

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

(повна назва факультету)

Кафедра комп'ютерних систем та мереж

(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр

(назва освітнього ступеня)

на тему: Комп'ютеризована система доступу до приміщення

Виконав(ла): студент(ка) IV курсу, групи СІ-42

спеціальності 123 «Комп'ютерна інженерія»

(шифр і назва спеціальності)

	<u>Рожик А. М.</u>
(підпис)	(прізвище та ініціали)
Керівник	<u>Жаровський Р. О.</u>
(підпис)	(прізвище та ініціали)
Нормоконтроль	<u>Тим С. В.</u>
(підпис)	(прізвище та ініціали)
Завідувач кафедри	<u>Осухівська Г. М.</u>
(підпис)	(прізвище та ініціали)
Рецензент	<u>Бревус В. М.</u>
(підпис)	(прізвище та ініціали)

Тернопіль
2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Осухівська Г.М.

(підпис)

(прізвище та ініціали)

« 25 » 06 2024 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

студенту Рожик Анастасії Миколаївні
(прізвище, ім'я, по батькові)

1. Тема роботи Комп'ютеризована система доступу до приміщення

Керівник роботи Жаровський Руслан Олегович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » 04 2024 року № 4/7-408

2. Термін подання студентом завершеної роботи 26.06.2024р

3. Вихідні дані до роботи Технічне завдання

4. Зміст роботи (перелік питань, які потрібно розробити)

1. Аналіз технічного завдання

2. Проектна частина

3. Практична частина

4. Безпека життєдіяльності, основи охорони праці

Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

Електрична функціональна схема

Електрична структурна схема

Блок схема роботи пристрою

UML діаграма

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
<i>Безпека життєдіяльності, основи охорони праці</i>	<i>Пилипець М. І., д.т.н., проф. каф. МТ</i>		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	<i>Розробка на затвердження технічного завдання</i>	<i>01.02 – 09.02</i>	<i>Виконано</i>
2.	<i>Аналіз технічного завдання</i>	<i>05.02 – 11.02</i>	<i>Виконано</i>
3.	<i>Аналіз вимог та принципів організації комп'ютеризованої системи доступу до приміщення</i>	<i>26.04 – 03.05</i>	<i>Виконано</i>
4.	<i>Вибір елементної бази</i>	<i>04.05 – 13.05</i>	<i>Виконано</i>
5.	<i>Розробка структурної та функціональної схеми</i>	<i>14.05 – 25.05</i>	<i>Виконано</i>
6.	<i>Реалізація проектних рішень</i>	<i>26.05 – 09.06</i>	<i>Виконано</i>
7.	<i>Безпека життєдіяльності, основи охорони праці</i>	<i>10.06 – 15.06</i>	<i>Виконано</i>
8.	<i>Оформлення кваліфікаційної роботи</i>	<i>16.06 – 20.06</i>	<i>Виконано</i>
9.	<i>Попередній захист кваліфікаційної роботи</i>	<i>14.06</i>	<i>Виконано</i>
10.	<i>Захист кваліфікаційної роботи</i>	<i>24.06 – 28.06</i>	<i>Виконано</i>

Студент _____
(підпис)*Рожик Анастасія Миколаївна*

(прізвище та ініціали)Керівник роботи _____
(підпис)*Жаровський Руслан Олегович*

(прізвище та ініціали)

АНОТАЦІЯ

Комп'ютеризована система доступу до приміщення // Кваліфікаційна робота бакалавра // Рожик Анастасія Миколаївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних систем та мереж, група СІ-42 // Тернопіль, 2024 // с. – 58, рис. – 27, табл. – 2, аркушів А1 – 4, бібліогр. – 18.

Ключові слова: система доступу, пін-код, UART, I2C, безпека.

Під час проєктування кваліфікаційної роботи було досягнуто мети щодо реалізації комп'ютеризованої системи доступу до приміщення за допомогою пін-коду. Використання сучасних методів і засобів забезпечення безпеки, таких як протоколи UART та I2C, дозволяє створити надійну та ефективну систему контролю доступу.

Апаратне забезпечення проєкту включає модуль введення пін-коду, який дозволяє користувачеві вводити персональний ідентифікаційний номер для доступу до приміщення; uart та i2c протоколи, які забезпечують надійну та швидку комунікацію між компонентами системи; датчики стану дверей, які контролюють відкриття та закриття дверей, забезпечуючи додатковий рівень безпеки; та мікроконтролер, який виконує налаштування та розподілення команд до основних компонентів системи.

Програмне забезпечення розроблено на основі мови програмування C/C++, використовуючи відкриті бібліотеки, що забезпечують стабільну роботу системи та її інтеграцію з іншими компонентами. Система підтримує функції автентифікації користувачів, реєстрації нових користувачів, та ведення журналу доступу для забезпечення прозорості та контролю.

ANNOTATION

Computerized access system to the premises // Bachelor's thesis // Rozhyk Anastasiia Mykolaivna // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Systems and Networks, group CI-42 // Ternopil, 2024 // p. - 58, fig. - 27, tables - 2, sheets A1 - 4, bibliography - 18 .

Keywords: access system, pin code, UART, I2C, security.

During the design of the qualification work, the goal of implementing a computerized access system to the premises using a pin code was achieved. The use of modern security methods and tools, such as uart and i2c protocols, allows you to create a reliable and efficient access control system.

The hardware of the project includes a pin code input module that allows the user to enter a personal identification number to access the premises; uart and i2c protocols that provide reliable and fast communication between system components; door status sensors that monitor door opening and closing, providing an additional level of security; and a microcontroller that configures and distributes commands to the main components of the system.

The software is developed on the basis of the C/C++ programming language, using open libraries that ensure stable operation of the system and its integration with other components. The system supports user authentication, new user registration, and access logging to ensure transparency and control.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ.....	9
1.1 Аналіз вимог до комп'ютерної системи.....	9
1.1.1 Загальні вимоги.....	9
1.1.2 Мета створення системи.....	9
1.1.3 Основні задачі та функції системи.....	10
1.1.4 Вимоги до системи.....	10
1.2 Аналіз можливих рішень поставленого завдання.....	12
1.2.1 Використання мікроконтролерів.....	12
1.2.2 Види клавіатур для введення коду.....	14
1.2.3 Використання світлодіодних індикаторів.....	14
1.2.4 Роль сервоприводів у системах доступу.....	14
1.2.6 Програмне забезпечення та інструменти розробки.....	15
1.2.7 Використання сканера зчитування відбитків пальців.....	16
1.2.8 Огляд аналогів системи.....	17
РОЗДІЛ 2 ПРОЕКТНА ЧАСТИНА.....	20
2.1 Розробка узагальненої структури комп'ютерної системи.....	20
2.1.1 Загальна архітектура системи.....	20
2.1.2 Взаємодія компонентів системи.....	20
2.2.1 Вибір мікроконтролера.....	21
2.2.2 Дисплей.....	27
2.2.3 Сервопривід.....	28
2.2.4 Сканер зчитування відбитків пальців.....	29

					КС КРБ 123.130.00.00 ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Комп'ютеризована система доступу до приміщення	Літ.	Арк..	Акрушів
Розроб.		Рожик А.М.				5		
Перевір.		Жаровський Р.О.						
Рецез.		Бреус В. М.						
Н. контр.		Тиш Є.В.						
Зав.каф		Осухівська Г.М.			ТНТУ, каф. КС, гр. СІ-42			

2.3 Реалізація алгоритму системи доступу до приміщення.....	32
2.3.1 Режими системи	32
2.3.2 Протоколи UART та I2C	33
2.3.3 Процес обробки та відображення даних.....	34
2.3.4 Блок-схема алгоритму	34
2.4 Проектування комп'ютерного засобу.....	34
2.4.1 Вибір апаратних компонентів.....	34
2.4.2 Опис UART та I2C протоколів	36
РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА	37
3.1 Реалізація або моделювання проектних рішень	37
3.1.1 Обґрунтування вибору середовища розробки	37
3.1.2 Детальний опис роботи програми	39
3.2 Тестування системи доступу до приміщення	46
РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ	49
4.1 Психологічні чинники небезпеки	49
4.2 Долікарська допомога при ураженні електричним струмом.....	52
ВИСНОВКИ.....	57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	58
Додаток А	60
Додаток Б.....	65
Додаток В	67

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК СКОРОЧЕНЬ

ADC – Analog-to-Digital Converter

EEPROM – Electrically Erasable Programmable Read-Only Memory

GPIO – General-Purpose Input/Output

I2C – Inter-Integrated Circuit

IDE – Integrated Development Environment

LCD – Liquid Crystal Display

LED – Light Emitting Diode

PWM – Pulse Width Modulation

RFID – Radio Frequency Identification

ROM – Read-Only Memory

SPI – Serial Peripheral Interface

SRAM – Static Random Access Memory

UART – Universal Asynchronous Receiver/Transmitter

USB – Universal Serial Bus

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Сучасний світ знаходиться на стадії активного розвитку технологій, які проникають у всі сфери життя людини. Однією з ключових потреб кожного є безпека житла, що зумовлює попит на ефективні та надійні системи захисту. Однією з таких систем є комп'ютеризована система доступу до приміщень, що дозволяє забезпечити високий рівень безпеки, використовуючи сучасні технології.

Захист будинку чи офісу стає все більш актуальною проблемою у зв'язку зі зростанням числа випадків крадіжок та несанкціонованого проникнення. Традиційні механічні замки поступово поступаються місцем електронним системам, які забезпечують кращий рівень захисту та пропонують більший комфорт у використанні. В цьому контексті комп'ютеризована система доступу, що використовує 4-значний код, є відмінним рішенням для багатьох користувачів.

Розробка даної системи спрямована на створення зручного, доступного та надійного засобу захисту приміщень. Вона включає в себе введення коду за допомогою мембранної клавіатури, активацію серводвигуна для відкриття дверей, реалізацію двох режимів закриття, а також звукову та індикаційну сигналізацію. Комплексний підхід до розробки даної системи дозволяє вирішити основні завдання, пов'язані з безпекою житла.

Розробка такої системи потребує комплексного підходу, що включає аналіз вимог, проектування, програмування, налаштування апаратних компонентів, а також тестування системи на надійність та безпеку. Важливим аспектом є також врахування можливості подальшої модернізації та адаптації системи до різних умов експлуатації.

Система дозволить користувачам бути впевненими у надійності захисту своїх приміщень, що є ключовим фактором у забезпеченні комфортного та спокійного життя.

					КС КРБ 123.130.00.00 ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Аналіз вимог до комп'ютерної системи

1.1.1 Загальні вимоги

Система комп'ютеризованого доступу до приміщення призначена для забезпечення безпеки та контролю доступу до будівлі шляхом використання чотиризначного коду або біометричними даними. Вона покликана:

- запобігати несанкціонованому доступу до приміщення;
- забезпечувати зручність і простоту у використанні для авторизованих користувачів;
- мінімізувати ризик втрати або крадіжки ключів.

Система використовується для захисту житлових будинків, офісів, складів та інших приміщень, де необхідно контролювати доступ. Основною метою є надання авторизованим особам швидкого та безпечного доступу, водночас блокуючи можливості для несанкціонованого проникнення.

1.1.2 Мета створення системи

Мета розробки комп'ютеризованої системи доступу полягає у створенні ефективного і надійного рішення для захисту приміщення. Основними завданнями системи є:

- забезпечення високого рівня безпеки за рахунок використання чотиризначного коду або біометричних даних;
- спрощення процесу авторизації користувачів;
- надання можливості швидкого і зручного змінення коду доступу у разі необхідності;

Змн.	Арк.	№ докум.	Підпис	Дата	КС КРБ 123.130.00.00 ПЗ			
Розроб.		Рожик А.М.			Аналіз технічного завдання	Літ.	Арк..	Акрушів
Перевір.		Жаровський Р.О.					9	
Рецез.		Бревус В. М.				ТНТУ, каф. КС, гр. СІ-42		
Н. контр.		Тиш Є.В.						
Зав.каф		Осухівська Г.М.						

– інформування користувачів про статус системи за допомогою звукових і світлових індикаторів.

Система повинна мати можливість оперативного реагування на введений код, забезпечуючи при цьому високу точність і швидкодію. Крім того, важливою є здатність системи фіксувати спроби несанкціонованого доступу, щоб запобігти потенційним загрозам.

1.1.3 Основні задачі та функції системи

Основні функції системи комп'ютеризованого доступу включають:

- введення чотиризначного коду користувачем;
- контроль і верифікація введеного коду;
- активація сервоприводу для відкриття дверей у разі введення правильного коду;
- використання світлодіодних індикаторів для візуального підтвердження правильності введеного коду;
- видача звукового сигналу для підтвердження дій користувача;
- наявність двох режимів закриття дверей для забезпечення додаткової безпеки;
- визначення стану дверей.

Кожна з цих функцій спрямована на забезпечення ефективної та безпечної роботи системи. Наприклад, світлодіодні індикатори дозволяють користувачам отримувати миттєвий зворотний зв'язок про стан системи, а звукові сигнали допомагають підтвердити правильність або помилковість введеного коду.

1.1.4 Вимоги до системи

При розробці системи комп'ютеризованого доступу до приміщення враховуються наступні вимоги:

- система повинна забезпечувати високий рівень захисту від несанкціонованого доступу;

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		10

- інтерфейс системи повинен бути інтуїтивно зрозумілим і простим для користувачів;
- система повинна оперативно реагувати на введення коду і виконувати відповідні дії;
- можливість швидкого змінення коду доступу у разі необхідності;
- система повинна мати низьке споживання енергії для забезпечення тривалої роботи без необхідності частого обслуговування.

Надійність включає використання компонентів високої якості, стійких до зношування і механічних пошкоджень. Зручність у використанні передбачає простий інтерфейс і чіткі інструкції для користувачів, що дозволяє зменшити кількість помилок при введенні коду.

Швидкодія системи досягається завдяки використанню сучасних мікроконтролерів і оптимізованих алгоритмів обробки даних. Гнучкість важлива для адаптації системи до різних умов експлуатації, а інформаційність забезпечує зручність використання завдяки наданню зрозумілої інформації про стан системи.

Нарешті, енергоефективність є ключовим фактором для автономних систем, що працюють на батареях або мають обмежене енергоспоживання. Використання енергоефективних компонентів і оптимізація енергоспоживання дозволяє збільшити час безперервної роботи системи.

Діагностика цілісності програмного забезпечення виконується щоразу під час увімкнення системи перед початком виконання основних функцій. Цей процес забезпечує перевірку всіх ключових компонентів і алгоритмів на наявність помилок і несправностей. Якщо виявлено збої у роботі, система негайно повідомляє про знайдені помилки, забезпечуючи можливість їх швидкого усунення. Таким чином, кожен користувач може бути впевнений у безперебійній роботі пристрою, що є критично важливим для стабільного функціонування всієї системи.

Перспективи розвитку даної комп'ютеризованої системи включають її інтеграцію як додаткового модуля у наявні великі системи для загального або

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

особистого використання. Систему можна застосовувати в різних галузях, адаптуючи її до різних сценаріїв із більшою чи меншою кількістю керуючих світлодіодів матриці чи інших компонентів. Така гнучкість дозволяє налаштовувати систему під конкретні потреби користувачів і розширювати її функціональні можливості.

