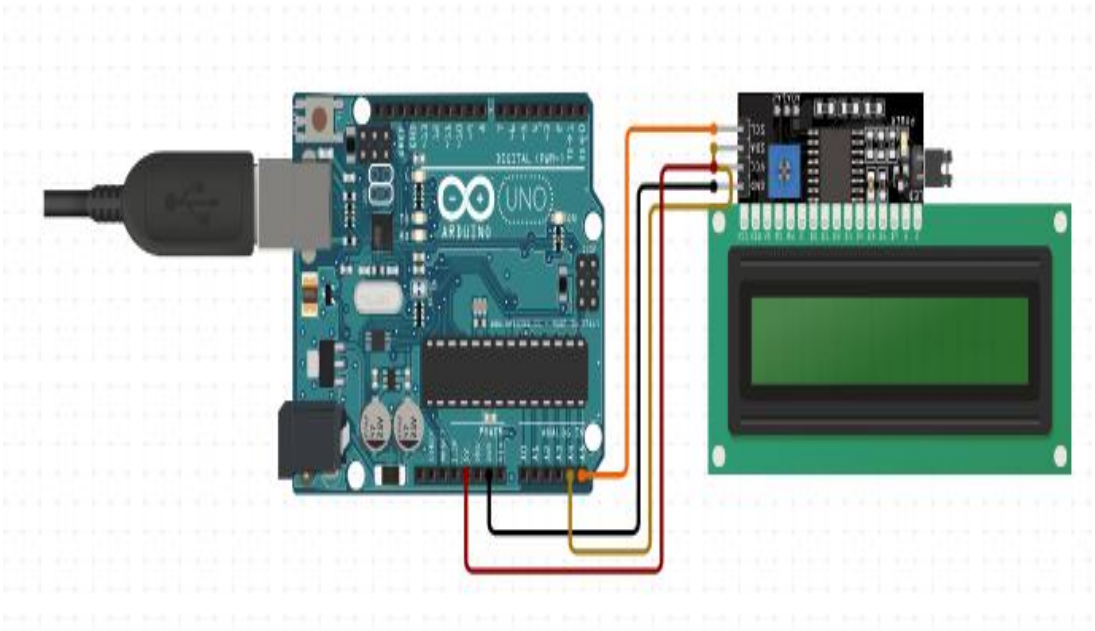


Рисунок 3.5 — Підключення LCD-дисплею до плати

3.2.4 Під’єднання до мікроконтролерної плати модулів звукової і світлової сигналізації

Модулі звукової і світлової сигналізації використовуються для повідомлення користувачів про стан системи контролю доступу [40].

Потрібно визначити тип модулів звукової і світлової сигналізації, які будуть використовуватися для підвищення безпеки системи контролю доступа. Це можуть бути бузери, динаміки або світлодіоди.

Потім, необхідно підключити модулі до плати Arduino UNO. Для цього використовуються відповідні піни(вхід та вихід) пристроїв на платі, що дозволяють керувати звуковими та світловими сигналами.

Перед використанням модулів потрібно перевірити їх технічні характеристики, такі як напруга живлення та електричний струм, щоб переконатися, що вони відповідають можливостям плати Arduino UNO.

Для програмного керування модулями є можливість використати вбудовані функції Arduino або відповідні бібліотеки, які дозволять генерувати звукові сигнали або керувати світловими індикаторами.

Отже, для підключення модулів звукової і світлової сигналізації до мікроконтролерної плати необхідно виконати наступні кроки:

– визначити тип модулів звукової і світлової сигналізації, які будуть використовуватися в системі;

– перевірити, чи відповідають модулі звукової і світлової сигналізації вимогам системи контролю доступу;

– з'єднати модулі звукової і світлової сигналізації з мікроконтролерною платою за допомогою відповідних проводів;

– перевірити правильність підключення модулів звукової і світлової сигналізації до мікроконтролерної плати;

– налаштувати модулі звукової і світлової сигналізації для роботи з мікроконтролером;

– перевірити працездатність модулів звукової і світлової сигналізації;

– звукові модулі можуть підтримувати відтворення різних звуків або мелодій. Передбачити у програмному забезпеченні можливість завантаження та програвання необхідних аудіо сигналів;

– для світлових модулів може знадобитися програмна реалізація різних режимів світіння: постійне, блимання, зміна кольору тощо.

3.2.5. Під’єднання до мікроконтролерної плати модуля реле

Модуль реле використовується для керування електронним замком.

Почати підключення модуля реле необхідно з визначення його типу , який плануємо використовувати. Існують різні модулі реле з різними кількостями каналів і характеристиками [41].

Після цього підключаємо модуль реле до мікроконтролера. Зазвичай для цього використовуються цифрові піни на платі Arduino, які відповідають за керування включенням та виключенням реле.

Перед підключенням необхідно впевнитись, що напруга живлення модуля реле сумісна з платою Arduino UNO. Більшість модулів реле працюють з напругою 5V.

Після підключення модуля реле до мікроконтролера потрібно використовувати відповідний код для керування реле через мікроконтролер. Можна використати функції digitalWrite() для управління цифровими пінами, які підключені до модуля реле.

Потрібно забезпечити необхідну безпеку при підключенні модуля реле до електричних навантажень, особливо якщо це великі пристрої, такі як мотори або лампи. Необхідно використовувати відповідні захисні елементи, такі як вимикачі, щоб уникнути можливих аварій.

Отже, для підключення модуля реле до мікроконтролерної плати необхідно виконати наступні кроки:

– визначити тип модуля реле, який буде використовуватися в системі;

– перевірити, чи відповідає модуль реле вимогам системи контролю доступу;

– з'єднати модуль реле з мікроконтролерною платою за допомогою відповідних проводів;

– перевірити правильність підключення модуля реле до мікроконтролерної плати;

– налаштувати модуль реле для роботи з мікроконтролером;

– перевірити працездатність модуля реле.

На рисунку 3.6 зображене з’єднання модуля реле із платою Arduino UNO

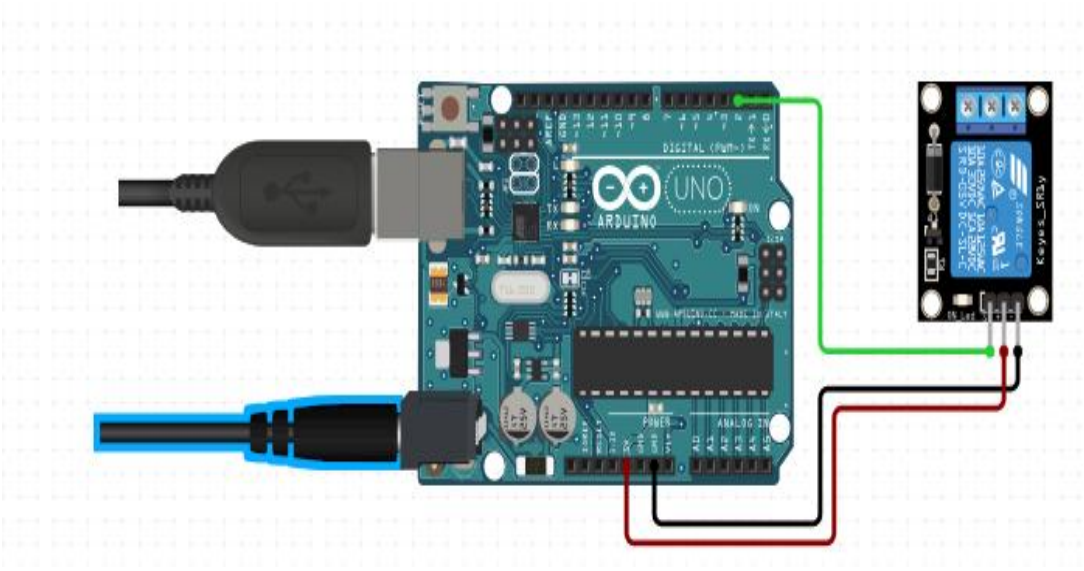


Рисунок 3.6 — Підключення модуля реле до плати Arduino UNO

Для коректного підключення реле необхідно попередньо підключити бібліотеку Relay.h. після чого, за допомогою директиви #define, перед компіляцією, необхідно визначити номер PIN:

