

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

«Програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino».
Назва теми

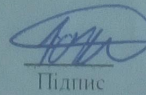
КВРКІ 180230.18.02.07 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

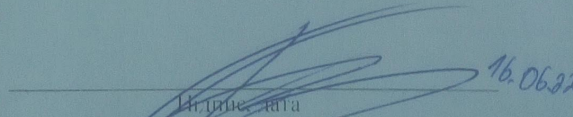
Освітня програма «Комп'ютерна інженерія»
Назва

Виконав: студент IV курсу, група КІ-18-2


Підпис

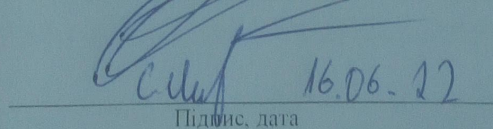
Юрій ЖИГАЛЬСЬКИЙ
Ініціали, прізвище

Керівник


Підпис, дата

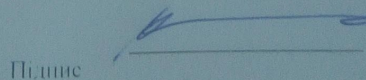
16.06.22 Ігор МУЛЯР
Ініціали, прізвище

Нормоконтролер


Підпис, дата

Сергій МОСТОВИЙ
Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки


Підпис

Юрій КЛЮЧ
Ініціали, прізвище

« 16 » червня 2022 р.

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЯ ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Кльоц Ю.П.

“ ” 2022 р.

103

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА**

Жигальському Юрію Вікторовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino

Керівник проекту (роботи) Муляр І.В., к.т.н, доцент

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

Затверджена наказом ректора університету від 01.03.2022 р. №

2. Строк подання студентом проекту (роботи) на кафедру _____

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

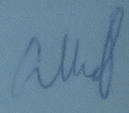
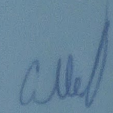
4. Дослідження предметної області та постановка задачі; обґрунтування базових положень щодо проектування пристрою контролю доступу. Опис схем електричних (структурної) проектованої системи; опис алгоритму роботи системи

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

Схема електрична структурна (Е1)», «Схема електрична функційна (Е2)».

«Схема електрична принципова (Е3)», «Алгоритм роботи (Е8)»

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		
Антиплагіат	Мостовий С.В., старший викладач кафедри кібербезпеки		

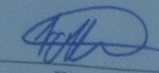
7. Дата видачі завдання «__» _____ 2022 р.

КАЛЕНДАРНИЙ ПЛАН

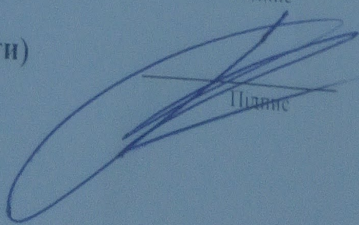
№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Приміт
1	Вибір напрямку дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2022	виконав
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2022	виконав
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	01.03.2022	виконав
4	Робота над розділом 2 – проектування пристрою для контролю доступу в приміщення за відбитком пальця	01.04.2022	виконав
5	Робота над розділом 3 – програмно-технічна реалізація замка з відбитком пальця	30.04.2022	виконав
6	Оформлення пояснювальної записки згідно вимог	20.05.2022	виконав
7	Попередній захист ВКР	16.05.2022	виконав
8	Захист ВКР на засіданні ЕК	17.06.2022	виконав

Студент

Керівник проекту (роботи)


Підпис

Ю.В. Жигальський
Ініціали, прізвище


Підпис

І.В. Муляр
Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino

Автор роботи: Юрій ЖИГАЛЬСЬКИЙ

Керівник роботи: к.т.н., доц. Ігор МУЛЯР

Пояснювальна записка: 55 с., 37 рис., 5 табл., 4 дод., 38 джерел.

Графічна частина: 4 плакати.

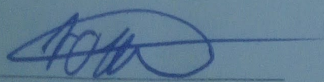
ПРОГРАМНО-АПАРАТНИЙ ПРИСТРІЙ, КОНТРОЛЬ ДОСТУПУ В ПРИМІЩЕННЯ, ARDUINO

Основна ідея проекту – створити недорогий пристрій для відкривання дверного механізму за допомогою зчитування відбитка пальця, на платформі Arduino.

Метою кваліфікаційної роботи є створити недорогий пристрій для відкривання дверного механізму за допомогою зчитування відбитка пальця, на платформі Arduino.

Об'єктом дослідження є процес зчитування біометричних даних з користувача, для подальшої їх обробки, для надання доступу в приміщення.

Предметом дослідження є програмно-апаратний засіб для контролю доступу в приміщення на основі платформи Arduino



Підпис студента

13.06.22

Дата

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

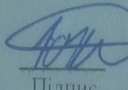
«Програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino».
Назва теми

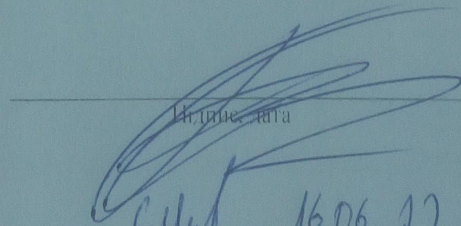
КВРКІ 180230.18.02.07 ПЗ
Шифр

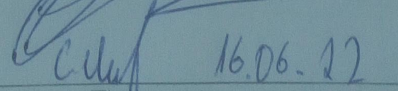
Галузь знань 12 «Інформаційні технології»
Шифр, назва

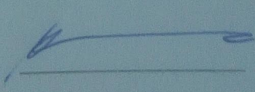
Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

Освітня програма «Комп'ютерна інженерія»
Назва

Виконав: студент IV курсу, група KI-18-2  Юрій ЖИГАЛЬСЬКИЙ
Підпис Ініціали, прізвище

Керівник  16.06.22 Ігор МУЛЯР
Підпис, дата Ініціали, прізвище

Нормоконтролер  16.06.22 Сергій МОСТОВИЙ
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки  Юрій КЛЬОЦ
Підпис Ініціали, прізвище

« 16 » червня 2022 р.

2.4 Підключення РК дисплею	35
2.5 Підключення Електромагнітного дверного замка 12V	37
2.6 Під'єднання GSM модуля	39
2.7 Висновок	42
3 ПРОГРАМНО-ТЕХНІЧНА РЕАЛІЗАЦІЯ ПРИСТРОЮ ДЛЯ КОНТРОЛЮ	
ДОСТУПУ В ПРИМІЩЕННЯ ЗА ВІДБИТКОМ ПАЛЬЦЯ	43
3.1 З'єднання необхідних компонентів	43
3.2 Підключаємо сенсор відбитків пальців до Arduino.	45
3.3 Підключення РК дисплею	49
3.4 Підключення Електромагнітного дверного замка	50
3.6 Збирання пристрою	52
3.7 Схеми до пристрою та оцінка їх вартості	54
3.8 Висновок	57
ВИСНОВКИ	58
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ.....	59
Додаток А Схема електрична структурна.....	63
Додаток Б Схема електрична Функційна.....	64
Додаток В Схема електрична принципова.....	65
Додаток Г Блоксхема алгоритму роботи програми.....	66
Додаток Д Лістинг коду для керування безпілотним апаратом	67

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

LED – Світловипромінюючий діод

РКД – Рідкокристалічний дисплей

DHT – Датчик температури і вологості

ШИМ – Широтно-імпульсна модуляція

GSM – Global System for Mobile

РКД – рідкокристалічний дисплей

					КВРКІ 180230.18.02.07 ПЗ	Арк
						4
Зм.	Арк.	№докум.	Підпис	Дата		

ВСТУП

Мабуть в кожного з нас були випадки в житті, коли губили ключі від квартири, або забували їх, або не могли потрапити до квартири за різних обставин пов'язаних з відсутністю ключів. Частіше за все в таких випадках потрібно турбувати інших людей, які мають дублікати ключів, або в гіршому випадку викликати майстрів, або навіть пошкоджувати замок. Погодьтеся, не сама приємна ситуація, яка за собою веде багато проблем, і дискомфорт. Але технологічний процес не стоїть на місці і зараз у вас є багатий вибір розумних дверних замків для контролю доступу в приміщення за відбитком пальця.

Системи дверних замків на основі відбитків пальців використовують біометричну ідентифікацію, щоб полегшити наше життя. Окрім того, що вони виглядають надзвичайно круто. Якщо говорити за безпечність, то замок з відбитком пальця має набагато більший рівень захисту ніж традиційний замок. Традиційна система на основі замків і ключа має багато вразливостей. Головним з них є те, що ключ можна легко скопіювати. Це призведе до неприємних сюрпризів у будь-який момент часу. Наслідки ще більш серйозні, коли заклад використовується як місце для бізнесу.

Багато людей думає, що такий замок- це дорого і не вигідно, але дарма. Хоча вам доведеться заплатити більше за дверний замок на основі відбитків пальців, він обов'язково прослужить довше, ніж звичайний замок і ключ, які схильні до іржі, зношування та розривів. Системи дверних замків за відбитком пальців також ідеально підходять для комерційних закладів, де вони часто використовуються.

Отже, періодичні витрати на заміну можна позбутися, встановивши попередню. Це дозволить вам заощадити свої тяжко зароблені гроші в довгостроковій перспективі.

Користуватися таким пристроєм значно зручніше і швидше. З системою на основі відбитків пальців все, що вам потрібно зробити, це притиснути палець до сканера без додаткових інструментів. Це робить процес досить простим і швидким.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						5
Зм.	Арк.	№докум.	Підпис	Дата		

Клавiші трохи складніше обробляти, не кажучи вже про те, що ви повинні не забути тримати їх при собі.

Наявність дверного замка на основі відбитків пальців додає вигляду та шарму приміщенню. Він одразу викликає трепет і посилає попереджувальний сигнал тим, хто може подумати про проникнення.

Оскільки технології стрімко рухаються вперед, немає причин, чому б ми також не взяли на себе лiдерство. Святiсть наших будинків/офісів має першочерговий пріоритет, і системи замків на основі відбитків пальців, безсумнівно, досягнуть цієї мети.

Тому створення програмно-апаратного пристрою для контролю доступу в приміщення на базі Arduino є як ніколи актуальним.

У роботі показано, процес створення програмно-апаратного пристрою для контролю доступу в приміщення на базі Arduino, розроблено прототипи замків, показано, як створити такий замок, які бувають варіанти замків і що нам для цього знадобиться.

У першому розділі передбачається провести аналіз та огляд теоретичних матеріалів, порівняння існуючих аналогів, обговорення їх «плюсів» і «мінусів» для створення розумного дверного замка з сенсором відбитків пальців.

У другому розділі буде зроблена оцінка моделей, які будуть використовуватися для конструювання і буде визначено з якими цілями використовуватимуться відповідні компоненти.

У третьому розділі буде детально описано реалізація схеми створення замка з датчиком відбитка пальця

Метою кваліфікаційної роботи є створення недорогого механізму для контролю доступу в приміщення за відбитком пальця на Arduino.

Об'єктом дослідження є процес зчитування інформації про відбиток пальця за допомогою датчику та порівняння його з збереженими відбитками.

Предметом дослідження є програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на базі Arduino.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						6
Зм.	Арк.	№докум.	Підпис	Дата		

1 ОГЛЯД ПРОГРАМНО АПАРАТНИХ ПРИСТРОЇВ ДЛЯ КОНТРОЛЮ ДОСТУПУ В ПРИМІЩЕННЯ ЗА ВІДБИТКОМ ПАЛЬЦЯ

1.1 Історія виникнення, та відбитки пальців, як біометричні дані

Ідентифікація відбитків пальців існує вже кілька століть. Більшу частину цього часу відбитки пальців використовувалися для ідентифікації злочинців. Доктор Генрі Фолдс і Вільям Гершель були одними з перших людей, які використали відбитки пальців як метод ідентифікації. У 1897 році Едвард Генрі винайшов систему, яка класифікувала відбитки пальців за категоріями на основі їх візерунків і призначала числові значення цим типам візерунків. На початку 1900-х років військові Сполучених Штатів почали використовувати систему класифікації Генрі для ідентифікації військовослужбовців. Останнім часом відбитки пальців досить часто використовуються для безпечного доступу, ідентифікації злочинців, ідентифікації померлого [1].