Крім того, система підлягає модернізації у випадку недостатньої ефективності або для доповнення функціональності відповідно до вимог та потреб користувача. Цей процес може включати оновлення програмного забезпечення, додавання нових апаратних компонентів або зміни в архітектурі системи для підвищення її продуктивності. Модернізація дозволяє не лише подовжити життєвий цикл пристрою, але й зробити його більш ефективним та зручним у використанні, що є важливим для задоволення потреб сучасних користувачів.

1.2 Аналіз можливих рішень поставленого завдання

1.2.1 Використання мікроконтролерів

Мікроконтролери, такі як Arduino Uno, є основними компонентами у побудові систем комп'ютеризованого доступу. Вони забезпечують:

- обробку введених даних з клавіатури або з датчика відбитків палців;
- контроль роботи світлодіодних індикаторів і сервоприводів;
- реалізацію алгоритмів перевірки коду і активації відповідних дій.

Мікроконтролери є основою будь-якої комп'ютеризованої системи доступу. Вони виконують обробку введених даних, контроль роботи вихідних пристроїв, таких як світлодіоди і сервоприводи, а також реалізують логіку системи. Arduino Uno, зокрема, обраний завдяки своїй простоті у використанні, наявності великої кількості бібліотек для підключення різноманітних датчиків і актуаторів, а також широкій спільноті підтримки [4].

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

Основні характеристики Arduino Uno, які роблять його придатним для даного проєкту, включають:

- 16 МГц тактова частота, яка забезпечує достатню швидкість для обробки введених даних і управління вихідними пристроями;
- 14 цифрових входів/виходів, що дозволяють підключити необхідні компоненти, такі як клавіатура, світлодіоди, сервоприводи і звукові пристрої;
- 6 аналогових входів, які можуть бути використані для підключення додаткових датчиків, якщо це необхідно;
- простота програмування за допомогою мови програмування C++ і середовища розробки Arduino IDE.

UML-діаграма системи зображена на рис.1.1.

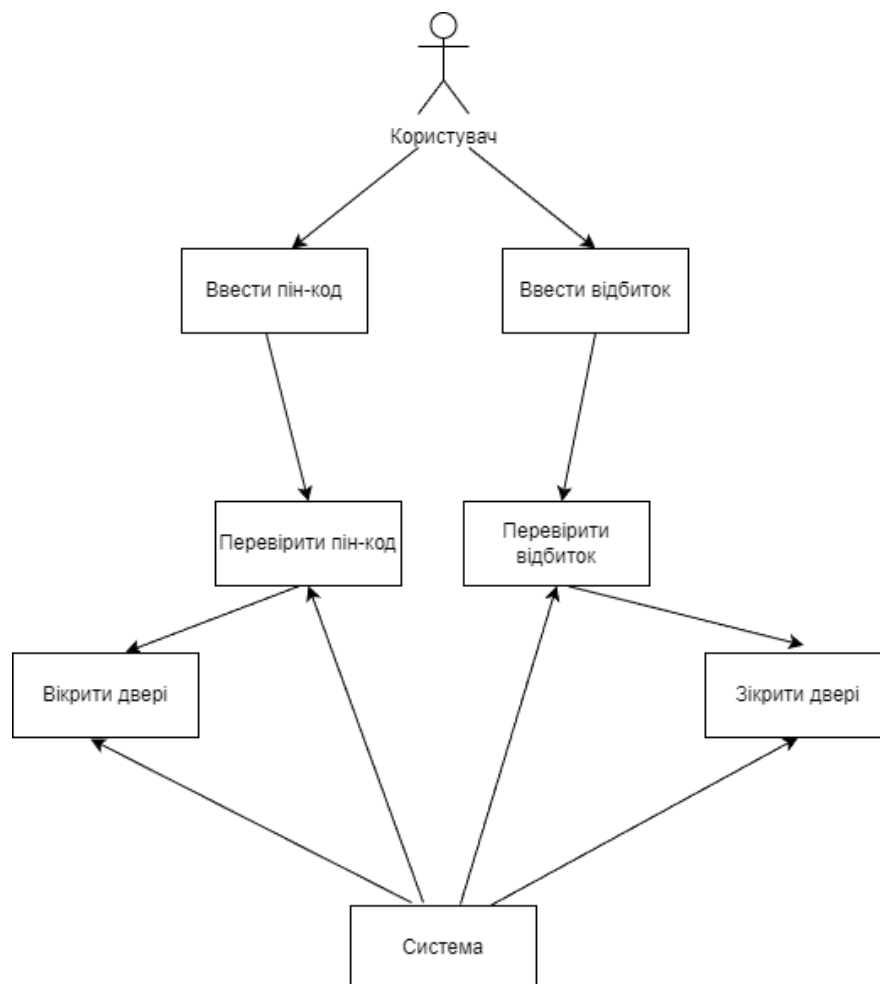


Рисунок 1.1 – UML-діаграма системи

1.2.2 Види клавіатур для введення коду

Матричні клавіатури, наприклад, 4x4 Keypad, широко використовуються для введення даних користувачем. Вони забезпечують:

- простоту інтеграції з мікроконтролерами;
- зручність у використанні;
- можливість введення великої кількості комбінацій кодів.

4x4 Keypad є популярним вибором завдяки своїй простоті і ефективності. Вона складається з 16 кнопок, розташованих у матричній конфігурації 4x4. Ця клавіатура забезпечує легкий і зручний спосіб введення чотиризначного коду, що є важливим для користувачів системи.

Клавіатура підключається до мікроконтролера через матричну конфігурацію, що дозволяє зменшити кількість необхідних входів/виходів. Введені дані обробляються за допомогою спеціальних бібліотек, які спрощують інтеграцію і забезпечують надійну роботу системи.

1.2.3 Використання світлодіодних індикаторів

Світлодіодні індикатори червоного і зеленого кольорів використовуються для:

- візуального інформування користувачів про статус системи;
- підтвердження правильності або помилковості введеного коду;
- індикації режимів роботи системи.

Світлодіодні індикатори є важливим елементом для забезпечення зворотного зв'язку з користувачем. Вони дозволяють миттєво інформувати користувача про правильність або помилковість введеного коду, а також про інші стани системи.

1.2.4 Роль сервоприводів у системах доступу

Сервоприводи відіграють ключову роль у механізмі відкриття дверей. Вони забезпечують:

- точність і надійність відкриття і закриття дверей;

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		14

- можливість реалізації різних режимів роботи;
- низьке енергоспоживання при високій потужності і швидкодії.

Сервоприводи використовуються для механічного відкриття і закриття дверей після введення правильного коду.

Основні переваги використання сервоприводів у системах доступу включають:

- високу точність позиціонування, що дозволяє надійно керувати механізмом дверей;
- низьке енергоспоживання, що є важливим для автономних систем;
- швидкодію, що забезпечує оперативне відкриття і закриття дверей.

Вони є ідеальним вибором завдяки своїй точності, надійності і енергоефективності. Сервоприводи можуть бути легко інтегровані з мікроконтролером і керовані за допомогою стандартних бібліотек.

1.2.6 Програмне забезпечення та інструменти розробки

Для розробки програмного забезпечення системи використовується Arduino Integrated Development Environment (IDE). Arduino IDE є офіційним середовищем розробки для платформ Arduino, яке підтримує написання, редагування та компіляцію коду, а також завантаження програм на мікроконтролери.

Основні характеристики Arduino IDE:

- простота у використанні; інтуїтивно зрозумілий інтерфейс дозволяє швидко розпочати роботу навіть початківцям;
- кросплатформеність; підтримка операційних систем Windows, macOS та Linux;
- багата бібліотека; наявність великої кількості готових бібліотек для різних датчиків і модулів;
- відкритий код; програмне забезпечення з відкритим кодом, що дозволяє модифікувати і адаптувати його під конкретні потреби.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		15

Основна мова програмування для розробки програмного забезпечення системи – це C/C++. Ця мова є стандартом для розробки вбудованих систем завдяки своїй ефективності та можливості працювати з низькорівневими ресурсами мікроконтролера.

Мови програмування C/C++ є важливою складовою розробки програмного забезпечення для систем. Вони відомі своєю високою продуктивністю, що дозволяє писати швидкодіючий код, особливо в контексті вбудованих систем, де ефективність виконання є критичною.

Однією з основних особливостей C/C++ є можливість роботи з апаратним забезпеченням на низькому рівні, що дозволяє розробникам маніпулювати низькорівневими ресурсами мікроконтролера. Це робить їх відмінним вибором для вбудованих систем.

Крім того, C/C++ мають велику спільноту, яка надає значну кількість прикладів і готових рішень, що полегшують розробку. Вони також підтримують об'єктно-орієнтоване програмування, багатопоточність і дозволяють розробникам ефективно керувати пам'яттю.

Завдяки широким можливостям та високій продуктивності, мови програмування C/C++ залишаються одними з найпопулярніших і потужних інструментів для розробки програмного забезпечення систем [3].

Особливості мови C/C++:

- простота та компактність;
- висока продуктивність.

Ці особливості роблять мову C універсальною та ефективною для широкого спектра застосувань, від системного до прикладного програмування.

1.2.7 Використання сканера зчитування відбитків пальців

Сканер відбитків пальців здійснює зчитування поверхні пальця, використовуючи оптичні, ємнісні або ультразвукові технології. Зчитані дані обробляються та зберігаються у вигляді цифрових шаблонів, які використовуються для подальшої ідентифікації. При прикладанні пальця до

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

сканера, система порівнює отриманий відбиток із збереженими шаблонами. У випадку збігу, користувачу надається доступ до приміщення.

Використання сканера зчитування відбитків пальців у нашій системі забезпечує високий рівень безпеки та зручність користування, що робить її ефективним рішенням для контролю доступу до приміщень різного типу.

Використання біометричних даних для ідентифікації користувачів дозволяє значно підвищити рівень безпеки порівняно з традиційними методами, такими як ключі чи картки. Біометрична автентифікація ґрунтується на унікальності відбитків пальців кожної людини, що робить підробку або крадіжку доступу практично неможливими.

1.2.8 Огляд аналогів системи

Для розробки системи необхідно ознайомитися з існуючими аналогами, щоб врахувати їхні переваги та недоліки. На сьогоднішній день існує кілька аналогів комп'ютеризованої системи доступу до приміщення.

Однією з найпоширеніших технологій, використовуваних у системах доступу, є технологія RFID (Radio Frequency Identification). Ця технологія дозволяє користувачам отримати доступ до приміщення за допомогою RFID-карт або брелоків, які взаємодіють з RFID-зчитувачем, встановленим на дверях.

Приклад роботи RFID зображено на рис.1.2.



Рисунок 1.2 – Приклад роботи RFID

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		17

Переваги:

- користувачам не потрібно пам'ятати та вводити код, достатньо лише мати при собі RFID-карту або брелок;
- процес авторизації займає лише кілька секунд.
- можливість налаштування рівнів доступу для різних користувачів.

Недоліки:

- залежність від фізичного носія: якщо карта або брелок буде загублено, доступ до приміщення буде ускладнений;
- необхідність придбання додаткових RFID-карт або брелоків для кожного користувача.

Кодові системи доступу, подібні до тієї, яку планується розробити, використовують числовий код для авторизації користувача. Це один з найпростіших і найбільш поширених способів контролю доступу.

Приклад кодової системи доступу зображено на рис 1.3.



Рисунок 1.3 – Приклад кодової системи доступу

Переваги:

- відсутність необхідності у додаткових пристроях або картках;
- можливість легко змінювати коди доступу.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

Недоліки:

– необхідність пам'ятати код може бути незручною для деяких користувачів.

Смарт-системи доступу використовують сучасні технології, такі як мобільні додатки, Wi-Fi, Bluetooth або NFC для забезпечення доступу до приміщення. Користувачі можуть керувати доступом за допомогою своїх смартфонів або інших мобільних пристроїв. Приклад смарт-системи доступу зображено на рис.1.4.



Рисунок 1.4 – Приклад смарт-системи доступу

Переваги:

- керування доступом зі смартфона дозволяє користувачам відкривати двері без необхідності носити додаткові пристрої або пам'ятати коди;
- можливість інтеграції з іншими смарт-пристроями та системами управління будинком.

Недоліки:

- у разі збоїв у роботі мобільного пристрою або мережі доступ до приміщення може бути ускладнений.
- вартість таких систем може бути вищою через необхідність використання спеціалізованого обладнання та програмного забезпечення.
- необхідність захисту мобільних додатків від зломів та вірусів.

					КС КРБ 123.130.00.00 ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТНА ЧАСТИНА

2.1 Розробка узагальненої структури комп'ютерної системи

2.1.1 Загальна архітектура системи

Комп'ютеризована система доступу до приміщення складається з кількох основних компонентів. Центральним елементом є мікроконтролер Arduino Uno, який обробляє введені дані та керує іншими компонентами. Для введення чотиризначного коду використовується матрична клавіатура Keypad 4x4. Візуальна індикація стану системи здійснюється за допомогою світлодіодних індикаторів червоного і зеленого кольорів. Сервопривід забезпечує механічне відкриття і закриття дверей, а п'єзоелектричний пристрій генерує звукові сигнали. Перемикач режимів дозволяє змінювати стан системи між режимами очікування та активного контролю доступу. Для відображення символічної інформації про стан системи використовується LCD дисплей 16x2.

2.1.2 Взаємодія компонентів системи

Компоненти системи взаємодіють наступним чином. Користувач вводить чотиризначний код за допомогою клавіатури Keypad 4x4, після чого введені дані передаються на мікроконтролер. Arduino Uno обробляє ці дані, перевіряючи правильність коду. Якщо код правильний, мікроконтролер активує сервопривід для відкриття дверей і загоряється зелений світлодіод, підтверджуючи успішний доступ.

У випадку неправильного коду, загоряється червоний світлодіод і п'єзоелектричний пристрій генерує звуковий сигнал, інформуючи користувача про помилку.

					КС КРБ 123.130.00.00 ПЗ		
					Проектна частина		
Змн.	Арк.	№ докум.	Підпис	Дата	Літ.	Арк.	Акрушів
Розроб.		Рожик А.М.				20	
Перевір.		Жаровський Р.О.					
Рецез.		Бревус В. М.					
Н. контр.		Тиш Є.В.					
Зав.каф		Осухівська Г.М.					
					ТНТУ, каф. КС, гр. СІ-42		

LCD дисплей 16x2 використовується для відображення інформації про стан системи, наприклад, "Введіть код" або "Неправильний код".

Готова спроектована схема структури комп'ютеризованої системи зображена на рис. 2.1.