#define RELAYMODULE_PIN_SIGNAL номер пін

Далі за допомогою бібліотеки проводиться ініціалізація об’єкта

Relay relayModule(RELAYMODULE_PIN_SIGNAL);

3.2.6. Під’єднання до мікроконтролерної плати модульної клавіатури

Для коректної роботи модуля необхідно, завчасно, підключити бібліотеку keypad.h. Так як клавіатура є матричною, необхідно прописати параметри модуля клавіатури, а саме кількість рядків, якими володіє клавіатура:

Підключення модуля зображене на рисунку 3.7.

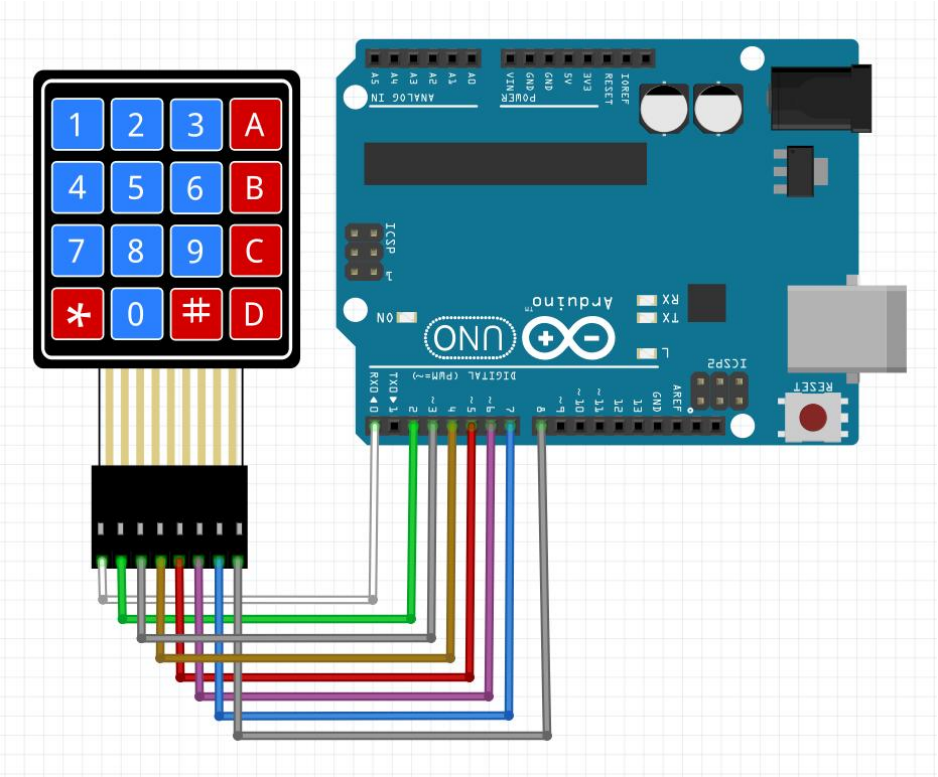


Рисунок 3.7 — Підключення модуля клавіатури до плати

Код для підключення матричної клавіатури до плати Arduino починається з підключення бібліотеки Keypad, яка спрощує взаємодію з клавіатурою. Далі визначаються розміри клавіатури (4 ряди та 4 стовпці) та масив символів, які відповідають кожній клавіші. Піни Arduino, до яких підключені ряди (2, 3, 4, 5) та стовпці (6, 7, 8, 9), задаються у вигляді масивів rowPins і colPins відповідно. Створюється об'єкт keypad, який містить карту клавіш і пінів [42]. У функції setup ініціалізується серіальний порт для виведення даних. У функції loop постійно перевіряється, чи натиснута клавіша за допомогою методу getKey(). Якщо клавіша натиснута, її символ виводиться у серіальний монітор. Цей код дозволяє зчитувати натискання клавіш на матричній клавіатурі та відображати їх у серіальному моніторі Arduino IDE.

3.3. Розроблення алгоритму функціонування системи

Алгоритм функціонування системи контролю доступу є однією з ключових складових розробки мікроконтролерної системи. Він визначає послідовність дій,

які повинні виконуватися мікроконтролером для забезпечення належної роботи системи. Нижче наведено детальний опис процесу розроблення алгоритму функціонування системи контролю доступу.

Крок 1. Визначення вимог до алгоритму.

На першому етапі необхідно визначити вимоги до алгоритму функціонування системи. Це включає в себе:

Визначення функціональних вимог до системи контролю доступу.

Визначення обмежень, з якими повинен впоратися алгоритм (наприклад, обмеження на час відгуку системи, обмеження на кількість одночасних користувачів тощо).

Визначення вимог до безпеки та надійності системи.

Крок 2. Розробка блок-схеми алгоритму.

На другому етапі необхідно розробити блок-схему алгоритму функціонування системи. Блок-схема є графічним представленням алгоритму, яке допомагає зрозуміти його логіку та послідовність дій. Блок-схема повинна включати в себе:

Блоки, що представляють вхідні дані (наприклад, сигнал від RFID-чипа, сигнал від датчика руху тощо).

Блоки, що представляють обробку даних (наприклад, перевірка відповідності RFID-чипа списку дозволених користувачів, обробка сигналу від датчика руху тощо).

Блоки, що представляють вихідні дані (наприклад, сигнал на відкриття/закриття електронного замка, сигнал на включення/вимкнення світлової/звукової сигналізації тощо).

Крок 3. Розробка псевдокоду алгоритму.

На третьому етапі необхідно розробити псевдокод алгоритму функціонування системи. Псевдокод є текстовим описом алгоритму, який допомагає зрозуміти його логіку та послідовність дій. Псевдокод повинен включати в себе:

– опис вхідних даних;

– опис обробки даних;

– опис вихідних даних;

– опис умовних та циклічних конструкцій, що використовуються в алгоритмі (наприклад, умовні оператори if-else, цикли while та for тощо).

Крок 4. Тестування та відладка алгоритму на четвертому етапі необхідно протестувати та відладувати алгоритм функціонування системи. Для цього необхідно:

– розробити тестові сценарії, що охоплюють всі можливі варіанти роботи системи;

– виконати тестування алгоритму на відповідності тестовим сценаріям;

– виявити та виправити помилки в алгоритмі;

– перевірити відповідність алгоритму вимогам до безпеки та надійності системи.

Крок 5. Імплементація алгоритму на мікроконтролері.