Відбитки пальців мають багато властивостей, які роблять ідентифікацію відбитків пальців хорошою біометричною ідентифікацією особи. Оскільки відбитки пальців по суті універсальні (тобто більшість людей мають відбитки пальців), цю систему може використовувати практично будь-хто. Ще однією перевагою відбитків пальців є їх унікальність. Мало того, кожна людина має відбитки пальців, але всі відбитки пальців є різними. Відбитки пальців навіть відрізняються від пальця до пальця на одній руці. Загалом, відбитки пальців можна легко записати, а процес ідентифікації є швидким, ефективним і, головне, точним. З етичної точки зору використання відбитків пальців стало загально визнаним суспільством як метод ідентифікації, і для цієї системи немає очікуваних проблем, тим більше, що вона розроблена для особистого використання. Загалом, відбитки пальців є точним, простим і прийнятним методом ідентифікації особи [15].

					КВРКІ 180230.18.02.07 ПЗ	Арк
						7
Зм.	Арк.	№докум.	Підпис	Дата		

1.2 Аналіз предметної області та виявлення наявних проблем і завдань

Дверний замок з відбитком пальця- це система, яка надає доступ уповноваженому персоналу на основі розпізнавання їх унікальних відбитків пальців. Відбитки пальців людини надзвичайно деталізовані і майже унікальні. Більше того, їх також дуже важко підробити або змінити, і вони можуть витримати протягом життя людини. Це робить їх дуже придатними як довгострокові маркери людської ідентичності. Коли технологія, яка може розпізнавати та розрізняти відбитки пальців, розгортається для забезпечення доступу до дверного отвору, ви отримуєте «Систему для контролю доступу в приміщення за відбитком пальця». Замки з відбитками пальців працюють шляхом сканування та перетворення даних відбитків у числовий шаблон [7].

Після того, як ви вперше помістили палець на сканер, відбудеться перетворення в числові дані, а шаблон відбитка пальця буде збережено. Потім цей процес повторюється щоразу, коли ви хочете надати комусь доступ. Наступного разу, коли хтось покладе палець на датчик, він зіставляє дані, отримані пальцем, із попередньо збереженими значеннями. Якщо збіг знайдено, доступ надається і двері відчиняються. З іншого боку, якщо хтось інший намагається пройти, доступ заборонений, а двері залишаються замкненими.

Тепер узгодження алгоритму є найважливішим процесом . Зазвичай це досягається за допомогою процесу зіставлення Minutia [13]. При цьому на подушечках ваших пальців розташовані кілька дрібниць, а також їх положення та напрямок під час першої реєстрації. Ця інформація зберігається в пам'яті. Під час збігу вже збережений шаблон відбитка пальця порівнюється з отриманим введенням. Якщо є збіг, зазвичай про це сигналізує зелений світлодіод і двері відкриваються. Процес дуже швидкий і завершується за частки секунди.

Більшість інтелектуальних дверних замків з відбитками пальців використовують структуру ручки, стандартний замок дверей з ручкою, як зображено на рисунку 1.1 [2].

					КВРКІ 180230.18.02.07 ПЗ	Арк
						8
Зм.	Арк.	№докум.	Підпис	Дата		



Рисунок 1.1- Стандартний розумний замок дверей з ручкою

Цей дверний замок складається з трьох частин: врізної частини замку, ручки та запірної планки.

За нормальних обставин врізна частина інтелектуального дверного замка з відбитками пальців аналогічна традиційному замку дверей, і як і раніше використовується корпус звичайного механічного замка [5].

Для дверних замків з декількома способами розблокування модуль розпізнавання відбитків пальців часто розміщується в частині ручки, що найбільше підходить для користувачів, щоб відкрити двері - звичка використовувати відбитки пальців для розблокування. Такий тип розміщення сенсора відбитків пальців показано на рисунку 1.2 [2].

Зм.	Арк.	№докум.	Підпис	Дата



Рисунок 1.2 – Дверний замок з датчиком відбитка пальця вбудованим в ручку

Панельна частина є частиною з високим технічним змістом всього дверного замка по відбитку пальця.

У цій частині зосереджено більшість електронних компонентів, у тому числі панелі паролів, модулі камер, батареї тощо, які забезпечують інші функції, які необхідні для інтелектуальних дверних замків.

За типом встановлення дверні замки з відбитком пальця можна поділити на:

1. Врізні;
2. Навісні [2].

Врізні встановлюються безпосередньо в двері. Вони найнадійніші проти силового взлому, але вони і найскладніші у встановленні. Врізний замок з відбитком пальця зображено на рисунку 1.3 [2].

Зм.	Арк.	№докум.	Підпис	Дата



Рисунок 1.3- Врізний замок з відбитком пальця

Навісні дверні замки мають автономну конструкцію, яка не залежить від елементів фіксації. Вони складаються з корпусу, механізм всередині нього, і запірної дужки, за допомогою якої і відбувається замикання замка. Зовнішній вигляд навісного замка з відбитком пальця показано на рисунку 1.4 [2].

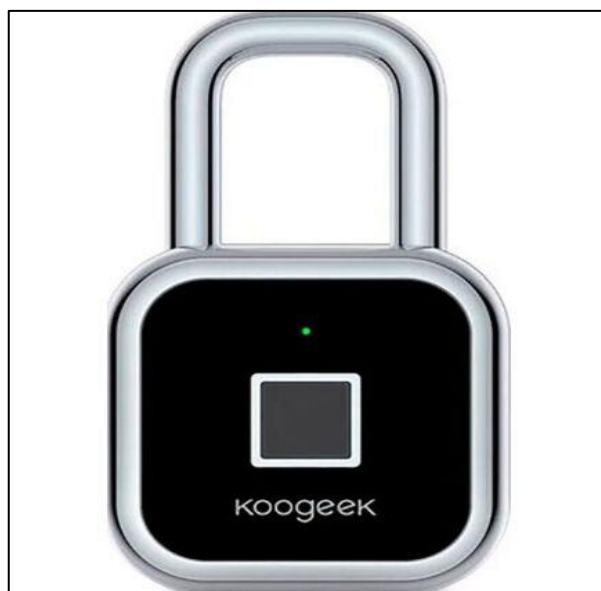


Рисунок 1.4- Навісний замок з відбитком пальця

Arduino — це електронна платформа з відкритим вихідним кодом, заснована на простому у використанні апаратному та програмному забезпеченні. Плати Arduino здатні зчитувати вхідні дані – світло на датчику, палець на кнопці або повідомлення в Twitter – і перетворювати їх на вихідні дані – активуючи двигун, вмикаючи світлодіод, публікуючи щось в Інтернеті. Ви можете задати своїй платі, що робити, надіславши набір інструкцій до мікроконтролера на платі. Для цього ви використовуєте мову програмування Arduino та програмне забезпечення arduino (IDE) на основі обробки.[7]

Протягом багатьох років Arduino був мозком тисяч проектів, від повсякденних об'єктів до складних наукових інструментів. Всесвітня спільнота студентів-виробників, любителів, художників, програмістів та професіоналів – зібралася навколо цієї платформи з відкритим кодом, їхній внесок додав неймовірну кількість доступних знань, які можуть бути дуже корисними як новачкам, так і експертам [3].

Arduino була створена в інституті проектування взаємодії Ivrea як простий інструмент для швидкого створення прототипів, призначений для студентів без досвіду в електроніці та програмуванні. Як тільки спільнота навколо неї стала більш ширшою, плата Arduino почала змінюватися, щоб адаптуватися до нових потреб і викликів, диференціюючи свою пропозицію від простих 8-розрядних плат до продуктів для додатків IOT, носіїв, 3D-друку та вбудованих середовищ. Усі плати Arduino повністю відкриті, що дає користувачам можливість самостійно створювати їх і в кінцевому підсумку адаптувати їх до своїх особливих потреб. Програмне забезпечення також є відкритим вихідним кодом, і воно зростає завдяки внеску користувачів з усього світу [15].

1.3 Порівняльний аналіз переваг та недоліків існуючих рішень

Системи на основі відбитків пальців, хоча і дуже корисні, однак мають деякі недоліки і як не дивно, багато з них випливають із самих переваг системи. Хоча їх дуже і дуже важко обдурити, це не неможливо. Сканери, які використовують

					КВРКІ 180230.18.02.07 ПЗ	Арк
						12
Зм.	Арк.	№докум.	Підпис	Дата		

оптичні системи для отримання інформації, іноді можуть бути обдурені зображенням пальця. З іншого боку, людина може обійти сканери на основі конденсаторів за допомогою форми. Цих ситуацій можна уникнути за допомогою імпульсних і теплових сповіщувачів, які також називаються живими пальцями.

Ще одна серйозна проблема з дверними замками на основі відбитків пальців полягає в тому, що якщо комусь таки вдасться створити копію/зліпок/зображення вашої руки, яка може відкрити двері, у вас серйозні проблеми. Оскільки ви не можете скинути відбитки пальців так, як ви можете за допомогою звичайного пароля, це означає або заміну замків, або використання комбінації PIN-коду та відбитків пальців.

Крім того, іноді сканер може відмовитися розпізнати ваш палець у разі утворення рубців, порізів чи садна. Відключення електроенергії, розряд батареї є іншими поширеними проблемами, пов'язаними з цими системами блокування дверей, які можуть залишити вас за межами робочого місця чи офісу. Їх запобігає інтеграція механічної системи, де ви можете використовувати ключ, щоб відімкнути двері в разі такої несправності [23].

Звичайно, більшість дверних замків з відбитками пальців мають більше одного методу відмикання.

Найбільш поширені смарт-замки з відбитками пальців на ринку – це пароль + біометрія (розпізнавання обличчя, розпізнавання відбитків пальців тощо).

Звичайно, існують і інші біометричні системи, які включають багато переваг, пов'язаних із системами блокування відбитків пальців. Наприклад, сканування райдужної [9] оболонки ока усуває невеликий потенціал порушень безпеки, які залишаються системами на основі відбитків пальців. Аутентифікація на основі голосу, з іншого боку, дозволяє просто говорити, щоб відкрити двері, навіть не вимагаючи, щоб ви клали на них палець.

Однак сканери райдужної оболонки ока дуже дорогі в порівнянні з системами дверних замків за відбитками пальців, і багатьом людям може здатися незручним досвід сканування очей. Хоча він здається ідеальним для державних

установ високого рівня безпеки, дверні замки за відбитками пальців набагато доступніші та зручніші, коли про них говорять вдома чи в офісі.

Так само, незважаючи на всі переваги, голосові біометричні системи відкривання дверей мають дуже серйозний недолік. Рівень невдач дуже високий. Можливо, у вас хрипне горло або застуда, і двері залишаться непохитними перед вами, відмовляючись розпізнати ваш голос [13].

Розглянемо різноманітні компоненти які можуть бути в дверному замку з відбитком пальця.

Вони включають в себе:

1. Передня і задня панелі;
2. зсувна кришка захисту панелей;
3. ручка;
4. датчик відбитка пальців;
5. клавіатура;
6. дисплей;
7. камера;
8. аварійне джерело живлення;
9. замкова щілина;
10. відсік для батареї;

Розглянемо їх більш детально.

Передня і задня панелі.

Панель розумного замку з відбитками пальців складається з трьох основних матеріалів: матеріалів із цинкового сплаву, матеріалів із нержавіючої сталі та матеріалів із алюмінієвого сплаву.