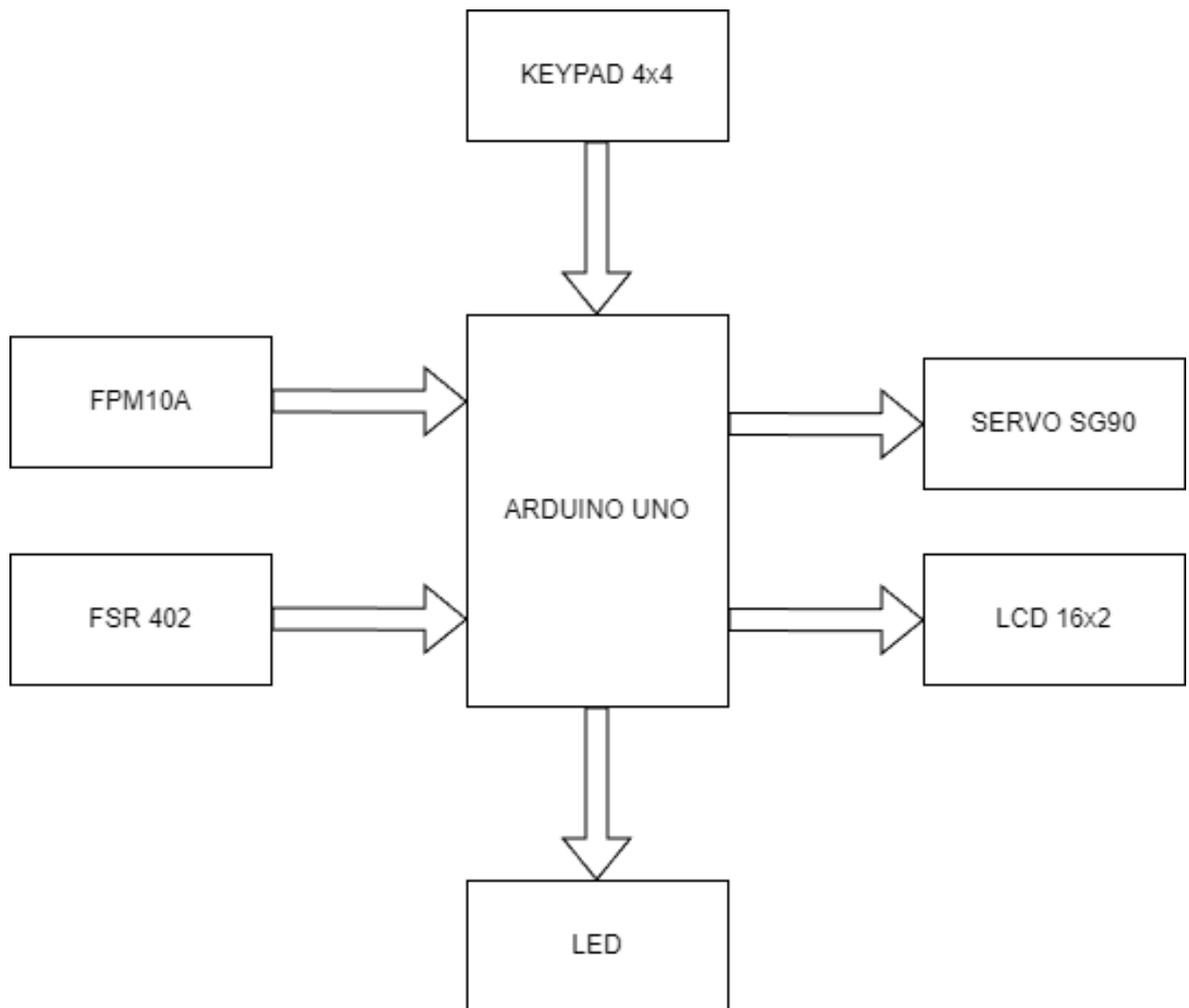


Рисунок 2.1 – Структурна схема спроектованої системи

2.2.1 Вибір мікроконтролера

Для реалізації системи було обрано мікроконтролер Arduino Uno. Цей вибір обґрунтовано його простотою у використанні, наявністю достатньої кількості входів/виходів, потужністю і швидкодією, а також широкою підтримкою спільноти. Arduino Uno є популярним мікроконтролером, який легко інтегрується з різними компонентами та забезпечує надійну роботу системи.

Його простота у використанні та доступність роблять його ідеальним вибором для проектування системи доступу до приміщення. Основні технічні характеристики плати наведено у табл. 2.1.

Таблиця 2.1 – Основні технічні характеристики Arduino Uno

Характеристика	Значення
Мікроконтролер	АТМega328P
Частота процесора	16 МГц
Пам'ять	32 Кб (Flash), 2 Кб (SRAM)
Вхідні/вихідні	14 ДВЧ, 6 ДВХ
Підтримка протоколів	UART, SPI, I2C, I2S
Підтримка оперативної системи	Windows, macOS, Linux

Вигляд плати зображено на рис. 2.2

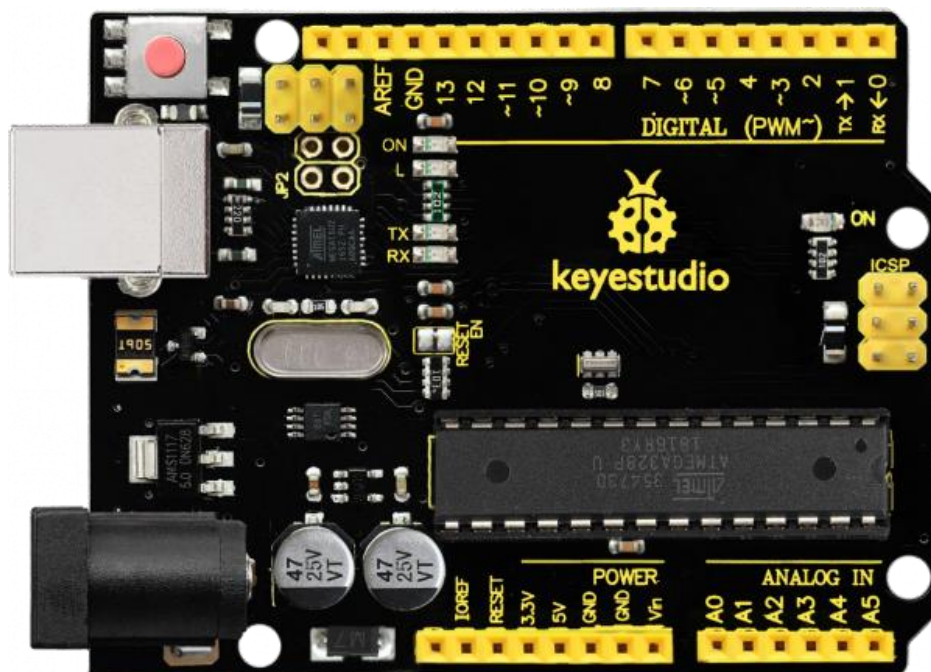


Рисунок 2.2 – Вигляд мікроконтролерної плати Arduino Uno R3

Мікроконтролер Atmel ATmega328P це високоякісний 8-бітний пристрій типу megaAVR, базується на архітектурі RISC (Reduced Instruction Set

Computing), удосконаленій для AVR. Ці конкретні мікроконтролери входять до категорії найбільш розповсюджених у лінійці AVR та виявилися ефективними в різноманітних областях застосування. Розпіновка ATmega328P ілюструється на рис. 2.3.

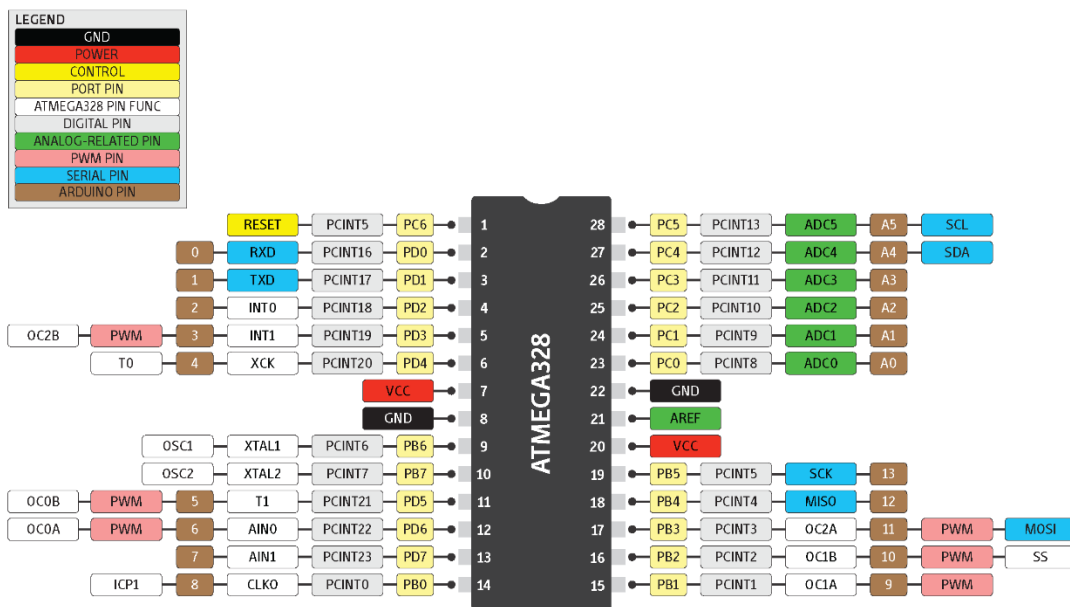


Рисунок 2.3 – Розпіновка ATmega328

Порт В (PB7:0), відомий також як XTAL1/XTAL2/TOSC1/TOSC2, є 8-розрядним двонаправленим портом введення/виведення, що включає в себе внутрішні підтягуючі резистори, кожен з яких може бути активований для кожного біта. Вихідні буфери порту В мають симетричні характеристики приводу з високою здатністю до споживання та джерела струму. У разі, коли виводи порту В підключені до низького рівня, вони функціонують як джерела струму за умови активованих внутрішніх підтягуючих резисторів. Виводи порту В мають три стани, які активуються у разі скидання, навіть у випадку, коли годинник не активний.

В залежності від налаштувань запобіжника для вибору тактового сигналу, вивід PB6 може використовуватися як вхід для підсилювача інверторного генератора або як вхід для робочої схеми внутрішнього генератора. Залежно від

Змн.	Арк.	№ докум.	Підпис	Дата

налаштувань запобіжника для вибору тактової частоти, PB7 може використовуватися як вихідний сигнал від підсилювача інверторного генератора.

Якщо внутрішній калібрований RC-генератор використовується як джерело тактового сигналу мікросхеми, вивід PB7..6 використовується як вхід TOSC2..1 для асинхронного таймера/лічильника², за умови встановлення біту AS2 в регістрі ASSR.

Порт С (PC5:0) складається з 7-розрядного двонаправленого порту введення/виведення з внутрішніми підтягуючими резисторами, які можуть бути активовані для кожного біта. Вихідні буфери PC5..0 також мають симетричні характеристики приводу з високою здатністю до споживання та джерела струму. Аналогічно до порту В, виводи порту С мають три стани, які активуються у разі скидання, навіть у випадку, коли годинник не активний.

PC6/RESET використовується як контакт вводу/виведення, якщо біт RSTDISBL вибраного запобіжника запрограмований. У випадку, коли RSTDISBL не запрограмований, PC6 використовується як вхід скидання. Низький рівень на цьому контакті протягом тривалого часу спричинить скидання, навіть у випадку, коли годинник не активний.

Порт D (PD7:0) складається з 8-розрядного двонаправленого порту введення/виведення з внутрішніми підтягуючими резисторами, які можуть бути активовані для кожного біта. Вихідні буфери порту D мають симетричні характеристики приводу з високою здатністю до приймання та джерела струму. Аналогічно до портів В і С, виводи порту D мають три стани, які активуються у разі скидання, навіть у випадку, коли годинник не активний.

Контакт AVCC призначений для живлення аналого-цифрового перетворювача (АЦП), а також для виводів PC3:0 та ADC7:6. Навіть якщо АЦП не використовується, він повинен бути підключений до вихідного контакту живлення VCC. У випадку використання АЦП, його слід підключити до VCC через фільтр низьких частот. Зверніть увагу, що виводи PC6..4 отримують живлення від VCC.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		24

AREF — аналоговий еталонний контакт для аналого-цифрового перетворювача.

ADC7:6 (лише для пакетів TQFP і QFN/MLF). У пакетах TQFP і QFN/MLF ADC7:6 служать аналоговими входами для АЦП. Ці контакти живляться від аналогового джерела живлення і служать 10-розрядними каналами АЦП.

У таблиці 2.2 наведено технічні характеристики мікроконтролера ATMEGA328P.

Таблиця 2.2 – технічні характеристики мікроконтролера ATMEGA328P

Параметр	Значення
Живлення, В	1,8-5,5
Тип ядра	AVR
Розрядність	8-Bit
Частота	20MHz
Робоча температура, °C	-40-+85°C
Ширина шини даних	8-біт
Тактова частота	20 мГц
Кількість входів/виходів	23
Об'єм пам'яті програм	32 кбайт (16k x 16)
Тип пам'яті програм	Flash
Об'єм EEPROM	1k x 8
Об'єм RAM	2k x 8
Наявність АЦП/ЦАП	АЦП 6x10b
Вбудовані інтерфейси	I2C, SPI, UART
Вбудована периферія	Brown-out detect/reset, POR, PWM, WDT
Напруга живлення	1.8-5.5
Робоча температура	-40-+85°C
Корпус	DIP-28

Ядро AVR це високоефективне 8-розрядне ядро з архітектурою RISC, що розроблене компанією Atmel (зараз Microchip Technology). Воно відоме своїм різноманітним набором інструкцій та високою швидкістю виконання завдань. Особливістю ядра є прямий доступ універсальних регістрів до арифметико-логічного пристрою (ALU), що дозволяє виконувати операції з двома регістрами за один тактовий цикл, що покращує продуктивність і знижує споживання енергії.

ATmega328P виготовлений з використанням технології високої щільності енергонезалежної пам'яті від компанії Atmel. Інтегрована флеш-пам'ять з підтримкою інтерфейсу ISP (In-System Programming) дозволяє перепрограмувати пам'ять безпосередньо у системі через інтерфейс SPI або з використанням зовнішніх програматорів. Наявність вбудованого завантажувача із підтримкою Boot Flash дозволяє оновлювати програмне забезпечення без переривання основних функцій пристрою.

Режим очікування зупиняє центральний процесор, але дозволяє SRAM, таймерам/лічильникам, USART, 2-провідному послідовному інтерфейсу, порту SPI та системі переривань продовжувати роботу. Режим вимкнення зберігає вміст регістрів, зупиняючи осцилятор і відключаючи всі інші функції мікросхеми до наступного переривання або апаратного скидання. У режимі енергозбереження асинхронний таймер продовжує працювати, підтримуючи базу таймера, поки решта пристрою знаходиться у сплячому режимі. Режим зменшення шуму АЦП зупиняє центральний процесор і всі модулі введення/виведення, крім асинхронного таймера та АЦП, щоб мінімізувати шум перемикання під час перетворення. У режимі очікування кварцовий/резонаторний осцилятор працює, тоді як решта пристрою спить, забезпечуючи швидкий запуск при низькому енергоспоживанні.