На п'ятому етапі необхідно імплементувати розроблений алгоритм на мікроконтролері. Для цього необхідно:

– вибрати відповідну мову програмування для мікроконтролера (наприклад, C/C++, Python тощо);

– написати програмний код, що реалізує алгоритм функціонування системи;

– завантажити програмний код на мікроконтролер;

– перевірити правильність роботи системи.

Крок 6. Тестування та відладка системи в цілому

На шостому етапі необхідно протестувати та відладувати систему в цілому. Для цього необхідно:

— виконати тестування системи на відповідність вимогам до функціонування;

— виявити та виправити помилки в роботі системи;

— перевірити відповідність системи вимогам до безпеки та надійності.

Крок 7. Оптимізація алгоритму На сьомому етапі необхідно оптимізувати розроблений алгоритм для забезпечення ефективної роботи системи [43]. Зокрема, слід:

– виконати профілювання алгоритму для виявлення найбільш ресурсоємних операцій та оптимізувати їх;

– застосувати методи оптимізації пам'яті та циклів;

– забезпечити ефективне використання ресурсів мікроконтролера, таких як тактові цикли та енергоспоживання;

– виконати тестування оптимізованого алгоритму на відповідність вимогам швидкодії та ресурсоспоживання.

Після завершення всіх етапів розроблення алгоритму функціонування системи контролю доступу, система повинна бути готова до експлуатації.

На рисунку 3.8 показаний алгоритм функціонування системи автоматизованої системи контролю доступу.

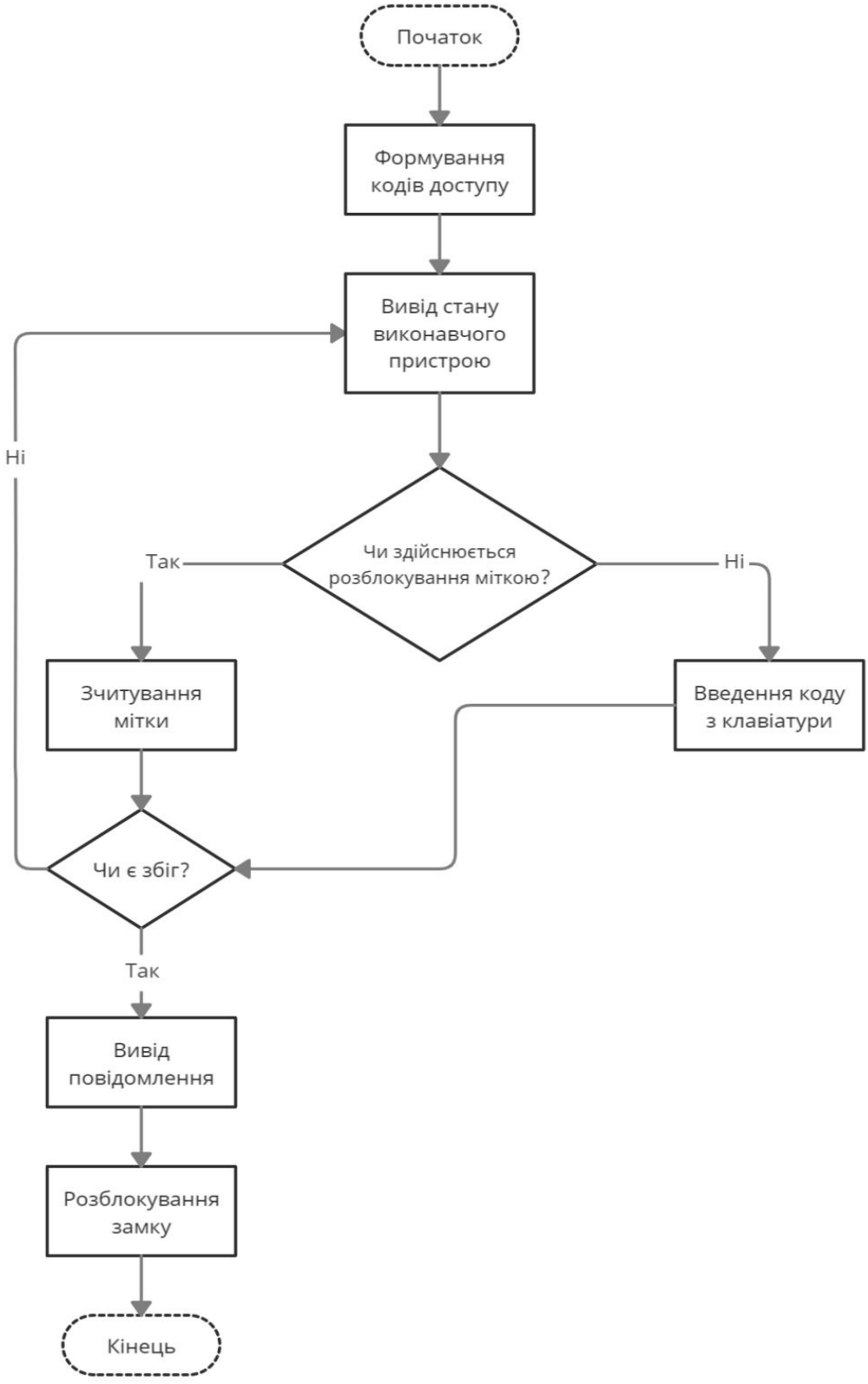


Рисунок 3.8 — Блок-схема алгоритму функціонування системи автоматизованої системи контролю доступу

3.4. Розроблення бази даних

База даних є однією з ключових складових системи контролю доступу [44]. Вона містить інформацію про користувачів, їхні права доступу, історію доступу та інші дані, необхідні для роботи системи. Розроблення бази даних включає в себе такі етапи:

– визначення вимог до бази даних. На цьому етапі необхідно визначити, які дані будуть зберігатися в базі даних, яким чином вони будуть використовуватися, якими будуть вимоги до швидкодії та надійності бази даних [45];

– вибір типу бази даних. Існує декілька типів баз даних, таких як реляційні, об'єктно-орієнтовані, документно-орієнтовані та інші. Вибір типу бази даних залежить від вимог до системи та характеру даних, які будуть зберігатися;

– проектування схеми бази даних. Схема бази даних визначає, як дані будуть організовані та зв'язані між собою. На цьому етапі необхідно визначити таблиці, поля, індекси, зв'язки між таблицями та інші елементи схеми [46];

– розроблення інтерфейсу до бази даних. Інтерфейс до бази даних визначає, як програмний код системи контролю доступу буде взаємодіяти з базою даних. На цьому етапі необхідно розробити набір функцій та процедур, які будуть використовуватися для доступу до даних в базі даних;

– тестування та налагоджування бази даних. Після розроблення бази даних необхідно провести її тестування та налагоджування. На цьому етапі необхідно перевірити, чи працює база даних відповідно до вимог, чи є в ній помилки та недоліки, та виправити їх [47];

– впровадження бази даних в систему контролю доступу. Після успішного тестування та налагоджування бази даних необхідно впровадити її в систему контролю доступу. На цьому етапі необхідно підключити базу даних до програмного коду системи, перевірити її роботу в умовах реального використання та виправити можливі помилки [48];

Розроблення бази даних є складним та відповідальним завданням, яке вимагає глибоких знань та досвіду в галузі проектування та розробки баз даних. Тому для розроблення бази даних для системи контролю доступу рекомендується залучити фахівців з досвідом роботи з подібними системами.