Панель з цинкового сплаву має гарну корозійну стійкість і високу твердість і є кращим вибором для панелей інтелектуальних замків з відбитками пальців основних виробників [17].

Зсувна кришка захисту панелей

					КВРКІ 180230.18.02.07 ПЗ	Арк
						14
Зм.	Арк.	№докум.	Підпис	Дата		

Інтелектуальний замок відбитків пальців зі зсувною кришкою може ефективно захистити модуль розпізнавання відбитків пальців та збільшити термін служби модуля розпізнавання відбитків пальців.

Однак багато дверних замків з відбитками пальців для будинку не мають розсувної кришки, тому що замки з відбитками пальців без розсувної кришки зручніше відкривати. [17]

Ручка

За формою рукоятки розумні замки з ручкою під палець можна розділити на натисно-витяжні та натискні.

Натискний тип має горизонтальну ручку, і двері потрібно натискати вниз, щоб відкрити двері, а тип натиску відкриває двері, натискаючи на ручку.

Домашнє блокування по відбитку пальця також може бути розділена на напівавтоматичне домашнє блокування по відбитку пальця і повністю автоматичне домашнє блокування по відбитку пальця.

Напівавтоматичний зазвичай означає, що вам потрібно натиснути або натиснути на ручку, щоб відкрити затвор після проходження розпізнавання відбитків пальців.

Повністю автоматичний домашній замок з відбитком пальця означає, що двигун автоматично відкриває засув після отримання розпізнавання відбитка пальця.

Напівавтоматичні замки з відбитками пальців необхідно підняти, щоб замкнути двері, а автоматичні замки з відбитками пальців замикаються автоматично, тому для повністю автоматичних замків потрібно більше електроенергії.

Датчик відбитка пальців [17]

Замки з датчиком відбитків пальців в основному мають два основних модулі ідентифікації: оптичний відбиток пальця та напівпровідниковий відбиток пальця.

Напівпровідниковий датчик відбитків пальців має набагато більш високу точність розпізнавання, ніж оптичний датчик відбитків пальців, а відсоток відмов низький [22].

					КВРКІ 180230.18.02.07 ПЗ	Арк
						15
Зм.	Арк.	№докум.	Підпис	Дата		

Тепер усі основні бренди датчиків відбитків пальців використовують напівпровідникові методи.

Шведський напівпровідниковий модуль ідентифікації з відбитка пальця простіше у використанні серед напівпровідникових модулів ідентифікації з відбитка пальця [22].

Клавіатура

Крім методів ідентифікації та розблокування відбитків пальців замки з датчиком відбитків пальців зазвичай підтримують режим введення пароля.

У кращих замках з датчиком відбитків пальців буде функція віртуального пароля.

З метою безпеки рекомендується регулярно змінювати довгостроковий пароль блокування по відбитку пальця.

Дисплей

Екран інтелектуального блокування дверей від відбитків пальців в основному використовується для відображення клавіатури та системних підказок.

У кращому розумному дверному замку відбитків пальців буде використовуватися дисплей, який не залишає відбитків пальців.

Відбиток пальця можна стерти одним стиранням, що ефективно запобігає витоку пароля.

Камера

Безпека замків від пальців впливових брендів вже досить висока, і людям з невеликим бюджетом не потрібно вибирати дверний замок відбитків пальців з камерою.

Дверний замок відбитків пальців із функцією камери — це вишенька на торті.

Аварійне джерело живлення

Оскільки розумні замки з відбитком пальця живляться від сухих або літєві акумуляторів, батарея неминуче розрядиться, і система розпізнавання відбитків пальців вийде з ладу.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						16
Зм.	Арк.	№докум.	Підпис	Дата		

Таким чином, замок відбитків пальців розроблений з портом аварійного живлення. Аварійне джерело живлення може перезапустити систему, коли внутрішнє джерело живлення відключено.

Порт аварійного живлення, як правило, сконструйований так, щоб бути більш прихованим, зазвичай прихованим у нижній частині замка.

Замкова щілина

Оскільки система ідентифікації відбитків пальців не завжди може гарантувати відсутність проблем, дверний замок також оснащується методом відкриття замкового механізму за допомогою механічного ключа.

Замок для відбитків пальців матиме замкову щілину. Як правило вона частіше за все прихована за для безпеки.

Відсік для батареї

Як правило, джерело живлення домашнього замка відбитків пальців є сухим літєвим акумулятором [17]. Літєва батарея краще, тому що літєва батарея може бути перезаряджена після розрядки, що зручніше.

Для порівняння я узяв кілька існуючих розумних замків.

На рисунку 1.5 зображено H-Gang Guardian TR811 [5]. У ньому використовується безліч нових технологій. Він може відкриватись за допомогою відбитка пальця та введення встановленого пароля.

Його можна використовувати на лівосторонніх та правосторонніх дверях, при цьому вони можуть бути дерев'яними чи залізними.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						17
Зм.	Арк.	№докум.	Підпис	Дата		



Рисунок 1.5 - Розумний замок H-Gang Guardian TR811

Характеристики:

- Пам'ять - на 100 відбитків пальців;
- Сирена- 80Дб;
- Матеріал з якого виготовлений - цинк; алюміній; ABS-пластик;
- Живлення - автономне, від 4 алкалінових батарейок 6V;
- Час роботи від батареї - до 1 року (при частоті відкривання 10 разів на добу);
- Робоча температура - від -15°C до +50°C №;
- Рівень вологості повітря – 40%-80%;

Замок ZkТесо PL10

Кодовий замок ZkТесо PL10 оснащений звуковим оповіщенням та колірною індикацією. Місткість замку - 90 зразків відбитків пальців. Працює він від чотирьох пальчикових батарей AA 1,5V. Монтується у дверях завтовшки 39-46 або 47-54 мм [5]. Дозволяє замикати двері квартир, гаражів та шаф. Зовнішній вигляд показано на рисунку 1.6.

Зм.	Арк.	№докум.	Підпис	Дата



Рисунок 1.6 - Розумний замок ZkTeco PL10

Характеристики:

- Пам'ять - на 90 відбитків пальців;
- Спосіб відкриття - ідентифікація відбитка пальця, механічний ключ;
- Матеріал з якого виготовлений - ABS-пластик;
- Живлення - автономне, від 4 алкалінових батарейок 6V;
- Час роботи від батареї - до 1 року (при частоті відкривання 15 разів на добу);
- Робоча температура - від 0°C до +50°C№;
- Рівень вологості повітря – 40%-80%;
- Країна виробник – China;

Розумний дверний замок Xiaomi Aqara Smart Door Lock Left Side [5]

Дверний замок Xiaomi Aqara Smart Door Lock Left Side, який зображений на рисунку 1.7, сумісний з іншими продуктами компанії Aqara. Наприклад, він може працювати з охоронними системами, датчиками відкриття та закриття вікон, увімкнення та відключення світла та іншими приладами.

Зм.	Арк.	№докум.	Підпис	Дата

КВРКІ 180230.18.02.07 ПЗ

Арк
19

Замок має клас безпеки В, тому його дуже важко зламати. При цьому система сигналізації включає тривогу та сповіщає всіх про спробу злому. Крім того, система сповіщає власника про подію за допомогою SMS-повідомлення, яке надходить на телефон власника після спроби зламування замка, а також після невдалого зчитування відбитка пальця або введення неправильного пароля (більше 3 разів).



Рисунок 1.7 - Розумний замок Xiaomi Aqara Smart Door Lock Left Side

Характеристики:

- Пам'ять - до 100 відбитків пальців;
- Спосіб відкриття пароль, відбиток пальця, програма Mi Home;
- Матеріал з якого виготовлений - метал;
- Живлення - 8 батарей АА;
- Час роботи від батареї - до 15 місяців (в режимі очікування);
- Спосіб підзарядки - Micro USB;
- Інтерфейси підключення – Bluetooth, Micro USB;
- Робоча температура - від -10°C до +50°C; [5]

1.4 Порівняльний аналіз переваг та недоліків існуючих рішень

1.4.1 Arduino

Arduino Atmega328p [7]

Arduino Atmega328p, яка зображена на рисунку 1.8 – це плата мікроконтролера на основі ATmega2560. Він має 54 цифрових входу/виходу (з яких 14 можуть використовуватися як виходи ШІМ), 16 аналогових входів, 4 UART (апаратні послідовні порти), кварцовий генератор 16 МГц, з'єднання USB, роз'єм живлення, ICSP HEADER, І КНОПКА ВІДПОВІДЬ. Він містить усе необхідне підтримки мікроконтролера; просто підключіть його до комп'ютера за допомогою кабелю USB або підключіть його до більшості плат, розроблених для Arduino Duemilanove або Diecimili. [11]

Характеристики:

- Мікроконтролер ATmega2560
- Робоча напруга 5 В
- Вхідна напруга (рекомендується) 7-12 В
- Вхідна напруга (межі) 6-20В
- Цифрові контакти введення/виводу 54 (з яких 14 забезпечують вихід ШІМ)
- Аналогові вхідні контакти 16
- Постійний струм на виведення I/P 40 мА
- Постійний струм для контакту 3,3 В 50 мА
- Флеш-пам'ять 256 КБ, у тому числі 8 КБ використовуються завантажувачем
- SRAM 8 КБ

					КВРКІ 180230.18.02.07 ПЗ	Арк
						21
Зм.	Арк.	№докум.	Підпис	Дата		

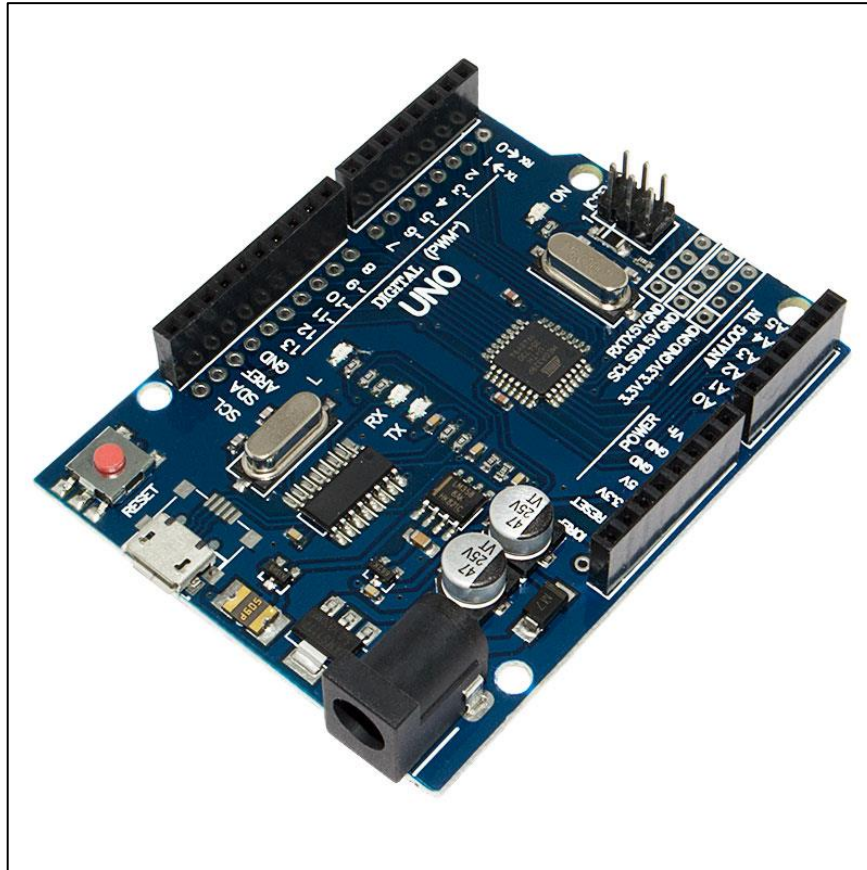


Рисунок 1.8 - Arduino Atmega328p

Arduino Atmega може живитись через USB-з'єднання або від зовнішнього джерела живлення. Джерело живлення вибирається автоматично.