Виробництво пристрою виконано з використанням технології високої щільності енергонезалежної пам'яті від Atmel. Вбудована флеш-пам'ять ISP забезпечує можливість перепрограмування пам'яті безпосередньо у системі через послідовний інтерфейс SPI, звичайним програматором або вбудованим

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

завантажувачем, що працює на ядрі AVR. Завантажувач підтримує використання будь-якого інтерфейсу для завантаження прикладних програм у флеш-пам'ять. Програмне забезпечення, що знаходиться в розділі Boot Flash, продовжує свою роботу під час оновлення розділу Application Flash, забезпечуючи можливість читання під час запису нових даних.

Поєднання 8-розрядного процесора RISC із внутрішньосистемною самопрограмованою флеш-пам'яттю на одному чіпі робить Atmel ATmega328P потужним мікроконтролером, який забезпечує гнучке та економічно ефективне рішення для багатьох вбудованих додатків керування. ATmega328P підтримується повним набором засобів розробки, включаючи компілятори C, асемблери макросів, налагоджувачі програм/симулятори, внутрішньосхемні емулятори та комплекти оцінки.

2.2.2 Дисплей

Дисплей розміром 16x2 базується на контролері HD44780 від японської компанії Hitachi. Контролер має однобайтні комірки пам'яті, вміст яких відображається на екрані. На рис. 2.4 зображено загальний вигляд LCD 16x2.

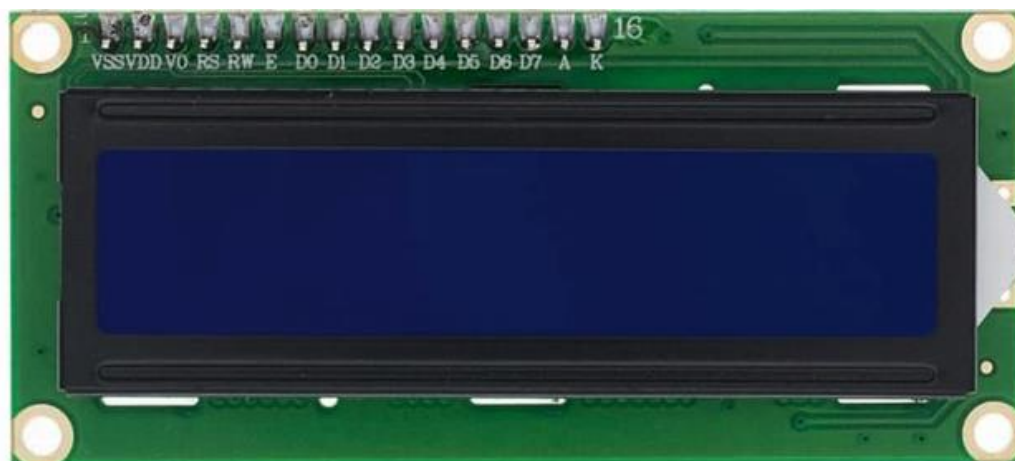


Рисунок 2.4 – Загальний вигляд LCD 16x2

Рідкокристалічний дисплей 1602A відображає два рядки по 16 символів кожен. Символи мають роздільну здатність 5x8 пікселів, хоча більшість

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		27

стандартних символів використовують роздільну здатність 5x7. Нижній рядок використовується для відображення курсору у вигляді підкреслення. Курсор може мати вигляд заповненого поля 5x8 пікселів, бути увімкненим/вимкненим або блимати [6].

LCD дисплей може працювати у 2 режимах:

- 4-бітному, де за 1 такт передається 0.5 байта, використовуючи контакти від D4 до D7;
- 8-бітному, де за 1 такт передається 1 байт, використовуючи контакти від D0 до D7.

2.2.3 Сервопривід

Сервопривід — це пристрій, який використовується в системах автоматичного керування або дистанційного управління для здійснення точного механічного переміщення регулюючого органу відповідно до вхідного сигналу з системи керування. Основна функція сервоприводу полягає в забезпеченні точного керування положенням або кутом обертання, що робить його ідеальним для застосувань, де потрібна висока точність і стабільність.

Маленький цифровий сервомотор Tower Pro SG90 з металеву зубчатою передачею використовується в системах позиціонування. Він є популярним завдяки невеликій ціні, потужності та якості.

Характеристики:

- живлення: 4.8-7.2 В;
- сила: 2 кг/см (4.8 В);
- кут повороту між крайніми положеннями: 180°;
- швидкість без навантаження: 0.17 с/60° (4.8 В).

На рис. 2.5 зображено загальний вигляд Micro Servo.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		28



Рисунок 2.5 – Загальний вигляд Micro Servo SG90

2.2.4 Сканер зчитування відбитків пальців

Сканер зчитування відбитків пальців є важливою складовою комп'ютеризованої системи доступу до приміщення. Він забезпечує високий рівень безпеки та зручності, використовуючи біометричну аутентифікацію для ідентифікації користувачів. У даному підпункті розглянемо основні аспекти застосування та інтеграції сканера відбитків пальців у систему доступу.

Основні переваги використання сканера відбитків пальців:

- біометрична ідентифікація забезпечує значно вищий рівень безпеки порівняно з традиційними методами, такими як ключі або паролі, оскільки відбитки пальців є унікальними для кожної людини;
- процес сканування відбитків пальців займає всього кілька секунд, що робить його швидким і зручним для користувачів;
- відбитки пальців є складними для підробки, що додає додатковий рівень захисту від несанкціонованого доступу;
- сканери відбитків пальців можуть бути легко інтегровані з іншими компонентами системи, такими як контролери доступу, програмне забезпечення управління доступом та бази даних.

Процес роботи сканера відбитків пальців включає такі етапи:

- користувач прикладає палець до сканера, який зчитує зображення відбитка;

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		29

- отримане зображення обробляється спеціальним алгоритмом, який витягує унікальні риси відбитка пальця;
- унікальні риси зберігаються в базі даних для подальшого порівняння;
- при кожному наступному вході користувач прикладає палець до сканера, і система порівнює нове зображення з раніше збереженими даними для ідентифікації.

Інтеграція сканера відбитків пальців у комп'ютеризовану систему доступу до приміщення передбачає використання мікроконтролера для управління сканером та обробки даних. Сканер підключається до мікроконтролера через послідовний інтерфейс, такий як UART або I2C, що забезпечує надійну передачу даних [3].

На рис. 2.6 зображено загальний вигляд сканера зчитування відбитків пальців.



Рисунок 2.6 – Загальний вигляд FPM10A

2.2.5 Клавіатура

Для зменшення кількості кнопок у системі та зручного введення даних під час виконання програми використовують матричну мембранну клавіатуру.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		30

Технічні характеристики:

- розміри: 68x77x0.8 мм;
- робоча напруга: до 12 В;
- максимальний струм: 100 мА;
- опір контактів: <200 Ом;
- ресурс: 1 мільйон натискань;
- робоча температура: від 0 до +70 градусів Цельсія;
- допустима вологість: 90% - 95%, 240 годин.

Об'єднання в один модуль кількох тактових кнопок спрощує конструкцію панелі управління приладу та економить порти Arduino чи мікроконтролера. Принцип роботи такої клавіатури полягає у подачі мікроконтролером логічної одиниці на кожен з виводів 4-ох рядів, а з виводів стовпців зчитуються значення. Якщо натиснути будь-яку з кнопок, вона замкне вивід ряду і вивід стовпця, з якими пов'язана, і на відповідному виводі стовпця з'явиться логічна одиниця.

На рис. 2.7 зображено загальний вигляд Кеурпад 4x4



Рисунок 2.7 – Загальний вигляд Кеурпад 4x4

2.2.6 Датчик тиску FSR402

FSR 402 (Force Sensitive Resistor) - це тонкий, легкий датчик тиску, який змінює свій опір залежно від прикладеної сили. Цей датчик широко використовується в системах, де потрібне виявлення тиску або сили, таких як робототехніка, системи керування доступом, медичне обладнання тощо.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		31

Технічні характеристики:

- резистивний;
- діапазон тиску від 0 до 10 кг;
- робоча напруга 1-5 в;
- довжина 56 мм, ширина активної області 18 мм;
- опір без навантаження $> 1 \text{ м}\Omega$;
- опір при максимальному навантаженні $\approx 1 \text{ к}\Omega$.

Датчик FSR 402 працює за принципом зміни опору при прикладенні сили. При відсутності сили опір датчика дуже високий (понад 1 МОм). При прикладенні сили опір зменшується до 1 кОм. Це зміна опору дозволяє вимірювати силу, прикладену до датчика, за допомогою мікроконтролера.

На рис. 2.8 зображено загальний вигляд датчика тиску FSR402



Рисунок 2.8 – Загальний вигляд датчика тиску FSR402

2.3 Реалізація алгоритму системи доступу до приміщення

2.3.1 Режими системи

Після того як апаратне забезпечення задовольнило всі зазначені вимоги, наступним кроком у проектуванні системи є складання алгоритму. Щоб майбутній проєкт зміг реалізувати всі необхідні задачі, система була розділена на кілька режимів.

Один із режимів відповідає за верифікацію користувача. Верифікація здійснюється шляхом введення пін-коду на клавіатурі. Користувач вводить пін-

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		32

код, який передається до центрального контролера для перевірки. Система перевіряє отриманий код на відповідність збереженим у базі даних. Якщо введений пін-код збігається з кодом у базі даних, доступ до приміщення дозволяється. У випадку невідповідності пін-коду, система блокує доступ і повідомляє про спробу несанкціонованого входу.

Інший режим роботи системи передбачає аутентифікацію користувача через сканер відбитків пальців. Цей метод забезпечує додатковий рівень безпеки, оскільки відбиток пальця є унікальним для кожної людини. Процес аутентифікації включає наступні кроки:

- користувач прикладає палець до сканера відбитків пальців;
- сканер зчитує зображення відбитка пальця та передає його до центрального контролера;
- центральний контролер обробляє отримане зображення, порівнюючи його з раніше збереженими відбитками пальців у базі даних;
- якщо відбиток пальця збігається з одним із збережених у базі даних, доступ до приміщення дозволяється;
- у випадку невідповідності відбитка пальця, система блокує доступ і повідомляє про спробу несанкціонованого входу.

Блок схема алгоритму роботи зображена в КС КРБ 123.130.00.00 ПМ.

2.3.2 Протоколи UART та I2C

Для реалізації обміну даними між компонентами системи використовуються протоколи UART та I2C.

UART забезпечує двонаправлений послідовний зв'язок через два дроти: TX (передача) і RX (прийом); простота використання і налаштування; підтримка різних швидкостей передачі даних; можливість передачі даних на великі відстані.

I2C дозволяє підключати кілька пристроїв до одного мікроконтролера за допомогою лише двох ліній: SDA (дані) і SCL (синхронізація); підтримка підключення до 127 пристроїв до однієї шини; можливість використання як для

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		33

внутрішньосистемного, так і для міжсистемного зв'язку; висока швидкість передачі даних.

Використання протоколів UART та I2C забезпечує наступні переваги:

UART: простота реалізації та налаштування; підтримка різних швидкостей передачі даних; можливість передачі даних на великі відстані;

I2C: можливість підключення великої кількості пристроїв до однієї шини; висока швидкість передачі даних; зручність у внутрішньосистемному та міжсистемному зв'язку.

Розроблена комп'ютеризована система доступу до приміщення є надійним та ефективним рішенням, яке забезпечує високий рівень безпеки та зручність використання. Вона поєднує в собі сучасні технології і гнучкість налаштувань.

2.3.3 Процес обробки та відображення даних

Для ефективного управління та відображення даних використовуються внутрішньосистемні програмовані функції мікроконтролера. Зокрема, використовується 32 Кбайт внутрішньосистемної програмованої флеш-пам'яті для зберігання програм, а також 2 Кбайт SRAM для оперативного зберігання даних під час виконання програми.

2.3.4 Блок-схема алгоритму

Проаналізувавши перелік задач, які повинна виконувати комп'ютеризована система доступу, було складено блок-схему алгоритму функціонування. Основний алгоритм представлено на додатку Б.

2.4 Проектування комп'ютерного засобу

2.4.1 Вибір апаратних компонентів

Після того як апаратне забезпечення задовольнило всі зазначені вимоги, наступним кроком проектування системи є проектування комп'ютерного засобу.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		34

Цей процес включає вибір апаратних компонентів, розробку електричних схем, створення прототипу, а також тестування і верифікацію функціональності.

Основні компоненти системи включають:

- ATmega328P, який забезпечує необхідну обчислювальну потужність і має достатню кількість вхідних та вихідних ліній;
- UART та I2C протоколи для забезпечення зв'язку між компонентами системи;
- сервомотори SG90 для закриття чи відкриття дверей;
- LCD екран для відображення інформації про систему;
- світлодіоди для відображення стану системи;
- стабілізоване джерело для забезпечення безперебійної роботи всіх компонентів.

Кожен з цих елементів є критично важливим для забезпечення надійності та ефективності кінцевого продукту.

Розробка електричних схем починається з визначення всіх з'єднань між компонентами системи. Основні схеми включають:

- забезпечує стабільне електроживлення для всіх компонентів;
- реалізує з'єднання між мікроконтролером, клавіатурою, дисплеєм та датчиками за допомогою UART та I2C протоколів;
- відповідає за відкриття та закриття замка на основі команд від мікроконтролера.

На етапі прототипування створюється робоча модель системи, яка включає всі вибрані компоненти. Основні завдання цього етапу:

- з'єднання всіх компонентів відповідно до розроблених схем;
- написання та завантаження прошивки, яка реалізує основні функції системи;
- тестування комунікації між компонентами через UART та I2C.

Тестування та верифікація включають перевірку правильності роботи системи та відповідності її функціональних можливостей вимогам проекту.

Основні аспекти тестування:

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35

2.4.2 Опис UART та I2C протоколів

Для забезпечення зв'язку між компонентами системи використовуються UART та I2C протоколи.

UART є асинхронним серійним інтерфейсом для обміну даними між мікроконтролером та іншими пристроями. Він працює за принципом передачі даних пакетами, кожен з яких включає стартовий біт, дані та стоп-біт. UART забезпечує надійну передачу даних на короткі відстані і широко використовується у вбудованих системах;

I2C є синхронним серійним інтерфейсом, який дозволяє підключати до однієї шини кілька пристроїв. Він використовує два дроти: SDA (лінія даних) та SCL (лінія синхронізації). I2C підтримує багатомайстерну конфігурацію, де кожен пристрій може бути майстром або слейвом.

Цей протокол забезпечує високу швидкість передачі даних та гнучкість у підключенні різних пристроїв.

На заключному етапі проектування проводиться інтеграція всіх компонентів у єдину систему та підготовка її до експлуатації. Основні завдання:

- збирання всіх компонентів у корпусі та їх кінцевий монтаж;
- повне тестування системи у робочих умовах для забезпечення її надійності та безвідмовної роботи;
- створення технічної документації, яка включає схеми, протоколи тестування та інструкції з експлуатації.