3.5. Опис інтерфейсу програмної частини системи

Інтерфейс програмної частини системи контролю доступу повинен бути зручним та інтуїтивно зрозумілим для користувачів [49]. Він повинен забезпечувати можливість введення даних про користувачів, налаштування прав доступу, перегляду історії доступу та виконання інших необхідних функцій.

Основні елементи інтерфейсу програмної частини системи:

– меню головного екрану. Містить пункти для переходу до основних функцій програми: введення даних про користувачів, налаштування прав доступу, перегляду історії доступу, тощо;

– форма введення даних про користувачів. Містить поля для введення ПІН-коду, імені та прізвища користувача, фотографії (якщо передбачено біометричну ідентифікацію), та іншої необхідної інформації. Також містить кнопки для збереження та скасування введення даних;

– форма налаштування прав доступу. Містить таблицю з переліком користувачів та їхніми правами доступу до різних об'єктів. Також містить кнопки для збереження та скасування змін;

– форма перегляду історії доступу. Містить таблицю з переліком подій доступу (вхід/вихід), датою та часом події, іменем та прізвищем користувача, та іншою необхідною інформацією. Також містить кнопки для фільтрації та сортування даних;

– повідомлення та діалогові вікна. Використовуються для інформування користувача про поточний стан системи, помилки введення даних, тощо. Також можуть використовуватися для підтвердження або скасування певних дій.

Інтерфейс програмної частини системи повинен бути розроблений з урахуванням вимог та побажань замовника, а також відповідно до сучасних стандартів та рекомендацій з дизайну інтерфейсів.

При розробці інтерфейсу програмної частини системи необхідно враховувати наступні аспекти:

– зручність та простота використання. Інтерфейс повинен бути інтуїтивно зрозумілим та легким у використанні для користувачів з різним рівнем підготовки;

– швидкість та ефективність роботи. Інтерфейс повинен забезпечувати швидкий та ефективний доступ до необхідних функцій та даних;

– надійність та безпека. Інтерфейс повинен забезпечувати надійну та безпечну роботу системи, запобігати несанкціонованому доступу та помилковим діям користувачів;

– масштабованість та гнучкість. Інтерфейс повинен бути гнучким та масштабованим, щоб забезпечити можливість розширення та модифікації системи в майбутньому;

– сумісність з апаратною частиною системи. Інтерфейс повинен бути сумісним з апаратною частиною системи та забезпечувати правильну взаємодію між ними;

– панель налаштувань системи. Містить елементи для налаштування часу очікування, політик доступу, часу блокування доступу після певної кількості невдалих спроб тощо;

– журнал подій. Окрема форма чи вікно для перегляду детальної інформації про всі події в системі, включаючи спроби несанкціонованого доступу, помилки та попередження;

– елементи імпорту/експорту даних. Можливість імпорту/експорту даних користувачів, налаштувань та журналу подій для зручності резервного копіювання, переносу між системами тощо.

Загалом, розроблення інтерфейсу програмної частини системи контролю доступу є важливим та відповідальним завданням, яке вимагає глибокого

розуміння потреб та вимог користувачів, а також сучасних стандартів та технологій розробки інтерфейсів.

При розробці інтерфейсу програмної частини необхідно також врахувати можливість масштабування та розширення функціоналу в майбутньому шляхом модульного дизайну та використання сучасних підходів до розробки користувацького інтерфейсу

3.6. Тестування прототипу мікроконтролерної системи

Після розробки та збірки прототипу мікроконтролерної системи контролю доступу, необхідно провести серію тестів для перевірки його функціонування та виявлення можливих недоліків та помилок.

Тестування прототипу мікроконтролерної системи повинно включати в себе наступні етапи:

– перевірка роботи апаратної частини системи. На цьому етапі необхідно перевірити, чи працюють всі компоненти апаратної частини системи (RFID-читач, електронний замок, індикатори, та ін.) відповідно до технічних характеристик та вимог до проекту [50];

– перевірка роботи програмної частини системи. На цьому етапі необхідно перевірити, чи працює програмне забезпечення, розроблене для мікроконтролера, відповідно до алгоритму функціонування системи та вимог до проекту [52];

– тестування системи в різних режимах роботи. На цьому етапі необхідно перевірити, чи працює система контролю доступу відповідно до вимог до проекту в усіх режимах роботи (режим очікування, режим ідентифікації, режим відкриття двері, режим закриття двері, та ін.);

– тестування системи на надійність та стійкість. На цьому етапі необхідно перевірити, чи працює система контролю доступу надійно та стійко в умовах тривалого використання та впливу зовнішніх факторів (температура, вологість, електромагнітні поля, та ін.);

– тестування системи на безпеку. На цьому етапі необхідно перевірити, чи забезпечує система контролю доступу належний рівень безпеки та захисту від несанкціонованого доступу та втручання;

– перевірка зовнішніх впливів. На цьому етапі необхідно перевірити, як працює система в різних умовах, наприклад, за різних температур, рівнів вологості, вібрацій, електромагнітних перешкод тощо [53];

– тестування різних сценаріїв використання. Система повинна бути протестована на різних сценаріях використання, включаючи нормальну роботу, помилки користувачів, спроби несанкціонованого доступу та інші можливі ситуації;

– стрес-тестування. Перевірка роботи системи під навантаженням, наприклад, при одночасному доступі великої кількості користувачів або при тривалій безперервній роботі.

При проведенні тестування прототипу мікроконтролерної системи, необхідно ретельно фіксувати всі виявлені недоліки та помилки, а також розробити план їх усунення та внесення змін до проекту.

Після усунення всіх недоліків та помилок, необхідно провести повторне тестування прототипу мікроконтролерної системи для перевірки його відповідності вимогам до проекту та готовності до впровадження в реальних умовах використання.

3.7 Висновки

У третьому розділі було розглянуто процес розроблення програмно-апаратної реалізації та тестування мікроконтролерної системи контролю доступу.

На основі вимог до системи, було розроблено функціональну схему мікроконтролерної системи, яка включає в себе RFID-модуль, електронний замок, LCD-дисплей, модулі звукової та світлової сигналізації та модуль реле.

Потім було розроблено електричну принципову схему мікроконтролерної системи, яка включає в себе під'єднання всіх компонентів до мікроконтролерної

плати. Також було розглянуто під'єднання до мікроконтролерної плати RFID-модуля, електронного замка, LCD-дисплею, модулів звукової та світлової сигналізації та модуля реле.

Далі було розроблено алгоритм функціонування системи, який передбачає наступні кроки: ідентифікація RFID-карти, перевірка доступу, відкриття/закриття електронного замка, відображення інформації на LCD-дисплеї, звукова та світлова сигналізація.

Було розроблено базу даних, яка містить інформацію про користувачів та їх права доступу. Також було розроблено інтерфейс програмної частини системи, який дозволяє адміністратору керувати системою контролю доступу.

Після цього було проведено тестування прототипу мікроконтролерної системи, яке включало в себе перевірку роботи всіх компонентів системи, перевірку роботи алгоритму функціонування системи, перевірку роботи бази даних та інтерфейсу програмної частини системи.

За результатами тестування було виявлено, що розроблена мікроконтролерна система контролю доступу відповідає вимогам, визначеним на етапі проектування, та працює надійно та ефективно.

Таким чином, у третьому розділі було розроблено та протестовано програмно-апаратну реалізацію мікроконтролерної системи контролю доступу, яка забезпечує надійний та ефективний контроль доступу до об'єктів з мінімальними витратами та високою надійністю.