Зовнішнє (не USB) живлення може надходити від адаптера змінного струму в постійний, або від акумулятора. Адаптер можна підключити, вставивши штекер 2,1 мм із центральним позитивним контактом у роз'єм живлення на платі. Виводи від акумулятора можна вставити в контактні гнізда Gnd і Vin роз'єму POWER. [11]

Плата може працювати від зовнішнього джерела живлення від 6 до 20 вольт. Однак при подачі менше 7 на контакт 5 може подаватися менше п'яти вольт, і плата може працювати нестабільно. При використанні більше 12 В регулятор напруги може перегрітися та пошкодити плату. Рекомендований діапазон від 7 до 12 вольт.

Atmega328p відрізняється від усіх попередніх плат тим, що не використовує мікросхему драйвера FTDI USB-to-serial. Натомість він оснащений Atmega8U2, запрограмованим як перетворювач USB-последовний порт.

Опис контактів живлення:

Зм.	Арк.	№докум.	Підпис	Дата

+VIN: - Вхідна напруга плати Arduino, коли вона використовує зовнішнє джерело живлення (на відміну від вольт від роз'єму USB або іншого регульованого джерела живлення). Ви можете подавати напругу через цей контакт або, якщо подавати напругу через роз'єм живлення, отримати доступ через цей контакт.

+5V: Регульоване джерело живлення, яке використовується для живлення мікроконтролера та інших компонентів на платі. Це може бути від VIN вбудованого регулятора, або від USB або іншого джерела живлення 5 В.

+3V3: - Джерело живлення 3,3 В, що генерується вбудованим регулятором. Максимальний струм 50 мА.

GND: контакти заземлення.

ATmega2560 має 256 КБ флеш-пам'яті для зберігання коду (з яких 8 КБ використовується для завантажувача), 8 КБ SRAM та 4 КБ EEPROM (які можна читати та записувати за допомогою бібліотеки EEPROM).[23]

Кожен із 54 цифрових контактів на Mega може використовуватися як вхід або вихід з використанням функцій pin Mode(), digital Write() та digital Read(). Вони працюють від 5 вольт. Кожен контакт може забезпечити або отримати максимум 40 мА і має внутрішній резистор (за замовчуванням відключений) на 20-50 кОм. Крім того, деякі контакти мають спеціальні функції [23]:

Серійний номер: 0 (RX) та 1 (TX); Серійний 1:19 (RX) та 18 (TX); Серійний 2:17 (RX) та 16 (TX); Серійний 3:15 (RX) та 14 (TX). Використовується для прийому (RX) та передачі (TX) послідовних даних TTL. Контакти 0 та 1 також підключені до відповідних контактів мікросхеми ATmega8U2 USB-to-TTL Serial.

Зовнішні переривання: 2 (переривання 0), 3 (переривання 1), 18 (переривання 5), 19 (переривання 4), 20 (переривання 3) та 21 (переривання 2). Ці контакти можуть бути налаштовані для запуску переривання за низьким значенням, переднім або заднім фронтом або зміною значення. Подробиці див. у розділі прикріпити функцію interrupt().

ШІМ: від 0 до 13. Забезпечте 8-бітовий вихід ШІМ із функцією аналогового запису (). SPI: 50 (MISO), 51 (MOSI), 52 (СКК), 53 (СС). Ці контакти підтримують

зв'язок SPI, використовуючи бібліотеку SPI. Висновки SPI також з'являються в заголовку ICSP, який фізично сумісний з Uno, Duemilanove та Diecimila.

Світлодіод: 13. До цифрового контакту 13 підключено вбудований світлодіод. Коли на контакті ВИСОКОЕ значення, світлодіод горить, коли на НИЗЬКОМУ - вимкнено.

I2C: 20 (SDA) та 21 (SCL). Підтримка зв'язку I2C (TWI) з використанням бібліотеки Wire

1.4.2 Серводвигун

Серводвигун - це поворотний привід або лінійний привід, який дозволяє точно керувати кутовим або лінійним положенням, швидкістю та прискоренням. Він складається з відповідного двигуна, з'єднаного з датчиком зворотного зв'язку. Для цього також потрібний відносно складний контролер, часто спеціальний модуль, розроблений спеціально для використання із серводвигунами.

Серводвигуни не відносяться до певного класу двигунів, хоча термін серводвигун часто використовується для позначення двигуна, що підходить для використання в системі управління зі зворотним зв'язком. Зображення сервоприводу показано на рисунку 1.9 [9].



Рисунок 1.9 - Серводвигун

Зм.	Арк.	№докум.	Підпис	Дата

1.4.3 Датчик відбитків пальців

Відбиток пальця – це відбиток, залишений гребенями тертя людського пальця. Відновлення часткових відбитків пальців з місця злочину є важливим методом криміналістики. Волога та жир на пальці призводять до появи відбитків пальців на таких поверхнях, як скло або метал. Умисні відбитки цілих відбитків пальців можуть бути отримані шляхом перенесення чорнила або інших речовин з вершин тертя на шкіру на гладку поверхню, наприклад папір. Записи відбитків пальців зазвичай містять відбитки подушечок на останніх суглобах і великих пальців, хоча карти відбитків пальців також зазвичай записують ділянки нижніх суглобів пальців.

Відбитки пальців людини деталізовані, майже унікальні, їх важко змінити і вони зберігаються протягом усього життя людини, що робить їх придатними як довгострокові маркери особи людини. Вони можуть використовуватися поліцією або іншими властями для виявлення осіб, які хочуть приховати свою особистість, або для виявлення людей, які неїездатні або померли і таким чином не можуть ідентифікувати себе, наприклад, після стихійного лиха.

Зображення датчику відбитків пальців представлено на рисунку 1.10 [9].



Рисунок 1.10 - Датчик відбитків пальців

Зм.	Арк.	№докум.	Підпис	Дата

1.4.4 Джерело живлення

Батарея на дев'ять вольт, або 9-вольтова батарея є поширеним розміром батареї, яка була введена для ранніх транзисторних радіоприймачів. Він має форму прямокутної призми із закругленими кінцями і поляризованим замикаючимся роз'ємом нагорі. Цей тип зазвичай використовується в раціях, годинниках та детекторах диму.

Формат дев'ятивольтової батареї зазвичай доступний у первинній вуглецево-цинковій та лужній хімії, у первинній літій-залізо-дисульфідній формі та в перезаряджуваній формі в нікель-кадмієвій, нікель-металогідридній та літій-іонній. Ртутно-оксидні батареї цього формату, які колись були поширені, вже багато років не виробляються через вміст у них ртуті. Позначення для цього формату включають NEDA 1604 та IEC 6F22 (для вугільно-цинкових) або MN1604 6LR61 (для лужних). Розмір незалежно від хімічного складу зазвичай позначається PP3 - позначення, спочатку зарезервоване виключно для вуглецево-цинкового, а в деяких країнах - E або E-block.

1.4.5 Світловипромінюючий діод

Світловипромінюючий діод (LED) - це напівпровідниковий джерело світла, яке випромінює світло при протіканні через нього струму. Електрони у напівпровіднику рекомбінують з електронними дірками, вивільняючи енергію у вигляді фотонів. Цей ефект називається електролюмінесценцією. Колір світла (відповідний енергії фотонів) визначається енергією, яка потрібна електронам для перетину забороненої зони напівпровідника. Біле світло виходить при використанні декількох напівпровідників або шару світловипромінюючого люмінофора на напівпровіднику. пристрій.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						26
Зм.	Арк.	№докум.	Підпис	Дата		

1.4.6 Рідкокристалічний дисплей (РКД)

Рідкокристалічний дисплей (РКД), зображений на рисунку 1.11 - це плоскопанельний дисплей або інший оптичний пристрій з електронною модуляцією, в якому використовуються світломодулюючі властивості рідких кристалів. Рідкі кристали не випромінюють світло безпосередньо, а використовують підсвічування або відбивач для створення кольорових або монохромних зображень. Доступні РК-дисплеї для відображення довільних зображень (як на звичайному комп'ютерному дисплеї) або фіксованих зображень з низьким інформаційним вмістом, які можна відобразити або приховувати, наприклад, присутні слова, цифри та семисегментні дисплеї, як у цифровому годиннику . . Вони використовують ту саму базову технологію, за винятком того, що довільні зображення складаються з великої кількості дрібних пікселів, тоді як інші дисплеї мають більші елементи. РК-дисплеї можуть бути нормально включені (позитивно), або вимкнені (негативно), залежно від розташування поляризатора. Наприклад, символічний позитивний РК-дисплей з підсвічуванням матиме чорні літери на фоні того ж кольору, що і підсвічування, а символічний негативний РК-дисплей матиме чорний фон з літерами того ж кольору, що і підсвічування. До білого кольору на синіх РК-дисплеях додаються оптичні фільтри, щоб надати їм характерного вигляду.



Рисунок 1.11- РКД

Зм.	Арк.	№докум.	Підпис	Дата

1.4.7 Зумер

Зумер- це сигнальний пристрій, зазвичай електронний, зазвичай використовується в автомобілях, побутових приладах, таких як мікрохвильова піч або ігрові шоу. Найчастіше воно складається з низки перемикачів або датчиків, підключених до блоку управління, який визначає була натиснута кнопка або закінчився заданий час, і зазвичай загоряється індикатор на відповідній кнопці або на панелі керування і звучить попередження у вигляді безперервного або переривчастого дзижчання або звукового сигналу. Спочатку цей пристрій був заснований на електромеханічній системі, яка була ідентична електричному дзвінку без металевого гонгу (що видає дзвін). Часто ці пристрої кріпилися до стіни або стелі і використовували стелю або стіну як резонатор. Інша реалізація з деякими пристроями, підключеними до змінного струму, полягала в реалізації схеми, що перетворює змінний струм на шум, досить гучний, щоб керувати гучномовцем, і підключити цю схему до дешевого 8-омного динаміка. В даний час більш популярно використовувати п'єзоелектричний ехолот на керамічній основі, такий як оповіщення про сина, який видає високий тон. Зазвичай вони були підключені до схем драйвера, які змінювали висоту звуку або включали і вимикали звук. Вигляд зумера показано на рисунку 1.12.



Рисунок 1.12- Зумер

Зм.	Арк.	№докум.	Підпис	Дата

1.4.8 Датчик DHT

Я буду використовувати не дорогі датчики температури і вологості. Ці датчики дуже прості та повільні, але чудово підходять для любителів, які хочуть вести базову реєстрацію даних. Датчики DHT складаються з двох частин: ємнісного датчика вологості та термістора. У середині також є дуже простий чіп, який виконує аналого-цифрове перетворення та видає цифровий сигнал із температурою та вологістю. Цифровий сигнал досить легко зчитується за допомогою будь-якого мікроконтролера. Датчик DHT зображений на рисунку 1.13 [10].

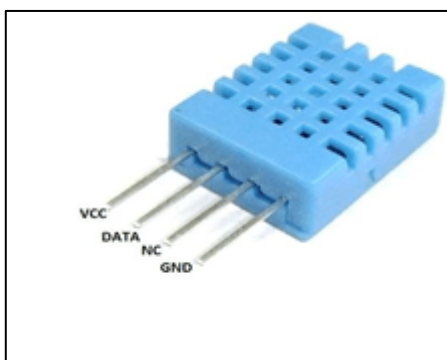


Рисунок 1.13 - Датчик DHT

1.4.9 Потенціометр

Потенціометр, зображений на рисунку 1.14, являє собою триполюсний резистор зі ковзним або обертовим контактом, який утворює регульований діляник напруги [10]. Якщо використовуються лише дві клеми, один кінець та контактор, він діє як змінний резистор або реостат. Вимірювальний прилад, званий потенціометром, являє собою діляник напруги U та використовуваний для вимірювання електричного потенціалу U (Напруга); компонент є реалізацією того ж принципу, звідси та його назва. Потенціометри зазвичай використовуються для керування електричними пристроями, такими як регулятори гучності на аудіообладнанні. Потенціометри, керовані механізмом, можуть використовуватися як датчики положення, наприклад, джойстику.