Проектування комп'ютерного засобу для системи доступу до приміщення є комплексним процесом, який вимагає уважного підходу на кожному етапі. Забезпечення правильного вибору компонентів, розробки схем, прототипування та тестування гарантує створення надійної та ефективної системи доступу.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		36

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Реалізація або моделювання проектних рішень

3.1.1 Обґрунтування вибору середовища розробки

Розробка комп'ютеризованої системи доступу до приміщення з використанням пін-коду та сканера відбитків пальців вимагає ретельного вибору середовища розробки. Вибір середовища залежить від кількох факторів, зокрема: простота використання, можливості інтеграції з апаратними компонентами, наявність необхідних бібліотек та підтримка розробника. Після ретельного аналізу різних варіантів було обрано Arduino IDE як основне середовище для розробки даної системи.

Arduino IDE є популярним середовищем розробки для мікроконтролерів, що надає простий у використанні інтерфейс та широкий спектр можливостей для програмування апаратного забезпечення. Основними перевагами Arduino IDE є його простота використання, широка підтримка апаратних компонентів, наявність бібліотек, активна підтримка спільноти та кросплатформність. Arduino IDE надає інтуїтивно зрозумілий інтерфейс, що дозволяє швидко освоїти основні принципи програмування навіть для новачків. Середовище підтримує написання коду на мові програмування C/C++, що є стандартом для розробки мікроконтролерів. Arduino IDE підтримує велику кількість мікроконтролерів та периферійних модулів, таких як сканери відбитків пальців, клавіатури, датчики та інші. Це дозволяє легко інтегрувати різні компоненти в одну систему. Інтерфейс Arduino IDE зображений на рис. 3.1

					КС КРБ 123.130.00.00 ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Рожик А.М.			Практична частина	Літ.	Арк..	Акрушів
Перевір.		Жаровський Р.О.					37	
Рецез.		Бревус В. М.				ТНТУ, каф. КС, гр. СІ-42		
Н. контр.		Тиш Є.В.						
Зав.каф		Осухівська Г.М.						

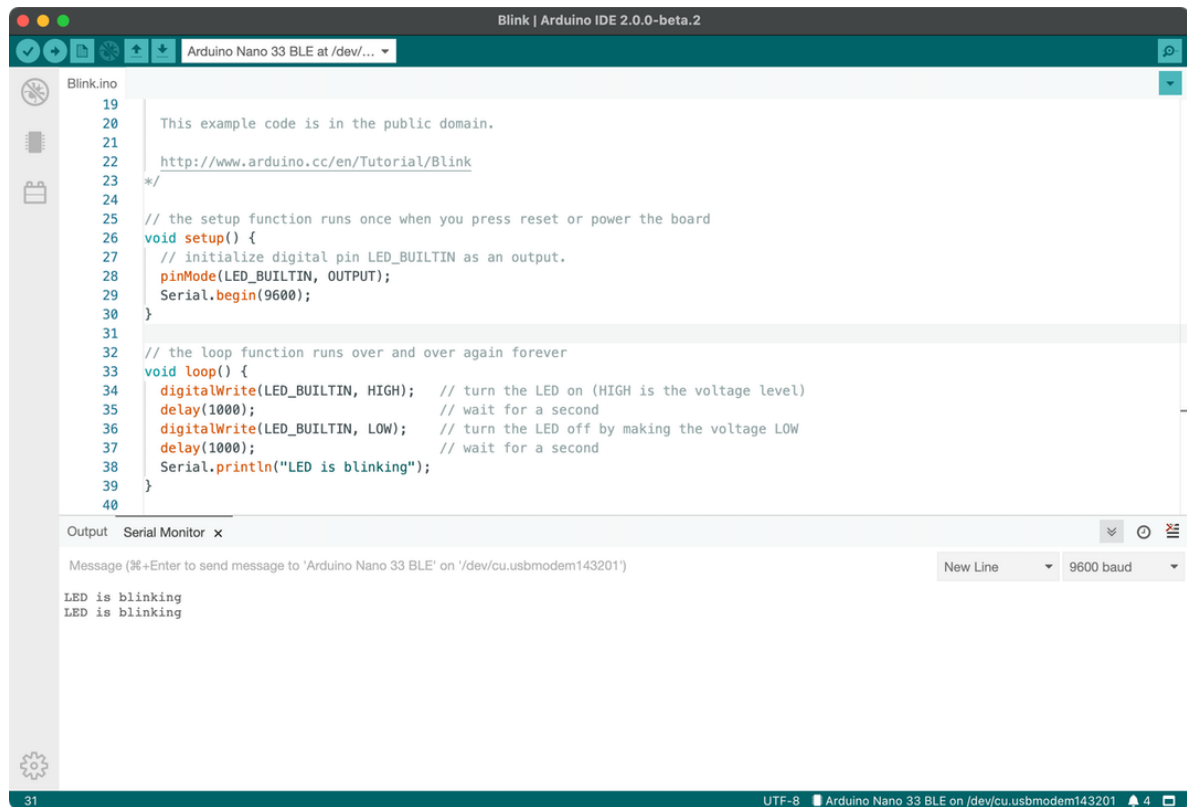


Рисунок 3.1 – Інтерфейс Arduino IDE

Після написання коду система проходить тестування для виявлення та усунення можливих помилок. Це включає тестування кожного компоненту окремо та перевірку їх сумісної роботи в системі. Після успішного тестування всіх компонентів здійснюється їх інтеграція в одну систему. На цьому етапі також проводиться оптимізація коду та налаштування системи для досягнення максимальної ефективності та стабільності.

Arduino IDE пропонує широкий спектр бібліотек, які значно полегшують розробку системи доступу до приміщення:

- бібліотека `LCD_I2C` використовується для керування символьними LCD-дисплеями, які працюють за протоколом I2C (Inter-Integrated Circuit). Вона дозволяє легко виводити текст і керувати іншими елементами дисплея, такими як курсор та позиція виводу;
- бібліотека `Servo` дозволяє керувати сервоприводами, які використовуються для точного керування певними механізмами або вирішення

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		38

певних завдань у робототехніці. Вона дозволяє легко встановлювати кут обертання сервопривода та виконувати інші операції з ним;

- бібліотека Keypad призначена для роботи з клавіатурою, звичайною або матричною. Вона дозволяє зчитувати введені користувачем значення та взаємодіяти з клавіатурою для управління вашим пристроєм;

- бібліотека Adafruit_Fingerprint розроблена Adafruit і призначена для роботи з відбитками пальців. Вона дозволяє легко взаємодіяти з сенсорними модулями відбитків пальців, включаючи зчитування, зберігання та порівняння відбитків;

- бібліотека SoftwareSerial дозволяє створювати додаткові віртуальні UART (Universal Asynchronous Receiver-Transmitter) порти на мікроконтролерах, які не мають вбудованої підтримки додаткових портів. Вона часто використовується для з'єднання з додатковими пристроями, такими як модеми, GPS-приймачі, Bluetooth-модулі.

Вибір Arduino IDE як середовища розробки для комп'ютеризованої системи доступу до приміщення обґрунтований його простотою використання, широкою підтримкою апаратних компонентів, наявністю необхідних бібліотек та підтримкою з боку спільноти розробників. Використання цього середовища дозволяє швидко та ефективно реалізувати всі необхідні функції системи, забезпечуючи високу якість та надійність кінцевого продукту.

3.1.2 Детальний опис роботи програми

Програмний код для системи доступу до приміщення складається з кількох основних частин: підключення бібліотек, оголошення змінних, налаштування початкових параметрів, основний цикл програми та допоміжні функції.

На початку коду підключаються необхідні бібліотеки. Бібліотеки забезпечують зручний доступ до функцій та методів, що полегшують роботу з апаратними компонентами, такими як LCD дисплей, серво мотор, клавіатура, сканер відбитків пальців та програмна серійна передача даних. На рис. 3.2 зображено лістинг підключення бібліотек.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		39


```

#include <LCD_I2C.h>
#include <Servo.h>
#include <Keypad.h>
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>

```

Рисунок 3.2 –Лістинг підключення бібліотек

Далі оголошуються змінні для налаштування роботи системи. Ці змінні визначають параметри, такі як час відкриття дверей, кількість помилок введення паролю та інші важливі константи, що використовуються в програмі. Лістинг оголошення змінних зображено на рис.3.3.

```

#define openTime 10
#define errPassTime 5
#define maxErrorPass 3
#define lockPassTime 20
#define servoSpeed 2

```

Рисунок 3.3 –Лістинг оголошення змінних

Оголошуються змінні для роботи з апаратними компонентами, такими як світлодіоди, серво мотор та буфер для зберігання введеного паролю. Ці змінні забезпечують зберігання поточного стану системи та взаємодію з апаратними компонентами. Лістинг оголошення змінних для апаратних компонентів зображено на рис.3.4.

```

int redled = 11;
int grled = 12;
int buzz = 13;
int servo = 10;

```

Рисунок 3.4 –Лістинг оголошення змінних для апаратних компонентів

					КС КРБ 123.130.00.00 ПЗ	Арк.
						40
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштовується матриця клавіатури та оголошується об'єкт для роботи з нею. Клавіатура використовується для введення пін-коду користувачем. Лістинг налаштування матриці клавіатури зображено на рис.3.5.

```
const byte numRows = 4;
const byte numCols = 4;
char keymap[numRows][numCols] =
{
    {'1', '2', '3', 'A'},
    {'4', '5', '6', 'B'},
    {'7', '8', '9', 'C'},
    {'*', '0', '#', 'D'}
};
byte rowPins[numRows] = {9, 8, 7, 6};
byte colPins[numCols] = {5, 4, 3, 2};
Keypad myKeypad = Keypad(makeKeypad(keymap), rowPins, colPins,
numRows, numCols);
```

Рисунок 3.5 – Лістинг налаштування матриці клавіатури

Оголошується об'єкт для роботи з LCD дисплеєм та програмною серійною передачею даних. LCD дисплей використовується для відображення інформації користувачеві, а програмна серійна передача даних забезпечує зв'язок зі сканером відбитків пальців. Лістинг налаштування LCD дисплею та серійної передачі даних зображено на рис.3.6.

```
LCD_I2C lcd(0x27);
SoftwareSerial mySerial(0, 1);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
```

Рисунок 3.6 – Лістинг налаштування LCD дисплею та серійної передачі даних

В функції setup() ініціалізуються компоненти системи: LCD дисплей, серво мотор, сканер відбитків пальців та світлодіоди. Ця функція виконується один раз

при старті програми і налаштовує початковий стан всіх компонентів. Лістинг функції setup зображено на рис.3.7.

```
void setup() {
    lcd.begin();
    lcd.backlight();
    lcd.setCursor(0, 0);
    lcd.print("System starting...");
    myservo.attach(servo);
    myservo.write(servoPosition);
    pinMode(redled, OUTPUT);
    pinMode(grled, OUTPUT);
    pinMode(buzz, OUTPUT);
    digitalWrite(redled, LOW);
    digitalWrite(grled, LOW);
    digitalWrite(buzz, LOW);
    finger.begin(57600);
    if (finger.verifyPassword()) {
        lcd.setCursor(0, 1);
        lcd.print("Scanner ready");
    } else {
        lcd.setCursor(0, 1);
        lcd.print("Scanner error");
    }
}
```

Рисунок 3.7 –Лістинг функції setup

В основному циклі програми здійснюється обробка введення пін-коду, зчитування відбитків пальців та управління доступом до приміщення. Цей цикл постійно повторюється, забезпечуючи безперервну роботу системи. Лістинг основного циклу програми зображено у додатку В.

Функції openDoor, closeDoor та lockSystem реалізують відкриття, закриття дверей та блокування системи відповідно. Вони керують рухом серво мотора та світлодіодами, щоб візуально інформувати користувача про стан системи. Лістинг функцій управління дверима та блокування системи зображено на рис 3.8.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		42

```

void openDoor() {
    while (servoPosition < 180) {
        servoPosition += servoSpeed;
        myservo.write(servoPosition);
        delay(15);
    }
}

void closeDoor() {
    while (servoPosition > 0) {
        servoPosition -= servoSpeed;
        myservo.write(servoPosition);
        delay(15);
    }
    digitalWrite(grled, LOW);
}

void lockSystem() {
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("System locked");
    delay(lockPassTime * 1000);
    errorPassCount = 0;
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Enter password:");
}

```

Рисунок 3.8 – Лістинг функцій управління дверима та блокування системи

Функція `fingerprintScan` здійснює зчитування відбитків пальців та перевірку їх на відповідність зареєстрованим шаблонам. Якщо відбиток пальця розпізнано, система надає доступ до приміщення [1]. Лістинг функції зчитування відбитків пальців зображено на рис.3.10.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		43

```

uint8_t fingerprintScan() {
    uint8_t p = finger.getImage();
    if (p != FINGERPRINT_OK) return p;

    p = finger.image2Tz();
    if (p != FINGERPRINT_OK) return p;

    p = finger.fingerFastSearch();
    if (p != FINGERPRINT_OK) return p;

    return p;
}

```

Рисунок 3.10 – Лістинг функції зчитування відбитків пальців

FSR 402 підключається до мікроконтролера за допомогою аналогового входу. Один кінець датчика підключається до джерела живлення, а інший - до землі через резистор. Від точки з'єднання між резистором і датчиком знімається напруга, яка подається на аналоговий вхід мікроконтролера. Лістинг зчитування значень з FSR 402 зображено на рис.3.11.

```

int fsrAnalogPin = A0; // FSR підключений до аналогового входу
A0
int fsrValue;

void setup() {
    Serial.begin(9600);
}
void loop() {
    fsrValue = analogRead(fsrAnalogPin); // Зчитування значення
з датчика FSR
    Serial.print("FSR Value: ");
    Serial.println(fsrValue);
    delay(500);
}

```

Рисунок 3.11 – Лістинг зчитування значень з FSR 402

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		44

Таким чином, програмний код реалізує всі необхідні функції для забезпечення доступу до приміщення з використанням пін-коду та сканера відбитків пальців. Кожна частина коду відповідає за певний аспект роботи системи, що забезпечує її надійність та функціональність. Усі частини коду взаємодіють між собою, забезпечуючи комплексний підхід до управління доступом, включаючи перевірку паролю та відбитків пальців, управління серво мотором для відкриття та закриття дверей, а також індикацію стану системи за допомогою світлодіодів та LCD дисплею.

Після підключення всіх необхідних компонентів отримуємо схему з'єднань готової до програмування системи, що зображена на рис. 3.12.