ВИСНОВОК

В результаті виконаної роботи було досліджено, що розробка надійної та ефективної системи контролю доступу є критично важливою задачею. Вибір методів ідентифікації доступу, таких як парольна та апаратна, визначається їхньою надійністю та зручністю використання. Парольна ідентифікація, хоч і є широко поширеним методом, має свої обмеження, включаючи загрозу вгадування або вкрадення паролю. З іншого боку, апаратна ідентифікація, що використовує фізичні пристрої, виявляється більш надійним варіантом, проте може зазнавати атак крадіжки або підробки.

Огляд існуючих систем контролю доступу дозволив визначити оптимальний підхід до розробки нової системи на основі мікроконтролера Atmega 328P. Під час вибору компонентів та інструментів для розробки електронної системи, увага приділялася їхній сумісності, надійності та функціональності. Результатом цього процесу стала розробка та успішне тестування програмно-апаратної реалізації мікроконтролерної системи контролю доступу, яка відповідає вимогам безпеки та ефективності, демонструючи свою здатність забезпечувати надійний контроль доступу до об'єктів

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Andrew S. Tanenbaum, & David J. Wetherall. Computer Networks. Prentice Hall, 2011. 404 p.

2. Andy Greenberg. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. Doubleday, 2019. 219 p.

3. Brian Chess, & Jakob West. Secure Programming with Static Analysis. Addison-Wesley Professional, 2007. 191 p.

4. Brian Krebs. Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door. Sourcebooks, 2014. 201 p.

5. Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996. 96 p.

6. Bruce Schneier. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company, 2015. 309 p.

7. Carl Ellison, & Bruce Schneier. Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. Counterpane Internet Security, Inc., 2000. 200 p.

8. Charlie Miller, & Chris Valasek. The Car Hacker's Handbook: A Guide for the Penetration Tester. No Starch Press, 2014. 95 p.

9. Christopher Kruegel, & Giovanni Vigna. Malware: Fighting Malicious Code. Prentice Hall, 2005. 267 p.

10. Clifford Stoll. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Doubleday, 1989. 89 p.

11. David Aucsmith. The Security Engineering Management Handbook. McGraw-Hill Education, 1997. 97 p.

12. David D. Clark. Designs for an Internet. 2003. 174 p.

13. David Sanger. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Crown, 2018. 188 p.

14. David Wagner, & Bruce Schneier. A Practical Analysis of the SSL Protocol. Dr. Dobb's Journal, 1999. 33 p.

15. Donn B. Parker. Fighting Computer Crime: A New Framework for Protecting Information. John Wiley & Sons, 1998. 98 p.

16. Dorothy E. Denning. Information Warfare and Security. Addison-Wesley Professional, 1999. 99 p.

17. Douglas Comer. Internetworking with TCP/IP. Prentice Hall, 2013. 127 p.

18. Eugene H. Spafford, et al. The Internet Worm Program: An Analysis. Purdue Technical Report CSD-TR-823, 1989. 89 p.

19. Fred Cohen. A Short Course on Computer Viruses. American Research Press, 1987. 46 p.

20. Fred Kaplan. Dark Territory: The Secret History of Cyber War. Simon & Schuster, 2016. 122 p.

21. Gary McGraw. Software Security: Building Security In. Addison-Wesley Professional, 2015. 188 p.

22. Harlan Carvey. Windows Forensic Analysis: DVD Toolkit. Syngress, 2011. 159 p.

23. Jeffrey Carr. Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media, 2011. 145 p.

24. Jeffrey Voas. Software Assessment: Reliability, Safety, and Testability. John Wiley & Sons, 2001. 92 p.

25. Kim Zetter. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown, 2014. 233 p.

26. Marcus J. Ranum. The Myth of Homeland Security. John Wiley & Sons, 2005. 105 p.

27. Mark Stamp. Information Security: Principles and Practice. Wiley, 2011. 237 p.

28. Matt Bishop. Computer Security: Art and Science. Addison-Wesley Professional, 2003. 303 p.

29. Michael Howard, & David LeBlanc. Writing Secure Code. Microsoft Press, 2003. 213 p.

30. Mikko Hypponen. If It's Smart, It's Vulnerable. Wiley, 2020. 120 p.

31. Misha Glenny. DarkMarket: Cyberthieves, Cybercops and You. Vintage, 2008. 105 p.

32. Nicole Perlroth. This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Publishing, 2021. 121 p.

33. Niels Ferguson, & Bruce Schneier. Practical Cryptography. John Wiley & Sons, 2003. 203 p.

34. P. W. Singer, & Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. 178 p.

35. Peter G. Neumann. Computer-Related Risks. Addison-Wesley Professional, 1995. 213 p.

36. Peter G. Neumann. Risks to the Public in Computers and Related Systems. ACM SIGSOFT Software Engineering Notes, 1994. 94 p.

37. Peter Wayner. Digital Copyright Protection. Apress, 2015. 88 p.

38. Radia Perlman. Interconnections: Bridges, Routers, Switches, and Internetworking Protocols. Addison-Wesley Professional, 2006. 322 p.

39. Richard A. Clarke, & Robert K. Knake. The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Publishing Group, 2019. 77 p.

40. Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. Addison-Wesley Professional, 2013.

41. 134 p.

42. Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2008. 411 p.

43. Sergey Bratus, et al. Security and Privacy in Cyber-Physical Systems. Springer, 2012. 301 p.

44. Shon Harris. CISSP All-in-One Exam Guide. McGraw-Hill Education, 2012. 568 p.

45. Simson Garfinkel, Alan Schwartz, & Gene Spafford. Practical UNIX and Internet Security. O'Reilly Media, 2003. 123 p.

46. Simson Garfinkel. PGP: Pretty Good Privacy. O'Reilly Media, 1995. 195 p.

47. Steven Furnell, & Sokratis Katsikas. Authentication: From Passwords to Public Keys. Springer, 2007. 56 p.

48. Stuart McClure, Joel Scambray, & George Kurtz. Hacking Exposed 7: Network Security Secrets and Solutions. McGraw-Hill Education, 2009. 182 p.

49. Ted Koppel. Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath. Crown, 2015. 89 p.

50. Tyler Cohen Wood. Catching the Catfishers: Disarm the Online Pretenders, Predators, and Perpetrators Who Are Out to Ruin Your Life. McGraw-Hill Education, 2020. 77 p.

51. Wenbing Zhao. Cyber Security: Principles, Methodologies, and Applications. Wiley, 2014. 98 p.

52. Whitfield Diffie, & Susan Landau. Privacy on the Line: The Politics of Wiretapping and Encryption. The MIT Press, 2007. 207 p.

53. William Stallings. Cryptography and Network Security: Principles and Practice. Prentice Hall, 2017. 289 p.

54. Василь Бугайов. Захист інформації в інформаційних системах. Київ: Видавництво "Видавничий дім", 2018. 45 с.

55. Володимир Гречаний. Захист інформації: від теорії до практики. Львів: Видавництво Львівської політехніки, 2019. 74 с.

56. Іван Коваленко. Кібербезпека підприємства: виклики та рішення. Київ: Видавництво "Книголав", 2020. 67 с.

57. Іван Приходько. Кібербезпека: технології захисту інформації. Київ: Видавництво "Комп'ютерна преса", 2016. 201 с.

58. Микола Лозовенко. Інформаційна безпека. Київ: Видавництво "ІНЖЕК", 2016. 112 с.