Зм.	Арк.	№докум.	Підпис	Дата

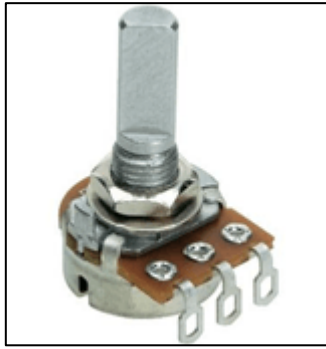


Рисунок- 1.14- Потенціометр

1.4.10 Кнопка

Кнопка – це простий механізм перемикання для керування будь-яким аспектом машини чи процесу [10]. Зображений на рисунку 1.15. Кнопки зазвичай виготовляються із твердого матеріалу, зазвичай із пластику або металу. Поверхня зазвичай плоска або має форму, що підходить для людського пальця або руки, щоб її можна було легко натискати або натискати. Кнопки найчастіше являють собою перемикачі зі зміщенням, хоча багатьом кнопкам без зміщення (через їхню фізичну природу), як і раніше, потрібна пружина, щоб повернутися в ненатиснутий стан.



Рисунок 1.15- Кнопка

Зм.	Арк.	№докум.	Підпис	Дата

1.4.11 Тримач батареї

Тримач батареї є один або кілька відсіків або камер для зберігання батареї. Для сухих елементів тримач також повинен мати електричний контакт із клемми батареї. Для вологих елементів кабелі часто підключаються до клем акумулятора, як у автомобілях або в обладнанні аварійного освітлення.

Тримач батареї являє собою або пластиковий корпус з формою корпусу, відформованою у вигляді відсіку або відсіків, в який міститься акумулятор або акумулятори, або окремий пластиковий утримувач, який кріпиться за допомогою гвинтів, люверсів, клею, двостороннього скотчу або інших засобів. Тримачі батареї можуть мати кришку для утримання та захисту батареї або можуть бути запечатані, щоб запобігти пошкодженню схем та компонентів через витік батареї. Спиральний пружинний дріт або плоскі виступи, що притискаються до клем акумулятора, є двома найбільш поширеними методами електричного з'єднання всередині тримача. Зовнішні з'єднання на тримачах батареї зазвичай виконуються контактами зі штирками, ніжками для поверхневого монтажу, наконечниками для паяння або дрововими виводами.

1.5 Висновок

У розділі було проаналізовано програмно-апаратні складові та засоби для створення пристрою для контролю доступу в приміщення за відбитком пальця. Розглянуто існуючі аналоги, їх переваги та недоліки

В кваліфікаційній роботі потрібно розв'язати наступну задачу: побудувати програмно-апаратний засіб для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						31
Зм.	Арк.	№докум.	Підпис	Дата		

2 ПРОЄКТУВАННЯ ПРИСТРОЮ ДЛЯ КОНТРОЛЮ ДОСТУПУ В ПРИМІЩЕННЯ ЗА ВІДБИТКОМ ПАЛЬЦЯ

2.1 Принцип роботи системи

У цій системі користувач буде вводити відбиток пальця в сканер відбитків пальців, який підключений до дверної засувки через мікроконтролер. Після сканування відбитка система запускає свою базу даних і шукає відповідність. Якщо знайдено відповідний відбиток, засувка відкривається, і двері відкриваються. Те ж саме відбувається, коли користувач хоче заблокувати двері. Правильний відбиток пальця змушує засувку закриватися, замикаючи двері за користувачем.

Якщо надано неправильний відбиток пальця, система подає звуковий сигнал, який показує на РК-дисплеї «Спробуйте ще раз». Якщо надано 5 або більше неправильних відбитків пальців, тобто якщо хтось намагається безперервно проникнути всередину, система переходить у захищений режим, де дзвонить тривожний сигнал, показуючи «Режим паніки» на РК-екрані. Власнику надходить повідомлення про спробу злому, яка буде реалізовуватися за допомогою GSM-модуля.

У нашій розробці ми використовували Atmega328p як мікроконтролер, який є серцем системи. Оскільки Atmega328p має лише 28 контактів (по 14 з кожного боку), нам довелося використовувати два мікроконтролери Atmega328p.

У нашій розробці вся система буде кріпитися до дерев'яної дошки в якості підставки..

2.2 Підключення Arduino ATmega328P

Спочатку потрібно з'єднати Atmega328p між собою. Робимо це так, як показано на рисунку 2.1.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						32
Зм.	Арк.	№докум.	Підпис	Дата		

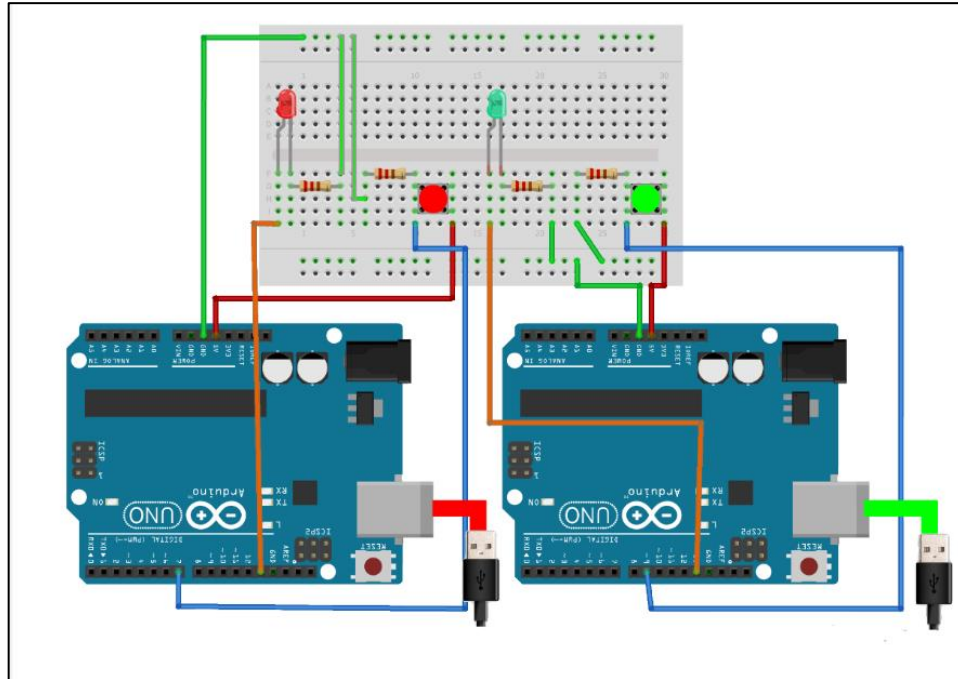


Рисунок 2.1 - З'єднання двох Arduino Atmega328p

Далі слід під'єднати датчик відбитків пальців.

2.3 Підключення датчика відбитків пальців

Цифровий зчитувач відбитків пальців

Біометричний датчик відбитків пальців ідеально підходить для створення системи, здатної захистити те, що вам потрібно за допомогою аналізу вашого відбитка пальця. Пристрій працює з послідовним протоколом, тому його можна використовувати з будь-яким мікроконтролером (arduino тощо) або картою розробки.

Пристрій може зберігати до 162 відбитків пальців у внутрішній флеш-пам'яті. Світлодіод пристрою загоряється щоразу, коли він знімає відбитки пальців.

-Модель: r307 Напруга живлення: 5В

-Робочий струм: 100 мА-150 мА

– Режим парності відбитків пальців: 1:1 1:n

-Швидкість передачі: $9600 * NN =$ від 1 до 12 (за замовчуванням 6)

-Час захоплення менше 1 секунди

Зм.	Арк.	№докум.	Підпис	Дата

-5 рівнів безпеки

-Розмір вікна: 14x18 мм

-Робоче середовище: від -10 °С до 40 °С (відносна вологість від 40% до 85%)

-Розміри: 5,5 x 2,1 x 2,0 см Вага: 22 г

Щоб мати можливість використовувати пристрій, необхідно зберегти відбитки пальців у його базі даних. Цим слідам надається ідентифікатор. Згодом можна запустити послідовність зчитування та порівняння для перевірки відбитків пальців користувачів і, таким чином, мати можливість розрізняти та виконувати дії на основі результату.

Що всередині в R307 датчик відбитків пальців показано на рисунку 2.2.