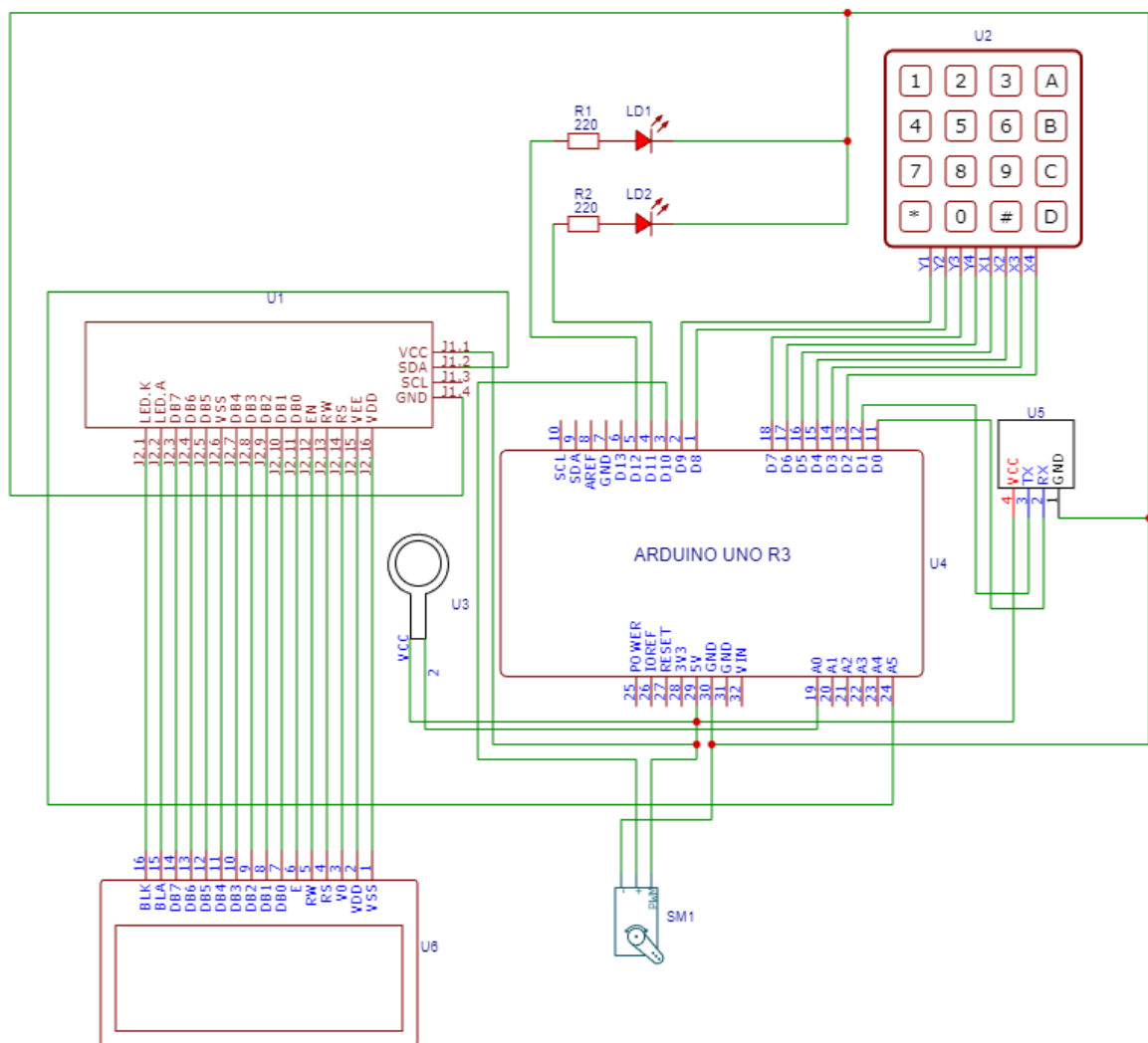


Рисунок 3.12 – Схема з'єднань системи

3.2 Тестування системи доступу до приміщення

Перед початком тестування була зібрана схема, яка включає всі необхідні компоненти системи. Всі елементи були з'єднані між собою за допомогою мідних дротів та макетної плати. Важливим елементом системи є РК дисплей (LCD 16x2 I2C), який підключений до плати Arduino через пінні A4 (SDA) та A5 (SCL) для забезпечення комунікації за протоколом I2C. Живлення дисплея здійснюється від 5V та GND на платі Arduino. Серво, що забезпечує рух дверей, було підключено до пінна 10, а живлення отримує від 5V та GND. Для введення пароля використовується клавіатура 4x4, підключена до пінів 9, 8, 7, 6 для рядків та 5, 4, 3, 2 для стовпців.

Світлодіоди грають важливу роль у візуалізації стану системи. Червоний світлодіод, що сигналізує про закриті двері, підключено до пінна 11 через резистор, а зелений світлодіод, що сигналізує про відкриті двері, підключено до пінна 12. Для звукової сигналізації використовується буюер, підключений до пінна 13, з живленням від 5V та GND на платі Arduino.

Після збирання схеми система була підключена до живлення і запущена для перевірки працездатності. При ввімкненні системи на дисплеї з'являється повідомлення "Password:", що свідчить про готовність системи до введення пароля. Повідомлення "Password:" зображено на рис.3.13.

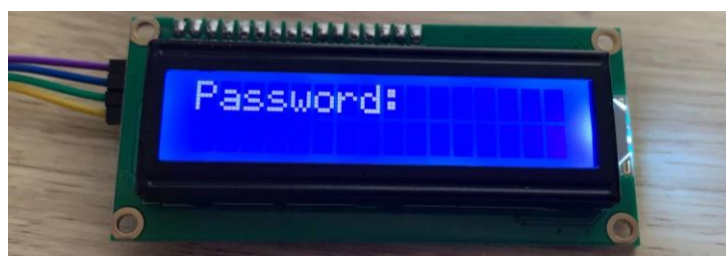


Рисунок 3.13 – Повідомлення "Password:"

Далі, користувач вводить пароль за допомогою клавіатури 4x4. Кожен введений символ відображається на дисплеї як "*", що забезпечує конфіденційність введених даних.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		46

У разі введення правильного пароля, на дисплеї з'являється повідомлення "Opening:", після чого двері починають відчинятися, зелений світлодіод засвічується, вказуючи на успішне відкриття дверей. Повідомлення "Opening:" зображено на рис.3.14.



Рисунок 3.14 – Повідомлення "Opening:"

Після закінчення заданого часу двері автоматично зачиняються, червоний світлодіод засвічується, і на дисплеї знову з'являється повідомлення "Password:", що свідчить про повернення системи у вихідний стан.

У разі введення неправильного пароля, на дисплеї з'являється повідомлення "Invalid password", і система переходить у режим очікування нового введення. Це дозволяє користувачеві спробувати ввести пароль ще раз. Повідомлення "Invalid password" зображено на рис.3.15.



Рисунок 3.15 – Повідомлення "Invalid password"

Якщо користувач тричі поспіль вводить неправильний пароль, система блокується на заданий час, і на дисплеї з'являється повідомлення "System locked". Після закінчення часу блокування система автоматично розблоковується і повертається у вихідний стан.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

Загальний вигляд створеної моделі системи зображено на рис. 3.16.



Рисунок 3.16 – Загальний вигляд створеної моделі системи

Під час тестування система продемонструвала високу надійність та ефективність, всі компоненти функціонували коректно, забезпечуючи надійну роботу системи доступу. Це дозволяє зробити висновок про успішну реалізацію проекту та можливість його подальшого використання у реальних умовах.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		48

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Психологічні чинники небезпеки

Стійко підвищують імовірність наразитись на небезпеку постійні функціональні зміни в нервовій системі або інших системах чи органах, що мають хворобливий характер або близький до цього стан. Такі зміни не означають непрацездатності, однак можуть чинити несприятливий вплив на людину з точки зору її безпеки: головні болі, серцеві захворювання, цукровий діабет. В основному перебіг хвороби позначається на поведінці людини, частково безпосередньо – у вигляді слабкості, недомагання, а частково побічно – шляхом загального впливу на психіку: подавленість, депресія, роздратованість, підвищуючи тим самим імовірність наразитись на небезпеку.

Підвищення захищеності операторів системи доступу до приміщення, що страждають такими недугами, можна досягти перш за все шляхом постійних медичних оглядів та необхідного лікування. Важливо також не допускати таких осіб до робіт з підвищеною небезпекою.

Імовірність наразитись на небезпеку стійко підвищують різноманітні вади органів чуття, такі як часткова втрата зору, слуху. Дефекти органів чуття можуть мати різну ступінь, однак навіть мінімальний дефект підвищує імовірність нещасного випадку. Важливе значення у підвищенні безпеки осіб з такими вадами відіграє набуття необхідних навичок, практика та загальне відповідальне ставлення до виконуваної роботи.

Підвищують імовірність наразитись на небезпеку порушення зв'язку між сенсорними та руховими центрами вищих відділів нервової системи.

					КС КРБ 123.130.00.00 ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Рожик А.М.			Безпека життєдіяльності, основи охорони праці	Літ.	Арк.	Акрушів
Перевір.		Жаровський Р.О.					49	
Консульт.		Пилипець М.І.				ТНТУ, каф. КС, гр. СІ-42		
Н. контр.		Тиш Є.В.						
Зав.каф		Осухівська Г.М.						

Внаслідок таких порушень людина не здатна з необхідною швидкістю та точністю реагувати на зовнішні впливи, що сприймаються її органами чуття.

Серед фахівців в галузі безпеки життєдіяльності переважає думка про те, що порушення узгодженості між сенсорними та моторними процесами відіграють значну роль у виникненні багатьох нещасних випадків. Вказані порушення можуть бути компенсовані в першу чергу завдяки правильному розподілу уваги. Значну роль також відіграє доведена до автоматизму належна ступінь відпрацювання навичок, що дозволяє людині відповідати на зовнішні подразнення не тільки з рефлексивною впевненістю, але й з потрібною точністю і саме в даний момент.

Імовірність наразитись на небезпеку можуть підсилювати дефекти, що виникають в узгодженості координації рухів. Такі порушення часто виникають в координації особливо тонких та складних рухів рук. В стані емоційної сором'язливості люди схильні підсилювати дефекти рухів. "Механіка" таких дефектів полягає у тому, що м'язи, які виконують ті чи інші рухи, керуються із різних рухових центрів кори головного мозку. У багатьох людей діяльність цих центрів протікає з недостатньою узгодженістю, в результаті чого при виконанні прийомів та операцій, що потребують складних, комбінованих рухів, деякі з них пропускаються, натомість появляються зайві, зовсім непотрібні для цієї операції. Людей з невпевненими рухами не варто залучати до робіт, де є небезпека нещасного випадку.

На імовірність наразитись на небезпеку впливає неврівноваженість емоційних процесів, таких як підвищена емоційна збудливість, раптові зміни радості та злоби, гострі емоційні реакції на незначні зовнішні подразнення підвищують загрозу нещасного випадку. Зовнішній вплив неврівноваженості емоційних процесів іноді позначається побічно у формі легковажності, необдуманості вчинків, поспішності їх виконання. Щоб позбутися неврівноваженості емоційних процесів необхідно займатись самовихованням та виробляти самовладання.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		50

Серед інших чинників, які стійко підвищують імовірність наразитись на небезпеку, необхідно назвати пагубну пристрасть до алкоголю, наркотиків, які негативно впливають на всі сфери психічного життя людини.

Підвищує імовірність наразитись на небезпеку і незадоволеність роботою, відсутність інтересу до неї. Людина, яка не цікавиться роботою і не отримує від неї задоволення, не здатна психологічно правильно налаштуватись і зосередити свою увагу на точному виконанні прийомів та рухів, її поведінка характеризується як невпевнена, а увага – розсіяна. Саме ті відхилення у поведінці працівника, що викликані незадоволеністю роботою, є досить часто причиною нещасних випадків. Тому з точки зору безпеки життєдіяльності дуже важливо, щоб людина зупинила свій вибір на такому виді занять, який найбільш повно відповідає її інтересам та нахилам.

Поряд з чинниками, що стійко підвищують індивідуальну імовірність наразитись на небезпеку, існують також чинники, які або проявляються лише в певні періоди трудового процесу, або впливають на поведінку людини протягом короткого часу (кількох годин чи навіть хвилин)[8].

Недосвідченість. Практичний досвід є безумовно важливим чинником, що підвищує безпеку праці. Він, до того ж, впливає на загальну поведінку працівника на робочому місці, що проявляється у високому темпі, ритмі, інтенсивності роботи. Досвідченість суттєво впливає на вміння працівника правильно розподілити увагу. Знаючи процес у всіх деталях, він краще пристосовує свою увагу до вимог роботи, зменшуючи її концентрацію, де це можливо, і тим самим дає своєрідний відпочинок нервовій системі. Досвідчений працівник менше втомлюється і, відповідно, підвищує свою безпеку.

Підвищена схильність наражатись на небезпеку в першу чергу обумовлена тим, що недосвідчена людина ще не навчилась пристосуватись до вимог, які висуває даний вид діяльності. Негативний вплив цього чинника проявляється двояко. По-перше, в результаті недостатньо вироблених навичок значно зростає імовірність різноманітних помилок, що можуть призвести до нещасного випадку. По-друге, усвідомлення того, що ці помилки можуть мати місце,

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		51

здійснює зворотний вплив. Початківець, який ще не зовсім впевнений і знає про це, виконує свою роботу з надмірною обережністю, здійснюючи робочі рухи, які інший робить автоматично, з максимальною концентрацією уваги. Таке постійне напруження нервово-психічної системи може спричинити швидке стомлення, в результаті якого він не зможе уважно слідкувати навіть тоді, коли це дійсно необхідно.

Підвищена ймовірність наразитись на небезпеку викликана не лише почуттям невпевненості, а й неправильними спробами справитись з цим почуттям. Інколи люди, прагнучи бездумною відвагою пригасити в собі почуття невпевненості, лише підсилюють імовірність нещасного випадку.

Ступінь досвідченості визначається не лише стажем роботи. За однаковий час працівники можуть набути різний досвід. Фактичний рівень досвідченості залежить від навичок та вправності, набутих працівником під час навчання та практики, від особливостей особистості і від характеру впливу виробничого колективу на працівника та його поведінку.

4.2 Долікарська допомога при ураженні електричним струмом

При ураженні електричним струмом користувачів системи доступу до приміщення необхідно якомога швидше звільнити їх від струмопровідних частин обладнання. Дотик до струмопровідних частин системи доступу у більшості випадків призводить до судом м'язів, тобто користувач самостійно не в змозі відірватися від провідника. Тому необхідно швидко відключити ту частину електрообладнання системи доступу, до якої доторкається користувач.

Будь-яке зволікання при наданні допомоги, а також невміння того, хто допомагає, надати кваліфіковану допомогу, призводить до загибелі людини, яка знаходиться під дією струму.

При звільненні потерпілих від струмопровідних частин або проводу в електроустановках напругою до 1000 В відключають струм, використовуючи сухий одяг, палицю, дошку, шапку, сухі рукавиці, рукав одягу, діелектричні

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		52

рукавиці. Провідники перерізають інструментом з ізольованими ручками, перерубують сокирою з дерев'яним сухим топорищем. Потерпілого можна також відтягнути від струмопровідних частин за одяг, уникаючи дотику до навколишніх металевих предметів та до відкритих частин тіла потерпілого. Відтягуючи потерпілого за ноги, не можна торкатися його взуття, оскільки воно може бути сирым і стає провідником електричного струму. Той, хто надає допомогу, повинен одягнути діелектричні рукавиці або обмотати їх шарфом, натягнути на них рукав піджака або пальта. Можна також ізолювати себе, ставши на гумовий килимок, суху дошку.

При звільненні потерпілих в електроустановках з напругою понад 1000В слід користуватися діелектричними рукавицями і взути діелектричні боти; діяти ізолюючою штангою або ізолюючими кліщами. Якщо є можливість, то вимкнути електроустановку. Можна замкнути або заземлити провідники (замкнути дроти накоротко, накинувши на них попередньо заземлений провід).