59. Олександр Іванов. Методи захисту інформації. Київ: Видавництво "Наукова думка", 2019. 256 с.

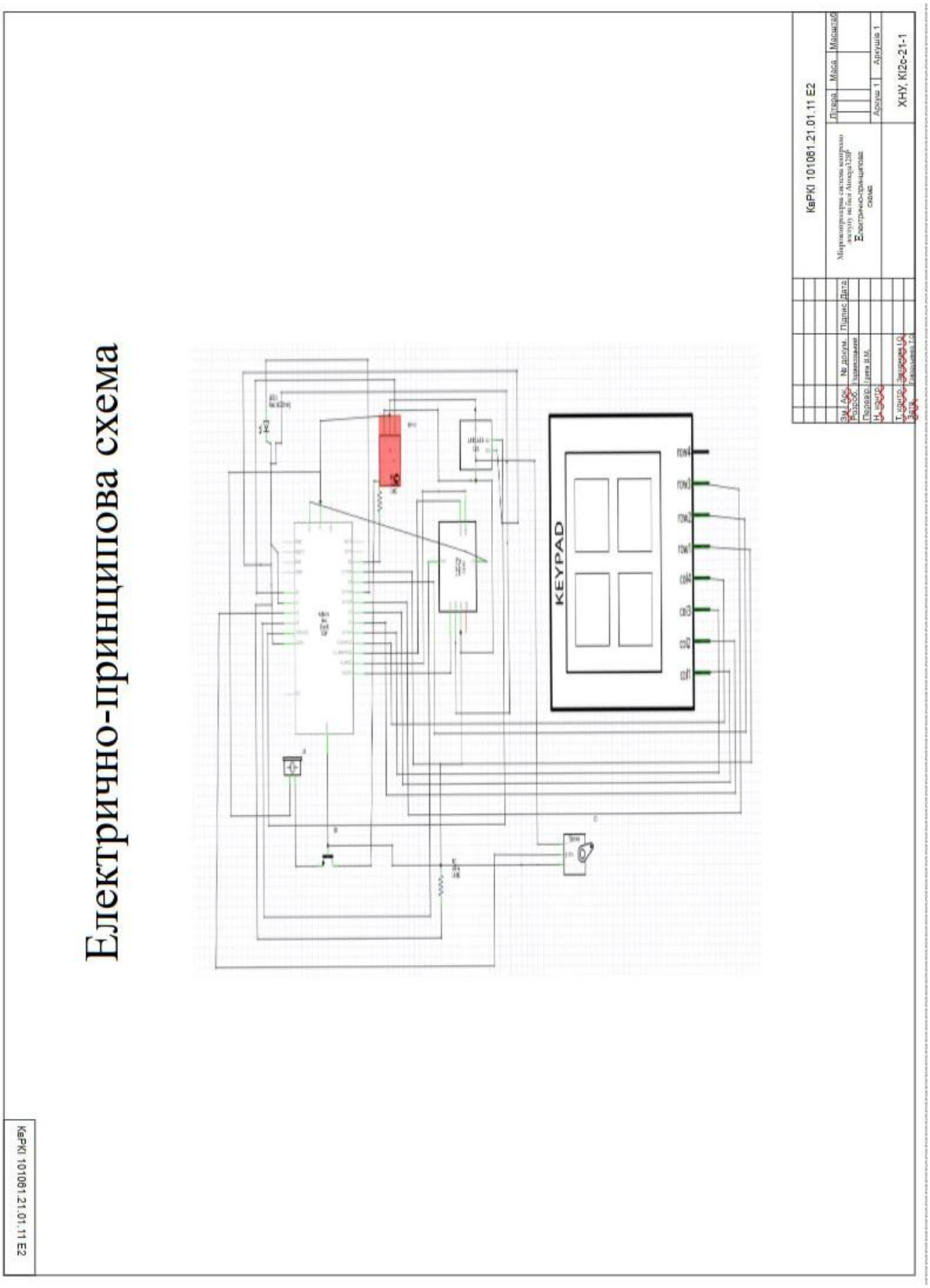
60. Олександр Петренко. Інформаційна безпека: захист інформації в сучасному світі. Київ: Видавництво "Міжнародний центр книги", 2018. 153 с.

61. Олена Іванова. Методи та засоби захисту інформації в інформаційних системах. Харків: Видавництво "Інтерсервіс", 2017. 152 с.

Додаток А

(обов’язковий)

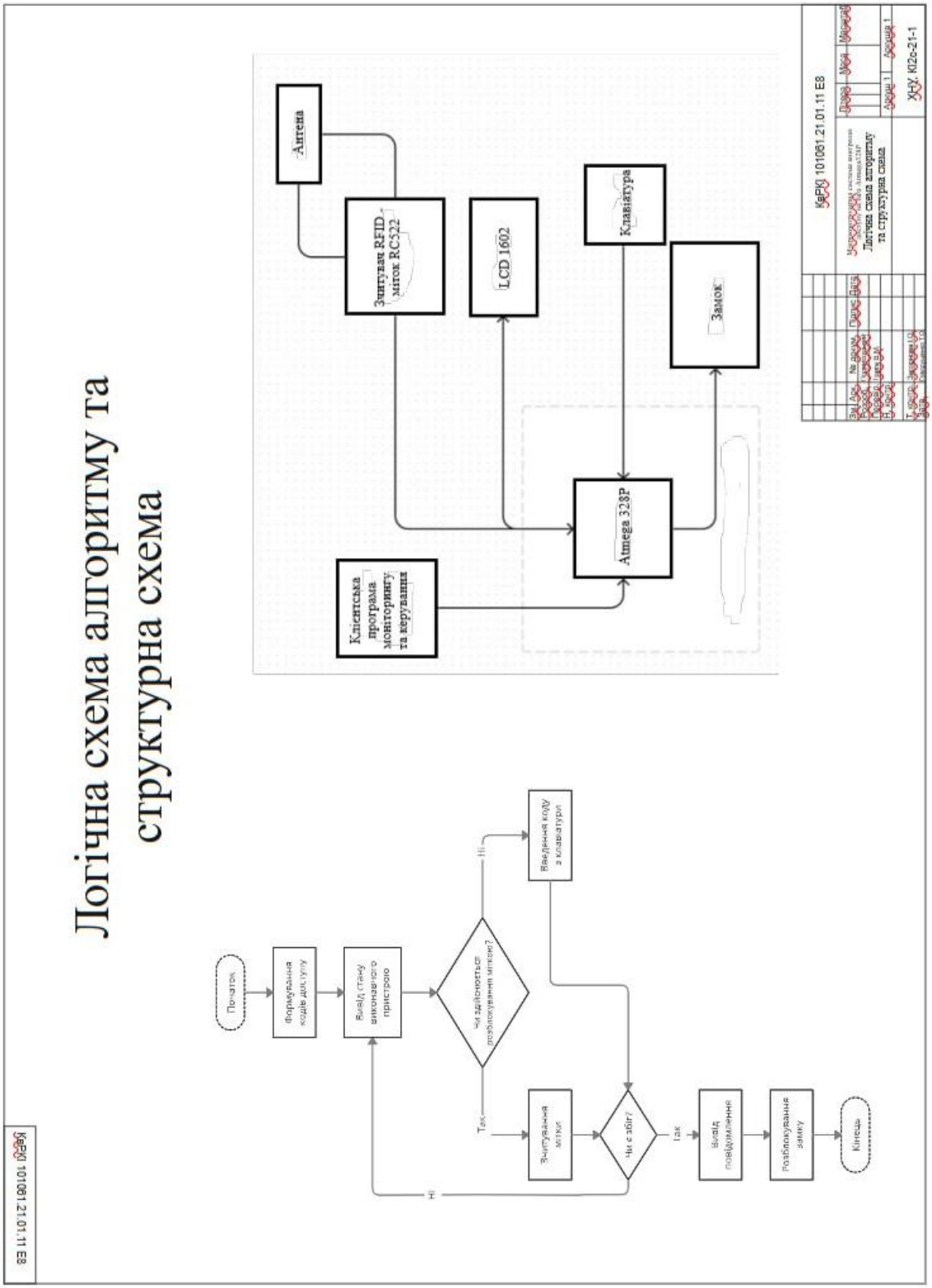
Копія креслення «Електрично-принципова схема мікроконтролерної системи контролю доступу на базі Atmega328P»