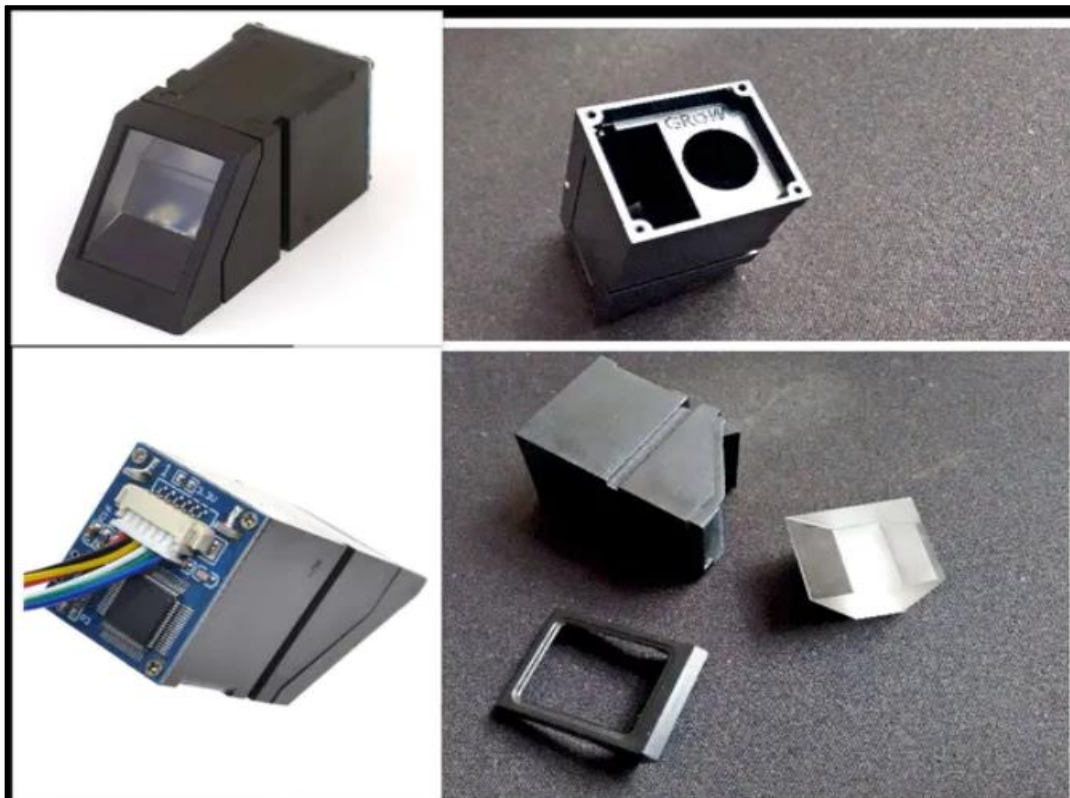


Рисунок 2.2 - Будова датчика зчитування відбитків пальців

Схема будови датчика відбитків пальців показана на рисунку 2.3

Зм.	Арк.	№докум.	Підпис	Дата

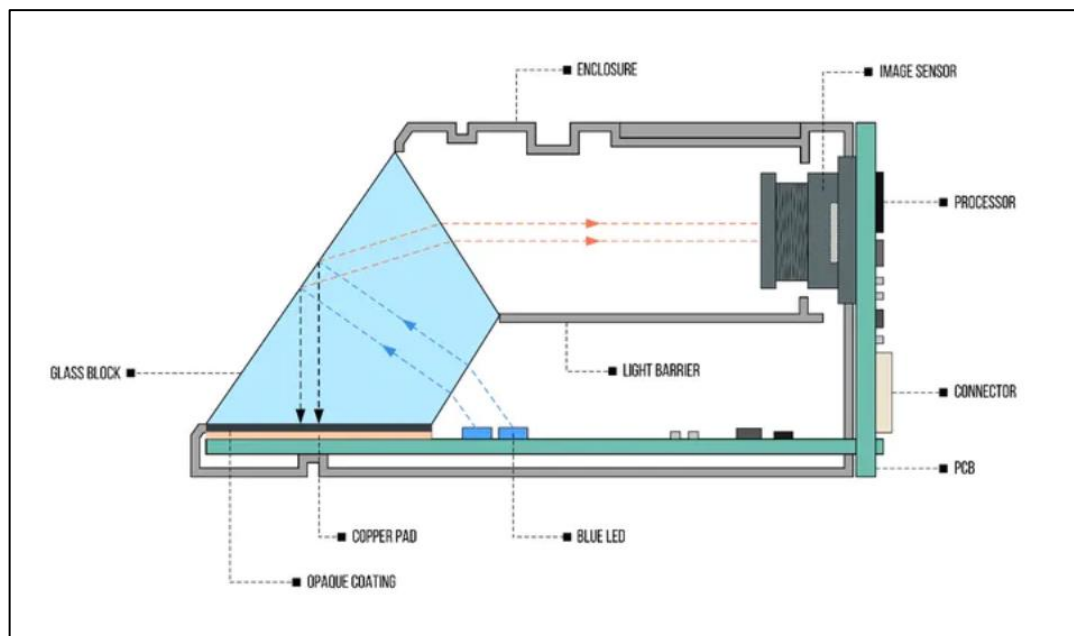


Рисунок 2.3- Схема датчика зчитування відбитків пальців

2.4 Підключення РК дисплею

РК-символьний дисплей — це унікальний тип дисплея, який може виводити лише окремі символи ASCII фіксованого розміру. Використовуючи ці окремі символи, ми можемо сформувати текст.

Якщо ми уважніше подивимося на дисплей, то можна помітити, що є невеликі прямокутні області, що складаються з сітки 5×8 пікселів. Кожен піксель може висвітлюватися окремо, тому ми можемо генерувати символи в кожній сітці.

Кількість прямокутних областей визначає розмір РК. Найпопулярнішим РК-дисплеєм є РК-дисплей 16×2 , який має два рядки з 16 прямокутними областями або символами. Звичайно, є й інші розміри, такі як 16×1 , 16×4 , 20×4 і так далі, але всі вони працюють за одним принципом. Крім того, ці РК-дисплеї можуть мати різний колір фону та тексту.

Розпіновка LCD 16×2

Він має 16 контактів, і перший зліва направо є контактом заземлення. Другий контакт - це VCC, до якого ми підключаємо 5-вольтовий контакт на платі Arduino. Далі йде висновок V_0 , до якого ми можемо прикріпити потенціометр для

Зм.	Арк.	№докум.	Підпис	Дата

контролю контрастності дисплея. Детальніше розпіновку можна подивитися на рисунку 2.4

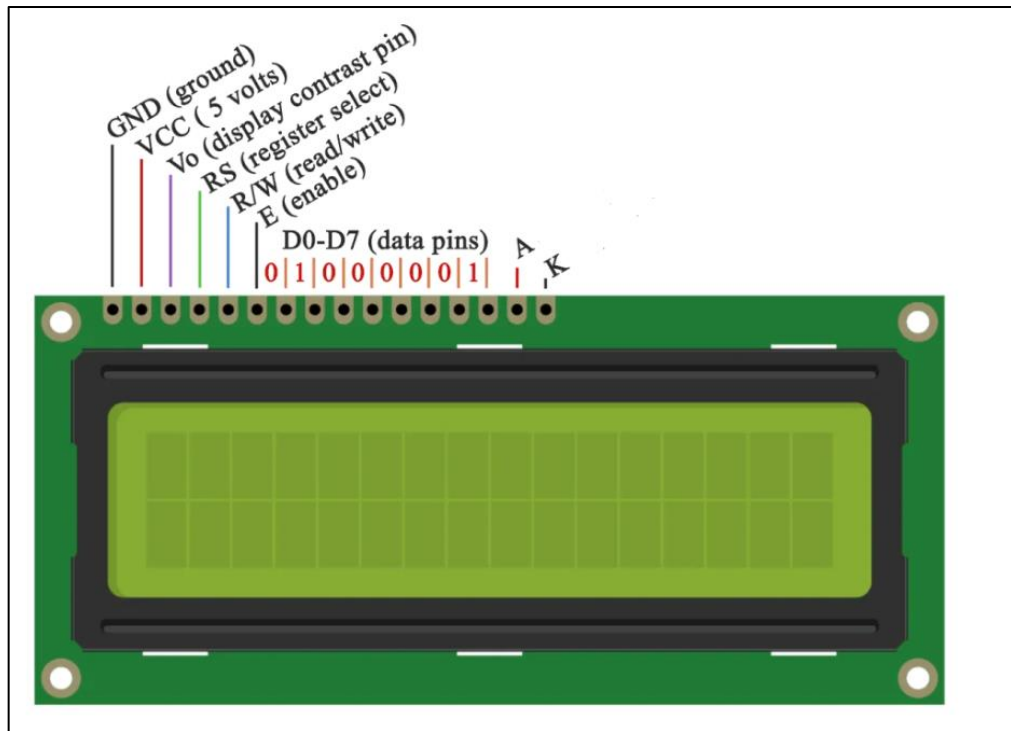


Рисунок 2.4 - Розпіновка РК дисплею

Далі, контакт RS або контакт вибору регістра використовується для вибору того, чи будемо ми надсилати команди чи дані на РК-дисплей. Наприклад, якщо контакт RS налаштований на низький стан або нуль вольт, тоді ми надсилаємо команди на РК-дисплей, наприклад: встановити курсор у певне місце, очистити дисплей, вимкнути дисплей тощо. І коли контакт RS встановлено на високий стан або 5 вольт, ми надсилаємо дані або символи на РК-дисплей.

Кожна шина I2C і двох сигналів: SCL і SDA. SCL – це тактовий сигнал, а SDA – сигнал даних. Тактовий сигнал генерується поточним майстром шини; деякі керовані пристрої можуть час від часу переводити годинник на низький рівень, щоб затримати відправку майстром додаткових даних (або вимагати більше часу для підготовки даних, перш ніж майстер спробує їх синхронізувати).

Схема підключення РК дисплею показана на рисунку 2.5.

Зм.	Арк.	№докум.	Підпис	Дата

2.5 Підключення Електромагнітного дверного замка 12V

На даному етапі я буду підключати електромагнітний дверний замок 12V, який зображений на рисунку 2.6

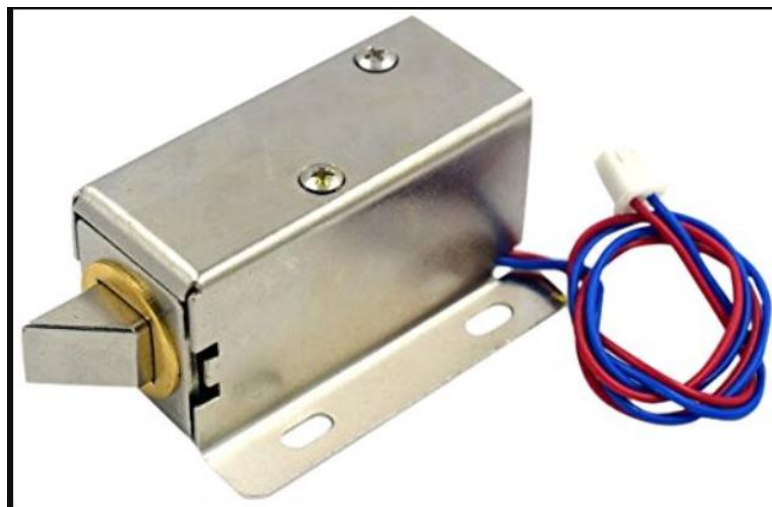


Рисунок 2.6 - Електромагнітний дверний замок

Дверний замок насправді є застібкою, яка відкривається або світиться за допомогою електромагнітного соленоїда. Як правило, спеціальне кріплення дверного замка, ймовірно, буде дорівнювати традиційній моделі, яка керується ключем.

Велика різниця між обома полягала б у тому, що додавання соленоїда від механіки, і це повертає засув у під'їзді, якщо спрацьовує альтернативне керування або кнопка.

Ручка буде триматися від дверей до тих пір, поки перемикач був натиснутий, або навіть у випадку соленоїда, поки не буде спрацьовано управління або кнопка. Всі ці форми дверних замків використовувалися всередині приміщень і для охоронного доступу.

Працює цей замок наступним чином:

Коли на електромагніт подається живлення, струм, який проходить через електромагніт, створює магнітний потік, який змушує пластину якоря притягнутися до електромагніту- це блокуюча дія.

Коли на електромагніт НЕ подається напруга, магнітний потік відсутній і пластина якоря не притягується до електромагніту- це відкриваюча дія.