Якщо провід торкається землі, то необхідно пам'ятати про небезпеку крокової напруги. Тому після звільнення потерпілого від струмопровідних частин слід винести його з небезпечної зони. Без засобів захисту пересуватися в зоні розтікання струму по землі слід не відриваючи ноги одна від одною.

Виділяють три стани людського організму внаслідок дії електроструму:

а) I стан – потерпілий при свідомості. Слід забезпечити повний спокій, 2-3 годинне спостереження, виклик лікаря;

б) II стан – потерпілий непритомний, але дихає. Людину покласти горизонтально, розстебнути комір і пасок, дати нюхати нашатирний спирт, викликати лікаря;

в) III стан – потерпілий не дихає або дихає з перервами, уривчасто, як вмираючий. Роблять штучне дихання і непрямий масаж серця.

Кожен працівник, обслуговуючий оперативний персонал повинні знати правила долікарської допомоги, способи штучного дихання і масажу серця.

Долікарську допомогу потерпілому надають на місці нещасного випадку. Констатувати смерть має право тільки лікар.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		53

Способи штучного дихання бувають ручні та апаратні. Ручні менш ефективні, але можуть застосовуватись негайно при порушенні дихання у потерпілого. При виконанні штучного дихання “з рота в рот”, та “з рота в ніс” в рот або в ніс потерпілого рятівник видихає зі своїх легенів в легені потерпілого об’єм повітря в кількості 1000-1500 мл. Цей метод найбільш ефективний, однак можлива передача інфекції, тому використовують носовичок, марлю, спеціальну трубку.

Підготовка до штучного дихання:

- звільнити потерпілого від одягу – розв’язати галстук, розстебнути комір сорочки;
- покласти потерпілого на спину на горизонтальну поверхню – стіл або підлогу;
- відвести голову потерпілого максимально назад, доки його підборіддя не стане на одній лінії з шиєю. При цьому положенні язик не затуляє вхід до гортані, вільно пропускає повітря до легенів. Разом з тим при такому положенні голови рот розкривається. Для збереження такого положення голови під лопатки кладуть валик із згорнутого одягу;
- пальцями обслідувати порожнину рота і якщо там є кров, слиз тощо, їх необхідно видалити, вийнявши також зубні протези; за допомогою носовичка або краю сорочки вичистити порожнину рота. Обов’язково провести штучне дихання.

Голову потерпілого відводять максимально назад і пальцями затискають ніс (або губи). Роблять глибокий вдих, притискають свої губи до губ потерпілого і швидко роблять глибокий видих йому до рота. Вдування повторюють кілька разів, з частотою 12-15 разів на хвилину. З гігієнічною метою рекомендується рот потерпілого прикрити шматками тканини (носовичок, бинт)[8].

Якщо пошкоджене обличчя проводити штучне дихання “із легенів у легені” неможливо, треба застосувати метод стиснення і розширення грудної клітки шляхом складання і притискання рук потерпілого до грудної клітки з їх наступним розведенням у боки. Контроль за надходженням повітря з легенів

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		54

потерпілого здійснюється за розширенням грудної клітки при кожному вдиханні. Якщо після вдихання грудна клітка потерпілого не розправляється, – це ознака непрохідності шляхів дихання. Найкраща прохідність шляхів дихання забезпечується за наявності трьох умов:

- максимального відведення голови назад;
- відкривання рота;
- висування вперед нижньої щелепи.

При появі у потерпілого перших слабких вдихів слід поєднати штучний вдих з початком самостійного вдиху. Штучне дихання слід проводити до відновлення глибокого ритмічного дихання.

Штучне дихання у більшості випадків треба робити одночасно з масажем серця.

Зовнішній масаж серця – це ритмічне стиснення серця між грудниною та хребтом. Треба знайти розпізнавальну точку – мечоподібний відросток груднини, – він знаходиться знизу грудної клітини над животом. Стати треба з лівого боку від потерпілого і покласти долоню однієї руки на нижню третину груднини, а поверх – долоню другої руки. Тепер ритмічними рухами треба натискати на груднину (з частотою 60 разів на хвилину). Сила стиснення має бути такою, щоб груднина зміщувалась в глибину на 4-5 см. Масаж серця доцільно проводити паралельно зі штучним диханням, для чого після 2-3 штучних вдихів роблять 15 стискань грудної клітки. При правильному масажі серця під час натискання на груднину відчуватиметься легкий поштовх сонної артерії і звузяться протягом кількох секунд зіниці, а також порожевіє шкіра обличчя і губи, з'являться самостійні вдихи. Щоб не пропустити повторного припинення дихання, треба стежити за зіницями, кольором шкіри і диханням, регулярно перевіряти частоту і ритмічність пульсу.

Наслідки своєчасної і правильно наданої допомоги на місці події можуть бути зведені нанівець, якщо при підготовці до транспортування і доставці потерпілого до медичної установи не будуть дотримані відповідні правила. Головне не тільки в тому, як доставити потерпілого і яким видом транспорту, а

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		55

наскільки швидко були вжиті заходи, які забезпечили максимальний спокій і зручне положення потерпілого.

Найкраще транспортувати потерпілого ношами. При цьому можна використовувати підручні засоби: дошки, одяг тощо. Можна переносити потерпілого на руках. Передусім потерпілого слід покласти на ноші, які застеляють ковдрою, одягом тощо, ставлять ноші з того боку потерпілого, де є ушкодження. Якщо тих, хто надає допомогу, двоє, вони повинні стати з двох боків нош. Один підкладає руки під голову і груднину, другий – під крижі і коліна потерпілого. Одночасно без поштовхів його обережно піднімають, підтримуючи ушкоджену частину тіла, і опускають на ноші. Слід накрити потерпілого тим, що є під руками, – одягом, ковдрою. Якщо є підозра на перелом хребта, потерпілого кладуть обличчям догори на тверді ноші (щит, двері). За відсутністю такого можна використати ковдру, пальто. В такому випадку потерпілого кладуть на живіт.

У разі, якщо виникає підозра на можливий перелом кісток тазу, проведення невідкладних заходів є критично важливим. Потерпілого необхідно негайно розмістити на спині з ногами, зігнутими в колінах і тазостегнових суглобах, для того, щоб забезпечити оптимальне розведення стегон. Під коліна обов'язково слід підкласти валик, виготовлений із м'якого матеріалу, такого як вата, рушник або навіть частина одягу.

Під час перенесення потерпілого по рівній поверхні, важливо носити його ногами вперед, уникати різких рухів та забезпечити горизонтальне положення нош. При підйомі на висоту або під час пересування по сходах, носії повинні вести потерпілого головою вперед, уникаючи будь-яких струсів або вібрацій. Щоб ноші не розгойдувались, необхідно йти не в ногу, злегка зігнувши коліна.

Під час транспортування потерпілого до лікувального закладу слід покласти його до машини на тих самих ношах, підстеливши під них що-небудь м'яке.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		56

ВИСНОВКИ

Розробка та впровадження системи контролю доступу на базі мікроконтролера Arduino з використанням клавіатури для введення пароля, сканера відбитків пальців, LCD-дисплея, сервоприводу та індикаторів виявилася успішною та дозволила досягти поставлених цілей. Основна мета проекту полягала у створенні надійної, простої у використанні та безпечної системи, яка може знайти застосування у побутових або офісних умовах для контролю доступу до приміщень.

Проект продемонстрував можливість ефективного використання доступних апаратних та програмних ресурсів для створення системи контролю доступу. Розроблена система може бути легко адаптована для різних умов експлуатації та масштабована для включення додаткових функцій та компонентів. Зокрема, можливе розширення функціоналу за рахунок інтеграції з мережею для віддаленого керування та моніторингу, додавання датчиків для виявлення руху або відкриття дверей, а також інших заходів для підвищення рівня безпеки.

У підсумку, розробка та тестування системи контролю доступу продемонстрували її життєздатність та відповідність початковим вимогам. Система виявилася простою у встановленні та налаштуванні, зручною у використанні та ефективною у забезпеченні контролю доступу до приміщень. Подальші дослідження та вдосконалення можуть бути спрямовані на покращення безпеки, надійності та функціональних можливостей системи для задоволення зростаючих потреб користувачів.

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		57

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Adafruit_Fingerprint_Sensor: бібліотека. URL: https://adafruit.github.io/Adafruit_Fingerprint_Sensor_Library/html/index.html (дата звернення: 15.05.2024).
2. Arduino Programming Notebook. URL: https://playground.arduino.cc/uploads/Main/arduino_notebook_v1-1.pdf (дата звернення: 23.05.2024).
3. Yatsyshyn V., Pastukh O., Palamar A., Zharovskyi R. Technology of relational database management systems performance evaluation during computer systems design. Scientific Journal of TNTU (Tern.). Vol. 109. No 1. 2023. pp. 54–65.
4. Yatsyshyn V., Pastukh O., Zharovskyi R., Shabliy N. Software tool for productivity metrics measure of relational database management system. Mathematical Modeling. No 1 (48). 2023. P. 7-17.
5. Біометрична безпека з використанням датчика відбитків пальців. URL: <https://create.arduino.cc/projecthub/SurtrTech/biometric-security-using-fingerprint-sensor-0bfaee> (дата звернення: 29.05.2024).
6. Використання РК-дисплеїв з Arduino. URL: <https://learn.adafruit.com/character-lcds> (дата звернення: 28.05.2024).
7. Вступ до серводвигунів. URL: <https://www.arduino.cc/en/Tutorial/LibraryExamples/Sweep> (дата звернення: 27.05.2024).
8. Гурик О.Я., Король О.І., Сенчишин В.С. Методичні вказівки до лабораторної роботи №2 з дисципліни "Основи охорони праці" "Дослідження метеорологічних умов у виробничих приміщеннях". Тернопіль, 2016. 35 с.
9. Документація по бібліотеці Keypad для Arduino. URL: <https://www.arduino.cc/en/Reference/Keypad> (дата звернення: 22.05.2024).
10. Документація по бібліотеці Servo для Arduino. URL: <https://www.arduino.cc/en/Reference/Servo> (дата звернення: 16.05.2024).

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		58

11. Енциклопедія інформаційних технологій: у 3 т. Київ: Академперіодика, 2015. Т. 3. 456 с.

12. Інтерфейс датчика відбитків пальців з Arduino. URL: <https://lastminuteengineers.com/fingerprint-sensor-arduino-tutorial/> (дата звернення: 03.06.2024).

13. Костик П.В., Тиш Є.В. Фактори впливу на ефективність проектування програмних інтерфейсів комп'ютерних систем. Інформаційні моделі, системи та технології: Матеріали VI наук.-техн. конф. ТНТУ ім. І.Пулюя (12-13 грудня 2018). Тернопіль, 2018. с. 85.

14. Лецишин Ю. З. Розробка системи зв'язку як інтегрованого елементу роботизованих систем. Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення з урахуванням досвіду антитерористичної операції. Збірник тез доповідей XXI Всеукраїнської науковопрактичної конференції. Житомир, 2016. С. 102. Недашківський О.М. Планування та проектування інформаційних систем. Київ, 2014. 215 с.

15. Лецишин Ю. З. Створення вбудованих систем на базі структурнопараметричних моделей цифрових каналів зв'язку: Лецишин Ю.З., Назаревич Т.О., Міська І.В. VIII Науково-технічна конференція «Інформаційні моделі, системи та технології». Тернопіль, 2020. С. 127.

16. Основи програмування на Arduino. URL: <https://www.arduino.cc/en/Tutorial/Foundations> (дата звернення: 30.05.2024).

17. Осухівська Г.М., Тиш Є.В., Луцик Н.С., Паламар А.М. Методичні вказівки до виконання кваліфікаційних робіт здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 123 «Комп'ютерна інженерія» усіх форм навчання. Тернопіль: ТНТУ, 2022. 28 с.

18. Програмування Arduino - Початок роботи з ескізами. URL: <https://www.arduino.cc/en/Guide> (дата звернення: 25.05.2024).

					КС КРБ 123.130.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		59

Додаток А
Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя
Факультет комп'ютерно-інформаційних систем і програмної інженерії

Кафедра комп'ютерних систем та мереж

“Затверджую”

Завідувач кафедри КС _____ Осухівська Г.М.

“09” __02__ 2024 р.

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ДОСТУПУ ДО ПРИМІЩЕННЯ

ТЕХНІЧНЕ ЗАВДАННЯ на 3 листках

На здобуття освітньо-кваліфікаційного рівня бакалавр

Напрямок 123 Комп'ютерна інженерія

Спеціальність 123 Комп'ютерна інженерія

«УЗГОДЖЕНО»

Керівник кваліфікаційної роботи

_____ к.т.н., доцент

Жаровський Р.О.

“08” __02__ 2024 р.

«ВИКОНАВЕЦЬ»

Студентка групи СІ-42

_____ Рожик А.М.

“06” __02__ 2024 р.

Тернопіль 2024

1. Назва та підстава для виконання роботи.

1.1. Комп'ютеризована система доступу до приміщення.

1.2. Підставою для виконання кваліфікаційної роботи бакалавра (КРБ) є Наказ по Університету (№ 4/7-468 від 26.04.2024 р.).

2. Виконавець.

2.1. Студентка групи СІ-42 кафедри КС Тернопільського національного технічного університету ім. І. Пулюя, Рожик Анастасія Миколаївна.

3. Мета роботи.

3.1. Метою роботи є розробити структуру та апаратне забезпечення комп'ютеризованої системи доступу до приміщення

4. Склад виробу.

4.1. До складу виробу повинні входити:

- мікроконтролер;
- клавіатура 4x4;
- LCD екран 16x2;
- сервопривід SG90;
- датчик відбитків пальців FPM10A;
- датчик тиску FSR402.

5. Технічні вимоги.

5.1. Вимоги по призначенню.

5.1.1. Вбудована система повинна мати наступні параметри:

- виведення інформації про стан дверей на LCD екран;
- відкриття дверей за допомогою сервоприводу SG90;
- введення пін-коду за допомогою клавіатури;
- зчитування відбитків пальців за допомогою датчика FPM10A;
- моніторинг стану дверей за допомогою датчика FSR402.

5.1.2. Система повинна живитись напругою постійного струму 5 В через USB порт та/або 12 В.

5.2. Вимоги до умов експлуатації.

5.2.1. По умовам експлуатації виріб повинен відповідати наступним вимогам:

- робочий температурний діапазон: від -20°C до +85°C;
- витримка впливу електромагнітних перешкод.

5.3. Конструктивні вимоги.

5.3.1. Конструювання корпусу приладу в КРБ не передбачено:

- розміри плати: не більше 2000 мм x 1000 мм;
- надійне кріплення всіх компонентів;

5.3.2. Для побудови системи має бути використана сучасна компоненти.

5.3.3. При побудові системи необхідно передбачити наявність роз'ємів живлення і обміну даними.

5.4. Вимоги до надійності.

5.4.1. Система повинна відповідати вимогам ДСТУ 2862-94.

5.4.2. Наробка на відмову, не менше 30000 год.

5.5. Вимоги метрології.

5.5.1. Вимірювання параметрів системи при моделюванні повинно виконуватись на універсальних вимірювальних приладах.