Додаток Б

(обов’язковий)

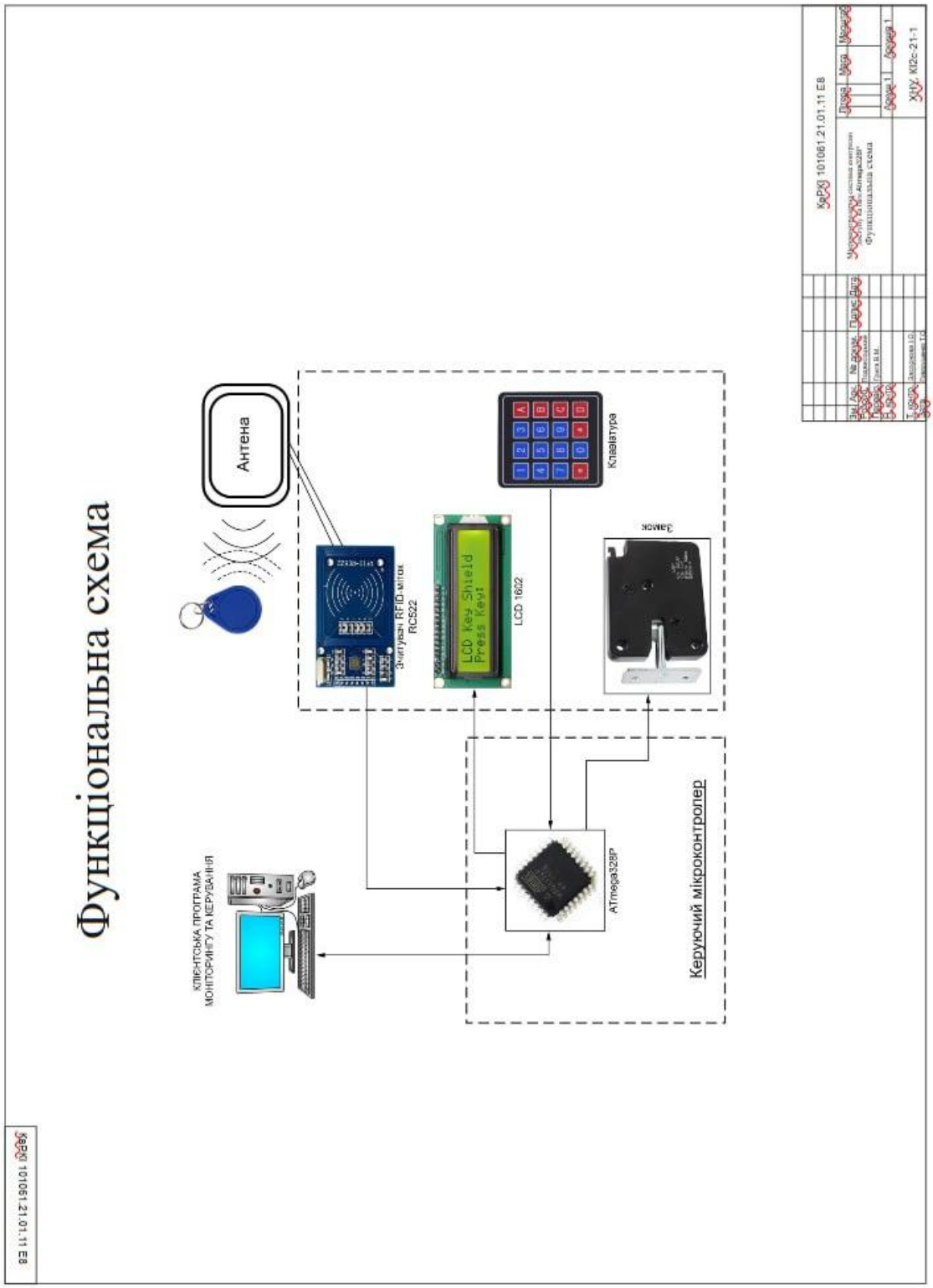
Копія креслення «Логічна схема алгоритму та структурна схема мікроконтролерної системи контролю доступу на базі Atmega328P»



Додаток В

(обов’язковий)

Копія креслення «Функціональна схема мікроконтролерної системи контролю доступу на базі Atmega328P»