Зм.	Арк.	№докум.	Підпис	Дата

Схема під'єднання електромагнітного замка до Arduino показана на рисунку

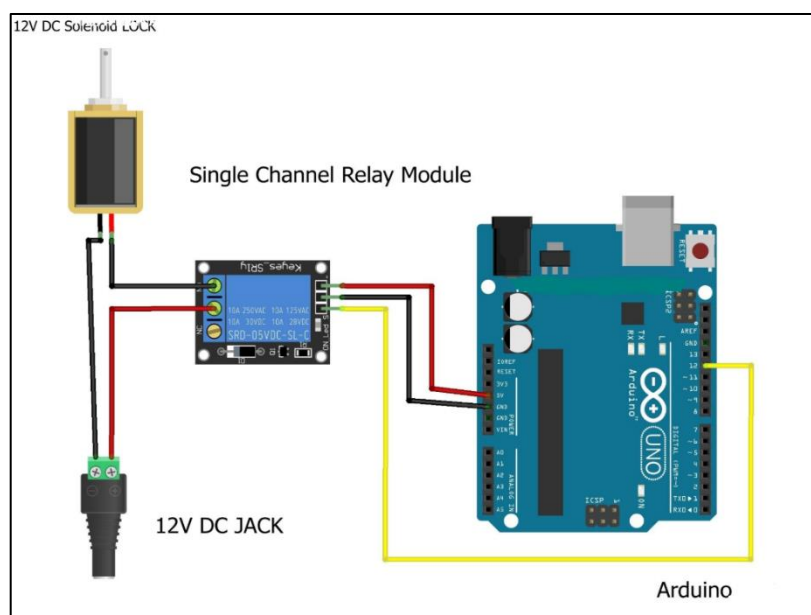


Рисунок 2.7- Схема під'єднання Електромагнітного замка до Arduino

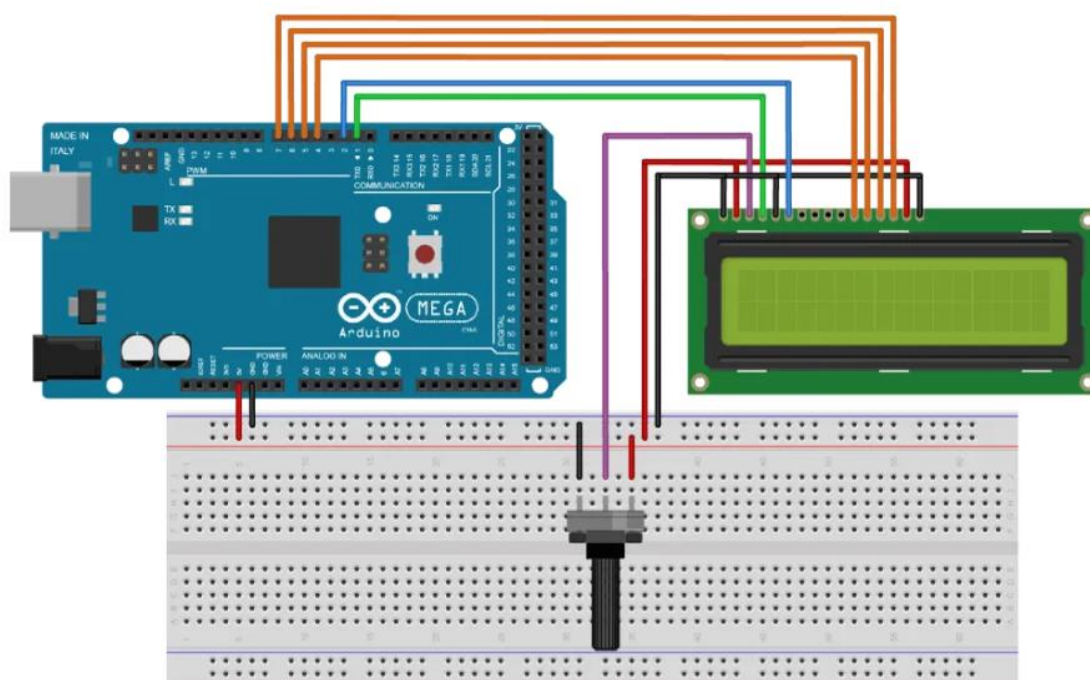


Рисунок 2.5- Схема підключення РКД

Ми можемо настроїти контрастність РК-дисплея, регулюючи вхідну напругу на виводі Vo . Ми використовуємо потенціометр, тому що ми можемо легко налаштувати контрастність, регулюючи вхідну напругу від 0 до 5 В.

Зм.	Арк.	№докум.	Підпис	Дата

Ми також можемо використовувати РК дисплей без потенціометра. Якщо ми не маємо потенціометра, ми все одно можемо відрегулювати контраст РК-дисплея за допомогою дільника напруги, що складається з двох резисторів. За допомогою дільника напруги нам потрібно встановити значення напруги між 0 та 5В, щоб отримати хороший контраст на дисплеї. Я виявив, що напруга близько 1 В чудово підходить для мого РК-дисплея. Я використовував резистор 1К та 220 Ом, щоб отримати хороший контраст.

Ми розглянули майже все, що нам потрібно знати про використання РК-дисплею Arduino. Ці РК-дисплеї дуже зручні для відображення інформації для багатьох проектів електроніки. У наведених вище прикладах я використав РК-дисплей 16×2, але той же принцип роботи можна застосувати і для будь-якого іншого розміру цих символних дисплеїв.

2.6 Під'єднання GSM модуля

Модуль GPRS A6, який ми можемо бачити на рисунку 2.8 - це в основному GSM-модем, підключений до друкованої плати з різними типами виходу, взятого з плати - скажімо, вихід TTL (для Arduino, 8051 та інших мікроконтролерів) і вихід RS232 для безпосереднього взаємодії з ПК (персональний). комп'ютер). На платі також будуть штирі або пристосування для кріплення мікрофона та динаміка, для виведення +5 В або інших значень живлення та з'єднань заземлення. Ці типи положень відрізняються в різних модулях.

На ринку доступно багато різновидів GSM-модемів і GSM-модулів. Для нашого проекту підключення gsm-модему або модуля до Arduino і, отже, надсилання та отримання SMS за допомогою Arduino – завжди добре вибрати сумісний з Arduino GSM-модуль – це модуль GSM з положеннями TTL-виходу.

Характеристики: - Робоча частота: чотиридіапазонна мережа, 850/900/1800 / 1900 МГц- Робоча напруга: 4,8-9 В постійного струму (живлення ланцюга вбудованого регулятора напруги для модуля A6) - Робочий струм: максимум 2 А- Струм сну: 5 мА - Вбудований утримувач Micro SIM-картки, ви можете встановити

Micro SIM-карту - Вбудований інтерфейс Micro USB для зовнішнього джерела живлення - Інтерфейс зв'язку: послідовний порт TTL / послідовний порт RS232 - Швидкість передачі даних: 115200 біт/с, а також може бути встановлена командою AT. - Інтерфейс логічна напруга: 3,3 В- Здійснюйте та відповідайте на телефонні дзвінки за допомогою гарнітури та електретного мікрофона.- Відправляйте та отримайте SMS-повідомлення.- Відправляйте та отримайте дані GPRS (TCP / IP, HTTP тощо) .- Використовуйте для тестування Ai- Модуль Thinker GPRS A6- Крок контактів: 2,54 мм- Інтерфейс вбудованої антени: SMA та IPX Якщо ви підключите це до arduino або для AT-команд, вам знадобиться лише 4 дроти. Я вирішив використати чотири різнокольорові дроти для легкого розуміння. Перше вставте картку micro-SIM в модуль A6

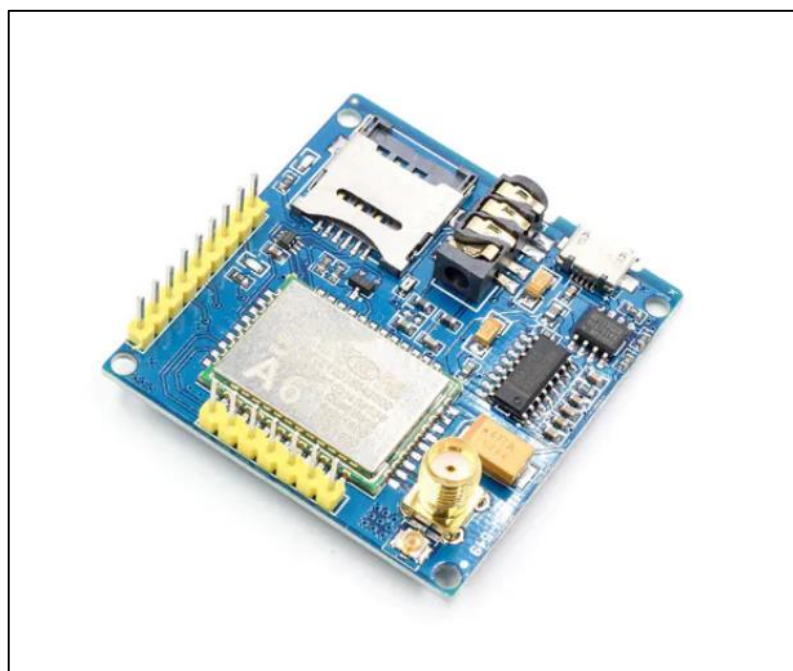


Рисунок 2.8 - GPRS-модуль A6

Завантаження GSM-модуля

1. Вставити SIM-карту в модуль GSM та заблокувати її.
2. Підключити адаптер до GSM модуля та увімкнути його!
3. Тепер потрібно зачекати деякий час (скажімо, 1 хвилину) і подивитися, як мигає «індикатор стану» або «індикатор мережі» (модулю GSM знадобиться деякий час, щоб встановити з'єднання з мобільною мережею)

Зм.	Арк.	№докум.	Підпис	Дата

4. Після успішного встановлення з'єднання індикатор стану/мережі буде блимати безперервно кожні 3 секунди. Ми можете спробувати зателефонувати на мобільний номер SIM-карти всередині GSM-модуля. Якщо ви чуєте зворотний дзвінок, модуль gsm успішно встановив мережеве з'єднання.

Тепер потрібно під'єднати модуль до Arduino

Щоб уникнути труднощів, я використовую метод під'єднання, у якому два цифрових контакти Arduino використовуються для послідовного зв'язку. Нам потрібно вибрати два контакти Arduino з підтримкою ШІМ для цього методу. Тому я вибираю висновки 9 і 10 (які є контактами з підтримкою ШІМ). Цей метод став можливим завдяки SoftwareSerial Library Arduino. SoftwareSerial — це бібліотека Arduino, яка забезпечує послідовний обмін даними через інші цифрові контакти Arduino. Бібліотека реплікує апаратні функції та справляється із завданням послідовного зв'язку.

Нижче, на рисунку 2.9 наведена принципова схема для підключення модуля gsm до Arduino – і, отже, використання схеми для надсилання SMS та отримання SMS за допомогою Arduino та gsm-модему.

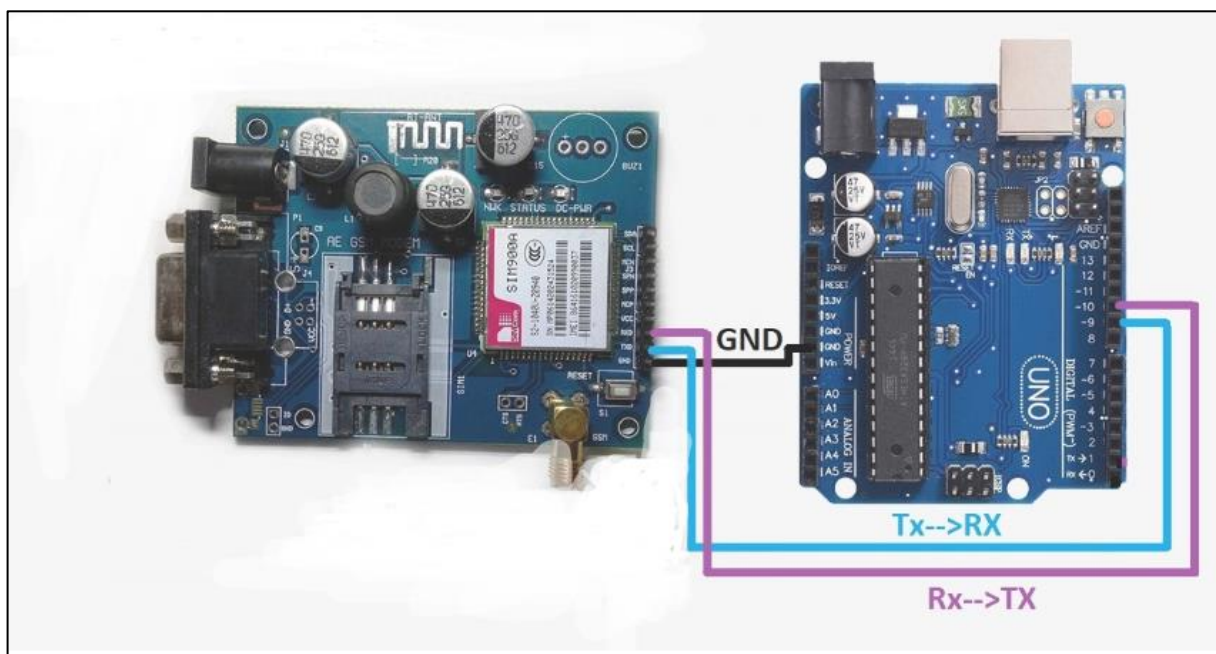


Рисунок 2.9 Схема з'єднання GSM-модуля з Arduino

Зм.	Арк.	№докум.	Підпис	Дата

2.7 Висновок

У другому розділі було детально розглянуто обрані моделі, які будуть використовуватися для конструювання дверного замкового механізму з датчиком відбитка пальця. Було розглянуто мету, ціль і принцип з'єднання, розглянуто будову кожного компоненту, який буде застосовуватися в наступному розділі.