6. Економічні показники.

6.1. Собівартість системи повинна бути не більше 2000 грн.

7. Вимоги до документації.

7.1. Конструкторська документація повинна відповідати вимогам ЄСКД та ДСТУ.

7.2. До складу документації повинно входити:

- ПЗ;
- функціональна схема;
- UML-діаграма ;
- структурна схема;
- блок схема алгоритму роботи КС.

*Примітка: У комплект документації можуть вноситися зміни та доповнення в процесі розробки.

8. Стадії та етапи розробки КРБ

8.1 Стадії та етапи виконання КРБ наведенні в таблиці 1.

Таблиця 1

№ з/п	Назва етапів роботи	Термін виконання етапів роботи
1	<i>Розробка і затвердження технічного завдання</i>	<i>01.02 – 09.02</i>
2	<i>Аналіз технічного завдання</i>	<i>05.02 – 11.02</i>
3	<i>Аналіз вимог та принципів організації комп'ютеризованої системи доступу до приміщення</i>	<i>26.04 – 03.05</i>
4	<i>Вибір елементної бази</i>	<i>04.05 – 13.05</i>
5	<i>Розробка структурної та функціональної схеми</i>	<i>14.05 – 25.05</i>
6	<i>Реалізація проектних рішень</i>	<i>26.05 – 09.06</i>
7	<i>Безпека життєдіяльності, основи охорони праці</i>	<i>10.06 – 15.06</i>
8	<i>Оформлення кваліфікаційної роботи</i>	<i>16.06 – 20.06</i>
9	<i>Попередній захист кваліфікаційної роботи</i>	<i>14.06</i>
10	<i>Захист кваліфікаційної роботи</i>	<i>24.06 – 28.06</i>

У дане ТЗ можуть вноситись зміни по узгодженню сторін.

Додаток Б

Перелік елементів електрично-принципової схеми

Позн.	Найменування	К-сть	Примітка
	<i>Мікросхеми</i>		
U4	Arduino Uno R3	1	
	<i>Периферія</i>		
U1	I2C converter	1	
U6	LCD 16x2	1	
U3	FSR402	1	
U5	FPM10A	1	
SM1	Servomotor SG90	1	
U2	Keyboard		
	<i>Резистори</i>		
R1,R2	MOR300SJTБ-220KR-Hitano	2	
	<i>Діоди</i>		
LD1	LGA33G400	1	
LD2	HL-803S11FD-16	1	

					<i>КС КРБ 123.130.00.00 ПЕ</i>						
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	<i>Комп'ютеризована система доступу до приміщення Перелік елементів</i>			<i>Літ.</i>	<i>Арк.</i>	<i>Аркушів</i>	
<i>Розроб.</i>		<i>Рожик А.М.</i>							66	21	
<i>Перевір.</i>		<i>Жаровський</i>						<i>ФІС, СІ-42</i>			
<i>Реценз.</i>		<i>Бревус В.М.</i>									
<i>Н. Контр.</i>		<i>Тиш Є.В.</i>									
<i>Затверд.</i>		<i>Осухівська Г.М.</i>									

Додаток В

Лістинг коду програми

```
#include <LCD_I2C.h>
#include <Servo.h>
#include <Keypad.h>
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>

#define openTime 10
#define errPasTime 5
#define maxErrorPass 3
#define lockPasTime 20
#define servoSpead 2

int fsrAnalogPin = A0; // FSR pin Analog 0

uint8_t id = 1;

int redled=11;
int grled=12;
int buzz=13;
int servo=10;

int openTimeCount=openTime;
int servoPosition=0;

int errorPassCount=0;
int script=0;
unsigned long time;
unsigned long currentMillis;
unsigned long previousMillis = 0;
const long interval = 1000;

Servo myservo;
```

```
String keys="";

const byte numRows= 4;
const byte numCols= 4;
char keymap[numRows][numCols]=
{
    {'1', '2', '3', 'A'},
    {'4', '5', '6', 'B'},
    {'7', '8', '9', 'C'},
    {'*', '0', '#', 'D'}
};

byte rowPins[numRows] = {9,8,7,6};
byte colPins[numCols]= {5,4,3,2};
Keypad myKeypad= Keypad(makeKeymap(keymap), rowPins, colPins,
numRows, numCols);

LCD_I2C lcd(0x27);

SoftwareSerial mySerial(0, 1);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

volatile bool fingerScanRequested = false;

void setup() {
    Serial.begin(9600);

    lcd.begin();

    lcd.backlight();

    lcd.setCursor(0, 0);
    lcd.print("Password:");

    myservo.attach(servo);

    pinMode(buzz, OUTPUT);
```

```

pinMode(redled, OUTPUT);
pinMode(grled, OUTPUT);

finger.begin(57600);
if (finger.verifyPassword()) {
  Serial.println("Sensor detected!");
} else {
  Serial.println("Sensor not detected");
  while (1); // ps
}

finger.getTemplateCount();
Serial.print("Sensor          contains          ");
Serial.print(finger.templateCount); Serial.println(" templates");

Serial.println("Please place your finger on the sensor to
enroll.");

while (getFingerprintEnroll() != FINGERPRINT_OK) {} // ps

pinMode(0, INPUT_PULLUP);
attachInterrupt(digitalPinToInterrupt(0), requestFingerprintScan,
FALLING);

delay(1000);
myservo.write(servoPosition);
digitalWrite(redled, HIGH);
}

void loop() {
  fsrValue = analogRead(fsrAnalogPin);
  if (fsrValue * (5.0 / 1023.0) < 4){
    digitalWrite(grled, HIGH);
  }
  switch(script){

```

```

case 0:{
    char keypressed = myKeypad.getKey();
    if (keypressed != NO_KEY || fingerScanRequested){
    if (fingerScanRequested) {
        fingerScanRequested = false;
        getFingerprintID();
    }
    lcd.setCursor(keys.length(), 1);
    lcd.print("*");
    keys+=keypressed;
    time = millis();
    if (keys.length() == 4 ){
        Serial.print("key-");
        Serial.println(keys);
        if (keys == "0007"){
            lcd.clear();
            lcd.setCursor(3, 0);
            lcd.print("Opening:");
            unlockbuzz();
            errorPassCount = 0;
            script = 1;
        }
        else if (errorPassCount >= maxErrorPass){
            lcd.clear();
            lcd.setCursor(0, 0);
            lcd.print("System locked");
            script = 5;
        }
        else {
            lcd.clear();
            lcd.setCursor(0, 0);
            lcd.print("Invalid password");
            script = 4;
        }
    }
    keys="";
    lcd.setCursor(keys.length(), 1);

```

```

        lcd.print("    ");
    }
}
break;
}
case 1:{ // open dor
    oppenDor();
    break;
}
case 2: { // pause to close
    if (millis() > (time+(openTime*1000))){
        script = 3;
        lcd.clear();
        lcd.setCursor(3, 0);
        lcd.print("Closing:");
    }
    currentMillis = millis();
    if (currentMillis - previousMillis >= interval) {
        lcd.setCursor(8, 1);
        lcd.print(String(openTimeCount)+" ");
        openTimeCount--;
        previousMillis = currentMillis;
    }
    break;
}
case 3:{ // close dor
    closeDor();
    break;
}
case 4:{ // error password
    if (millis() > (time+(errPassTime*1000))){
        errorPassCount++;
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Password:");
        script = 0;
    }
}

```



```

    }
    break;
}
case 5:{ // error password
    if (millis() > (time+(lockPassTime*1000))){
        errorPassCount = 0;
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Password:");
        script = 0;
    }
    break;
}
}
}

```

```

void oppenDor() {
    if (millis() > (time + 10 * servoSpead)){
        if (servoPosition % 11 == 0) {
            lcd.setCursor(servoPosition/11, 1);
            lcd.print("_");
        }
        if (servoPosition % 10 == 0) {
            if (servoPosition % 20 == 0){
                digitalWrite(redled, LOW);
                digitalWrite(grled, HIGH);
            }
            else {
                digitalWrite(redled, HIGH);
                digitalWrite(grled, LOW);
            }
        }
        servoPosition++;
        myservo.write(servoPosition);
        time = millis();
    }
}

```

```

if (servoPosition == 180){ // двері повністю відчинено
  Serial.println("Door open");
  lcd.clear();
  lcd.setCursor(4, 0);
  lcd.print("Door open");
  digitalWrite(redled, LOW);
  digitalWrite(grled, HIGH);
  time = millis();
  script = 2;
}
}

void closeDor() { // закриття дверей
  if (millis() > (time + 10 * servoSpead)){
    if (servoPosition % 11 == 0) {
      lcd.setCursor((((servoPosition/11)-16)*-1), 1);
      lcd.print("_");
    }
    if (servoPosition % 10 == 0) {
      if (servoPosition % 20 == 0){
        digitalWrite(redled, LOW);
        digitalWrite(grled, HIGH);
      }
      else {
        digitalWrite(redled, HIGH);
        digitalWrite(grled, LOW);
      }
    }
    servoPosition--;
    myservo.write(servoPosition);
    time = millis();
  }
  if (servoPosition == 0){ // двері повністю зачинено
    Serial.println("Door close");
    digitalWrite(redled, HIGH);
    digitalWrite(grled, LOW);
  }
}

```

```

    time = millis();
    openTimeCount=openTime;
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Password:");
    script = 0;
}
}

void unlockbuzz() { // сигнал, при
відкритті дверей
    delay(100);
    tone(buzz,700,100);
    delay(100);
    tone(buzz,550,50);
    delay(100);
    tone(buzz,700,100);
    delay(100);
    tone(buzz,550,50);
    delay(100);
}

void countbuzz() { // сигнал, при відкритті
дверей
    tone(buzz,700,100);
    delay(100);
    tone(buzz,900,50);
    delay(100);
}

void requestFingerprintScan() {
    fingerScanRequested = true;
}

int getFingerprintID() {
    uint8_t p = finger.getImage();

```

```

switch (p) {
    case FINGERPRINT_OK:
        Serial.println("Image taken");
        break;
    case FINGERPRINT_NOFINGER:
        Serial.println("No finger detected");
        return p;
    case FINGERPRINT_PACKETRECEIVEERR:
        Serial.println("Communication error");
        return p;
    case FINGERPRINT_IMAGEFAIL:
        Serial.println("Imaging error");
        return p;
    default:
        Serial.println("Unknown error");
        return p;
}

// OK success!
p = finger.image2Tz();
switch (p) {
    case FINGERPRINT_OK:
        Serial.println("Image converted");
        break;
    case FINGERPRINT_IMAGEMESS:
        Serial.println("Image too messy");
        return p;
    case FINGERPRINT_PACKETRECEIVEERR:
        Serial.println("Communication error");
        return p;
    case FINGERPRINT_FEATUREFAIL:
        Serial.println("Could not find fingerprint features");
        return p;
    case FINGERPRINT_INVALIDIMAGE:
        Serial.println("Could not find fingerprint features");
        return p;
}

```

```

    default:
        Serial.println("Unknown error");
        return p;
}

// OK converted!
p = finger.fingerFastSearch();
if (p == FINGERPRINT_OK) {
    Serial.println("Found a print match!");
    Serial.print("Found ID #"); Serial.print(finger.fingerID);
    Serial.print("        with        confidence        of        ");
Serial.println(finger.confidence);
} else if (p == FINGERPRINT_PACKETRECEIVEERR) {
    Serial.println("Communication error");
} else if (p == FINGERPRINT_NOTFOUND) {
    Serial.println("Did not find a match");
} else {
    Serial.println("Unknown error");
}

return p;
}

uint8_t getFingerprintEnroll() {
    int p = -1;
    Serial.print("Waiting for valid finger to enroll as #");
    Serial.println(id);
    while (p != FINGERPRINT_OK) {
        p = finger.getImage();
        switch (p) {
            case FINGERPRINT_OK:
                Serial.println("Image taken");
                break;
            case FINGERPRINT_NOFINGER:
                Serial.print(".");
                break;

```

```

    case FINGERPRINT_PACKETRECIIEVEERR:
        Serial.println("Communication error");
        break;
    case FINGERPRINT_IMAGEFAIL:
        Serial.println("Imaging error");
        break;
    default:
        Serial.println("Unknown error");
        break;
}
delay(100);
}

// OK success!
p = finger.image2Tz(1);
switch (p) {
    case FINGERPRINT_OK:
        Serial.println("Image converted");
        break;
    case FINGERPRINT_IMAGEMESS:
        Serial.println("Image too messy");
        return p;
    case FINGERPRINT_PACKETRECIIEVEERR:
        Serial.println("Communication error");
        return p;
    case FINGERPRINT_FEATUREFAIL:
        Serial.println("Could not find fingerprint features");
        return p;
    case FINGERPRINT_INVALIDIMAGE:
        Serial.println("Could not find fingerprint features");
        return p;
    default:
        Serial.println("Unknown error");
        return p;
}

```

```

Serial.println("Remove finger");
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
    p = finger.getImage();
    delay(100);
}
Serial.print("ID "); Serial.println(id);
p = -1;
Serial.println("Place the same finger again");
while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
        case FINGERPRINT_OK:
            Serial.println("Image taken");
            break;
        case FINGERPRINT_NOFINGER:
            Serial.print(".");
            break;
        case FINGERPRINT_PACKETRECEIVEERR:
            Serial.println("Communication error");
            break;
        case FINGERPRINT_IMAGEFAIL:
            Serial.println("Imaging error");
            break;
        default:
            Serial.println("Unknown error");
            break;
    }
    delay(100);
}

// OK success!
p = finger.image2Tz(2);
switch (p) {
    case FINGERPRINT_OK:

```

```

        Serial.println("Image converted");
        break;
    case FINGERPRINT_IMAGEMESS:
        Serial.println("Image too messy");
        return p;
    case FINGERPRINT_PACKETRECIIEVEERR:
        Serial.println("Communication error");
        return p;
    case FINGERPRINT_FEATUREFAIL:
        Serial.println("Could not find fingerprint features");
        return p;
    case FINGERPRINT_INVALIDIMAGE:
        Serial.println("Could not find fingerprint features");
        return p;
    default:
        Serial.println("Unknown error");
        return p;
}

// OK converted!
Serial.print("Creating model for #"); Serial.println(id);
p = finger.createModel();
if (p == FINGERPRINT_OK) {
    Serial.println("Prints matched!");
} else if (p == FINGERPRINT_PACKETRECIIEVEERR) {
    Serial.println("Communication error");
    return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
    Serial.println("Fingerprints did not match");
    return p;
} else {
    Serial.println("Unknown error");
    return p;
}

Serial.print("ID "); Serial.println(id);

```



```
p = finger.storeModel(id);
if (p == FINGERPRINT_OK) {
    Serial.println("Stored!");
} else if (p == FINGERPRINT_PACKETRECEIVEERR) {
    Serial.println("Communication error");
    return p;
} else if (p == FINGERPRINT_BADLOCATION) {
    Serial.println("Could not store in that location");
    return p;
} else if (p == FINGERPRINT_FLASHERR) {
    Serial.println("Error writing to flash");
    return p;
} else {
    Serial.println("Unknown error");
    return p;
}

return FINGERPRINT_OK;
}
```