Додаток Г

Код програми

Код програми:

```
#include "Arduino.h"
#include "Buzzer.h"
#include "Keypad.h"
#include "LiquidCrystal_PCF8574.h"
#include "LED.h"
#include "RFID.h"
#include "Relay.h"
#include "Servo.h"

// Визначення пінів
#define BUZZER_PIN_SIG  2
#define KEYPADMEM3X4_PIN_ROW1  7
#define KEYPADMEM3X4_PIN_ROW2  8
#define KEYPADMEM3X4_PIN_ROW3  9
#define KEYPADMEM3X4_PIN_ROW4  10
#define KEYPADMEM3X4_PIN_COL1  3
#define KEYPADMEM3X4_PIN_COL2  4
#define KEYPADMEM3X4_PIN_COL3  6
#define LEDB_PIN_VIN  5
#define RFID_PIN_RST  A3
#define RFID_PIN_SDA  A1
#define RELAYMODULE_PIN_SIGNAL  A0
#define SERVO360MICRO_PIN_SIG  A2

// Глобальні змінні та визначення
char keypadmem3x4keys[4][3] = {
```

```
  {'1', '2', '3'},
  {'4', '5', '6'},
  {'7', '8', '9'},
  {'*', '0', '#'}
};

#define LCD_ADDRESS 0x3F
#define LCD_ROWS 2
#define LCD_COLUMNS 16
#define SCROLL_DELAY 150
#define BACKLIGHT 255

// Ініціалізація об'єктів
Buzzer buzzer(BUZZER_PIN_SIG);
Keypad keypadmem3x4(KEYPADMEM3X4_PIN_COL1,
KEYPADMEM3X4_PIN_COL2, KEYPADMEM3X4_PIN_COL3,
KEYPADMEM3X4_PIN_ROW1, KEYPADMEM3X4_PIN_ROW2,
KEYPADMEM3X4_PIN_ROW3, KEYPADMEM3X4_PIN_ROW4);
LiquidCrystal_PCF8574 lcdI2C;
LED ledB(LEDB_PIN_VIN);
RFID rfid(RFID_PIN_SDA, RFID_PIN_RST);
Relay relayModule(RELAYMODULE_PIN_SIGNAL);
Servo servo360Micro;

const int timeout = 10000; // Визначення тайм-ауту 10 секунд
char menuOption = 0;
long time0;

// Функція setup
void setup() {
```

```
  Serial.begin(9600);
  while (!Serial);
  Serial.println("start");

  keypadmem3x4.begin(keypadmem3x4keys);
  lcdI2C.begin(LCD_COLUMNS, LCD_ROWS, LCD_ADDRESS, BACKLIGHT);
  rfid.init();
  menuOption = menu();
}

// Основний цикл
void loop() {
  if (menuOption == '1') {
    buzzer.on();
    delay(500);
    buzzer.off();
    delay(500);
  } else if (menuOption == '2') {
    char keypadmem3x4Key = keypadmem3x4.getKey();
    if (isDigit(keypadmem3x4Key) || keypadmem3x4Key == '*' || keypadmem3x4Key ==
'#') {
      Serial.print(keypadmem3x4Key);
    }
  } else if (menuOption == '3') {
    lcdI2C.clear();
    lcdI2C.print("  Circuito.io  ");
    lcdI2C.selectLine(2);
    lcdI2C.print("     Rocks!  ");
    delay(1000);
  } else if (menuOption == '4') {
```

```
    for (int i = 255; i > 0; i -= 5) {
      ledB.dim(i);
      delay(15);
    }
    ledB.off();
  } else if (menuOption == '5') {
    String rfidtag = rfid.readTag();
    rfid.printTag(rfidtag);
  } else if (menuOption == '6') {
    relayModule.on();
    delay(500);
    relayModule.off();
    delay(500);
  } else if (menuOption == '7') {
    servo360Micro.attach(SERVO360MICRO_PIN_SIG);
    servo360Micro.write(180);
    delay(2000);
    servo360Micro.write(0);
    delay(2000);
    servo360Micro.write(90);
    delay(2000);
    servo360Micro.detach();
  }

  if (millis() - time0 > timeout) {
    menuOption = menu();
  }
}

// Функція меню
```

```
char menu() {
  Serial.println(F("\nWhich component would you like to test?"));
  Serial.println(F("(1) Buzzer"));
  Serial.println(F("(2) Membrane 3x4 Matrix Keypad"));
  Serial.println(F("(3) LCD 16x2 I2C"));
  Serial.println(F("(4) LED - Basic Blue 5mm"));
  Serial.println(F("(5) RFID Card Reader - RC522"));
  Serial.println(F("(6) Relay Module"));
  Serial.println(F("(7) Continuous Rotation Micro Servo - FS90R"));
  Serial.println(F("(menu) send anything else or press on board reset button\n"));

  while (!Serial.available());

  while (Serial.available()) {
    char c = Serial.read();
    if (isAlphaNumeric(c)) {
      if (c == '1')
        Serial.println(F("Now Testing Buzzer"));
      else if (c == '2')
        Serial.println(F("Now Testing Membrane 3x4 Matrix Keypad"));
      else if (c == '3')
        Serial.println(F("Now Testing LCD 16x2 I2C"));
      else if (c == '4')
        Serial.println(F("Now Testing LED - Basic Blue 5mm"));
      else if (c == '5')
        Serial.println(F("Now Testing RFID Card Reader - RC522"));
      else if (c == '6')
        Serial.println(F("Now Testing Relay Module"));
      else if (c == '7')
        Serial.println(F("Now Testing Continuous Rotation Micro Servo - FS90R"));
```

```
      else {
        Serial.println(F("Illegal input!"));
        return 0;
      }
      time0 = millis();
      return c;
    }
  }
  return 0;
}
```

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра КІ

ID перевірки:
1016351809

Дата перевірки:
12.06.2024 19:44:02 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
12.06.2024 20:46:45 EEST

ID користувача:
100005591

Назва документа: **Подвисоцький_Мікроконтролерна система контролю доступу на базі Atmega328P**

Кількість сторінок: **69** Кількість слів: **11742** Кількість символів: **97016** Розмір файлу: **2.57 MB** ID файлу: **1016155642**

6.69%
Схожість

Найбільша схожість: **0.9%** з Інтернет-джерелом (https://ebin.pub/bitskrieg-the-new-challenge-of-cyberwarfare-97815095..

5.81% Джерела з Інтернету | 786 ..... Сторінка 71

2.27% Джерела з Бібліотеки | 104 ..... Сторінка 77

0% Цитат

Не знайдено жодних цитат

Не знайдено жодних посилань

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 1

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 8%**

ID: 129954 Назва: ВКР Мікроконтролерна система контролю доступу на базі Atmega328P Додано в БД: 2024-06-12 Автора: В. І. Подвисоцький Керівники: В. М. Грига Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	81743	750	1498 (2%)	26 (3%)

Джерело плагіату

ID	Опис	Напівість плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Подвисоцький Владислав Іванович

Тема: Мікроконтролерна система контролю доступу на базі Atmega328P

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3___ Кількість сторінок записки ___62___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є розроблення мікроконтролерної системи контролю доступу на базі Atmega328P для підвищення ефективності та надійності системи пожежної безпеки.

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

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі кваліфікаційної роботи проведено огляд предметної області та обґрунтування щодо розроблення системи контролю доступу, яка забезпечить високий рівень безпеки та зручності використання, а також проведено аналіз методів ідентифікації доступу, а саме парольної ідентифікації та апаратної ідентифікації, виконано постановку задачі дослідження. В другому розділі кваліфікаційної роботи здійснено вибір компонентів мікроконтролерної системи контролю доступу на базі Atmega328P, змодельовано структурну та функціональну схеми. Також, було обрано середовище програмування Arduino IDE. В третьому розділі кваліфікаційної роботи виконано реалізацію мікроконтролерної системи контролю доступу та проведено її тестування. А також розроблено електро-принципову схему мікроконтролерної системи контролю доступу на базі Atmega328P.

4. Позитивні сторони роботи: висока точність: система дозволяє точно ідентифікувати користувачів завдяки використанню біометричних даних або унікальних кодів доступу, що значно підвищує безпеку об'єкта і зменшує ризик несанкціонованого доступу.

5. Негативні сторони роботи: складність інтеграції: незважаючи на те, що мікроконтролери є відносно доступними, інтеграція системи в існуючу інфраструктуру може бути складною і вимагати додаткових ресурсів та часу, що може ускладнити впровадження для організацій з обмеженими технічними можливостями.

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

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

8. Інші зауваження: _____

9. Оцінка дипломної роботи: задовільно

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Бедрацюк Ігор Петрович, зав. кафедри ІПЗ ХНУ

"12" 06 2024 р. _____(підпис)

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

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

Подвисоцького Владислава Івановича
ПІБ здобувача вищої освіти

ФІТ, 3 курсу, групи КІ2с-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

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

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

7 червня 2024 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Мікроконтролерна система контролю доступу на базі Atmega328P

Автор: Подвисоцький Владислав Іванович

Спеціальність: 123– Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Грига Володимир Михайлович, , к.т.н., доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) більшість запозичень яких є джерела з інтернету, кількість запозичень з яких становить 5,81%;
4) запозичення з друкованих ресурсів, та ресурсів з бібліотеки становить 2,27%.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 6.69% і адресується до 890 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ В. М. Грига

Гарант ОП _____ С.М. Лисенко

Завідувач кафедри КІІС _____ Т. О. Говорущенко