Конкретно було розглянуто складання і під'єднання плат Arduino, під'єднання до них датчика відбитків пальців R307, РК дисплею, електромагнітного замка, GSM модуля для відправки СМС власнику замка у випадку. Коли хтось сторонній намагається відкрити замок.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						42
Зм.	Арк.	№докум.	Підпис	Дата		

3 ПРОГРАМНО-ТЕХНІЧНА РЕАЛІЗАЦІЯ ПРИСТРОЮ ДЛЯ КОНТРОЛЮ ДОСТУПУ В ПРИМІЩЕННЯ ЗА ВІДБИТКОМ ПАЛЬЦЯ

3.1 З'єднання необхідних компонентів

Для реалізації пристрою для контролю доступу в приміщення за відбитком пальця нам знадобиться:

- 1) модуль датчика оптичного зчитувача відбитків пальців R307 1шт;
- 2) мікроконтролер ATMEL ATmega328P 2шт;
- 3) РКД 12С 1шт;
- 4) мотор-редуктор постійного струму (DC 3 ~ 6 В) 2шт;
- 5) драйвер крокового двигуна L298N 1шт;
- 6) GA6-B міні GPRS GSM модуль A6 SMS голосовий модуль 5 В 1шт;
- 7) USB-послідовні перетворювачі з FTDI 2шт;
- 8) перемикач увімкнення/вимкнення акумулятора на 1 9 В;
- 9) тримач 1 батарейки типу AA / Корпус 4 камер;
- 10) 16 МГц - кварцеві генератори;
- 11) ртутні батареї на 9 В особливо важких умов 3шт;
- 12) керамічних конденсатора 104 (по 100 нФ кожен) 2шт;
- 13) керамічний конденсатор 220 (22 пФ) 1шт;
- 14) зумер 1шт;
- 15) макетні дошки 3шт;
- 16) Micro Sim 1шт;
- 17) світлодіоди;
- 18) батарейки типу AA 3шт;
- 19) дроти та перемички

Всі ці деталі можна придбати у спеціальних магазинах, або замовити в інтернеті.

З'єднуємо Arduino між собою. Процес показано на рисунку 3.1.

					КВРКІ 180230.18.02.07 ПЗ	Арк
Зм.	Арк.	№докум.	Підпис	Дата		43



Рисунок 3.1 - З'єднання Arduino між собою

На рисунку 3.2 зображено електричну схему Arduino Atmega328p.

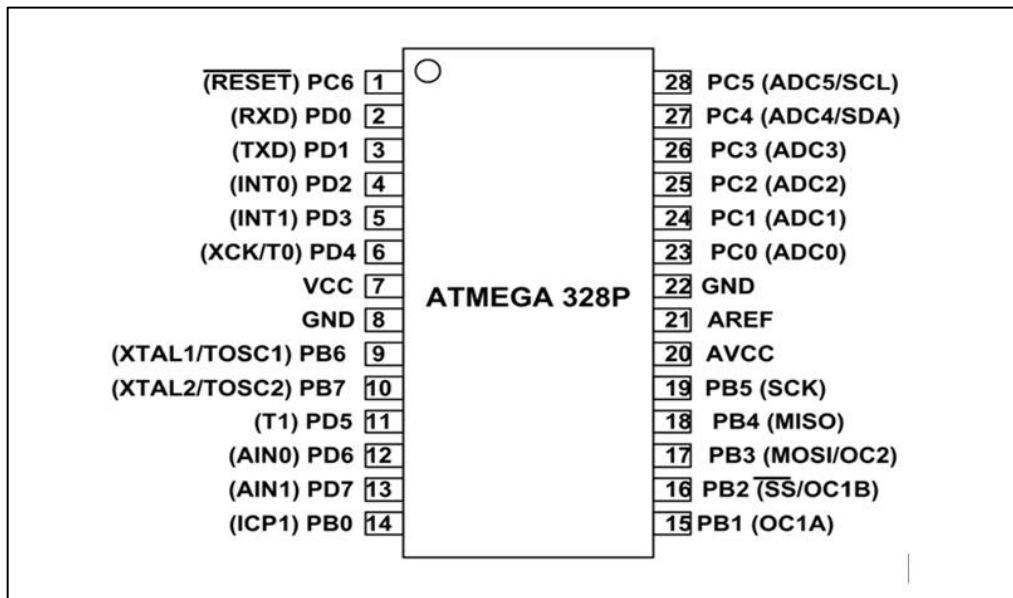


Рисунок 3.2 - Електрична схема Atmega328P

Схема з'єднання двох Arduino показана на рисунку 2.1

Схема підключення сенсора відбитків пальців до Arduino показана на рисунку 3.3.

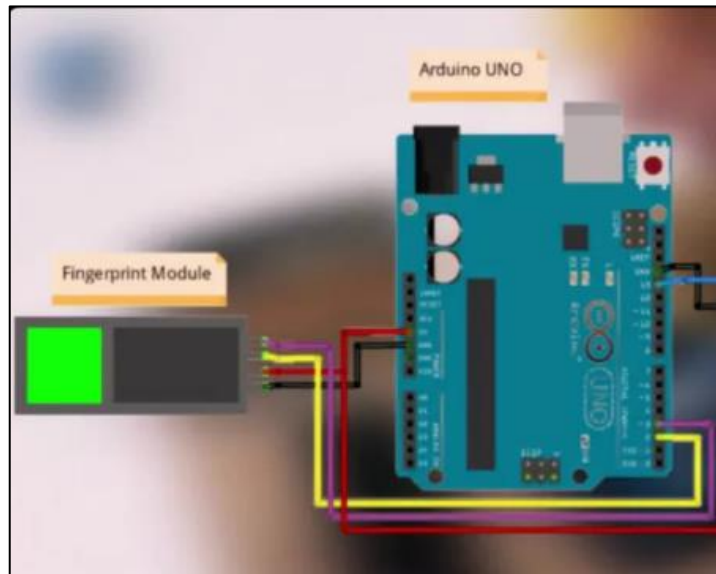


Рисунок 3.3- Схема підключення датчика відбитка пальця

Частина з'єднань дуже і дуже проста, цей датчик відбитків пальців має 6 проводів, з яких тільки 4 проводи корисні для інтерфейсу Arduino, з яких 2 проводи будуть використовуватися для живлення та 2 для даних.

Результат роботи показано на рисунку 3.4.

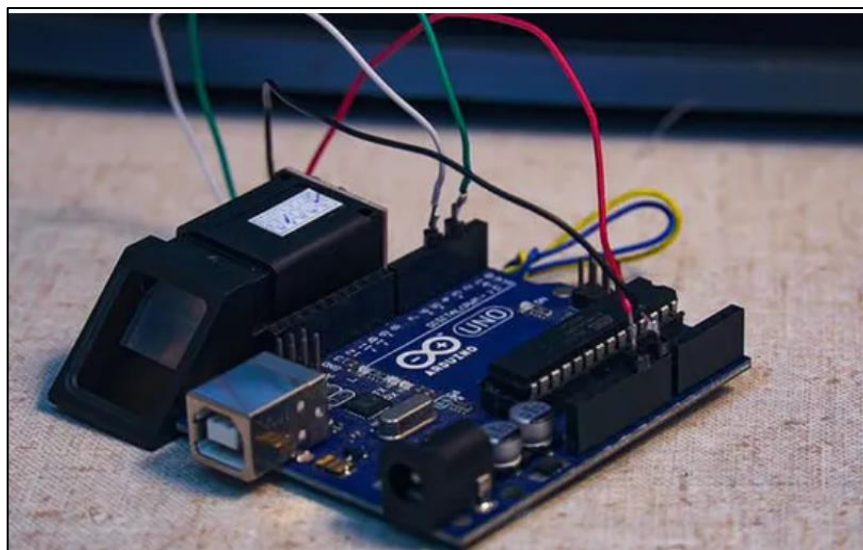


Рисунок 3.4 -Підключення сканера відбитків пальців

Зм.	Арк.	№докум.	Підпис	Дата

Для того, щоб сканер відбитків пальців у нас працював нам також знадобиться підключити бібліотеку Adafruit's Fingerprint в Arduino IDE

Спочатку нам потрібно зареєструвати відбитки пальців у EPROM нашого сенсорного модуля, тому я виконав наступні кроки, щоб зареєструвати свої відбитки пальців.

- Відкрив ардуїно IDE
- У меню ФАЙЛ та розділ Приклади потрібно знайти бібліотеку відбитків пальців Adafruit.
- Далі потрібно завантажити приклад реєстрації.
- Потрібно відкрити серійний монітор та вибрати швидкість передачі даних 9600
- Потрібно ввести ідентифікаційний номер, коли послідовний монітор запропонує ввести ідентифікаційний номер відбитка пальця.
- Прикласти палець, який потрібно зареєструвати, на датчик.
- Знову помістіть палець на датчик, як тільки з'явиться запит послідовного монітора.

Вас попросять двічі прикласти той самий палець до сканера. Якщо ви отримуєте повідомлення « Відбитки збігаються! », як показано нижче, ваш відбиток пальця успішно збережено. Якщо ні, повторюйте процес, поки не досягнете успіху.

Рисунок 3.5 демонструє реєстрацію відбитка пальця.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						47
Зм.	Арк.	№докум.	Підпис	Дата		

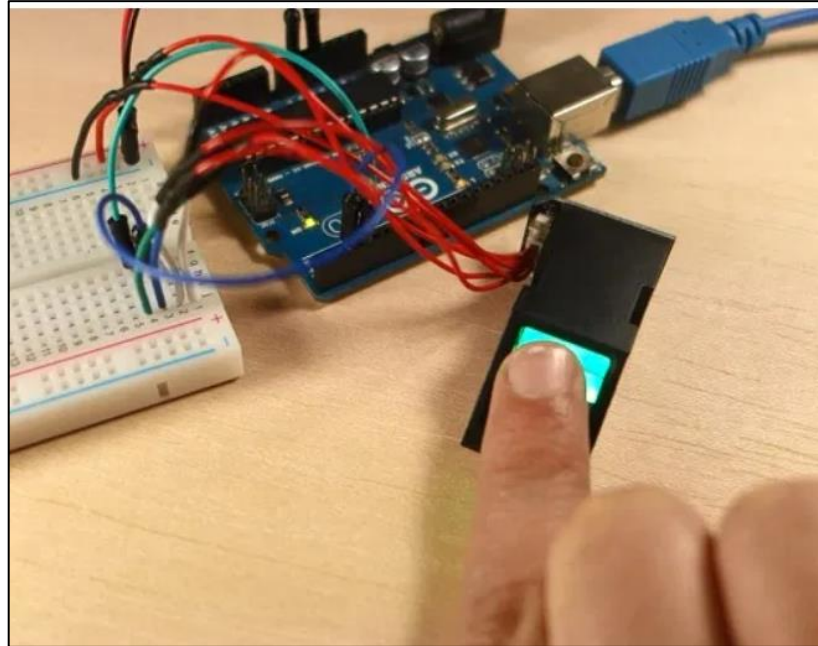


Рисунок 3.5 Реєстрація відбитка пальця

Модуль датчика відбитків пальців, використаний у цьому проекті, був оснащений дуже тонкими проводами, тому були потрібні дроти, зручні для паяння на макетній платі. Рекомендовано використовувати різні кольори, залежно від функції контакту. Це можна побачити на рисунку 3.6 . У моєму випадку:

- DNC - білі дроти
- VCC - червоний провід
- TX – синій провід
- RX - зелений провід
- Земля – чорний провід

Зм.	Арк.	№докум.	Підпис	Дата

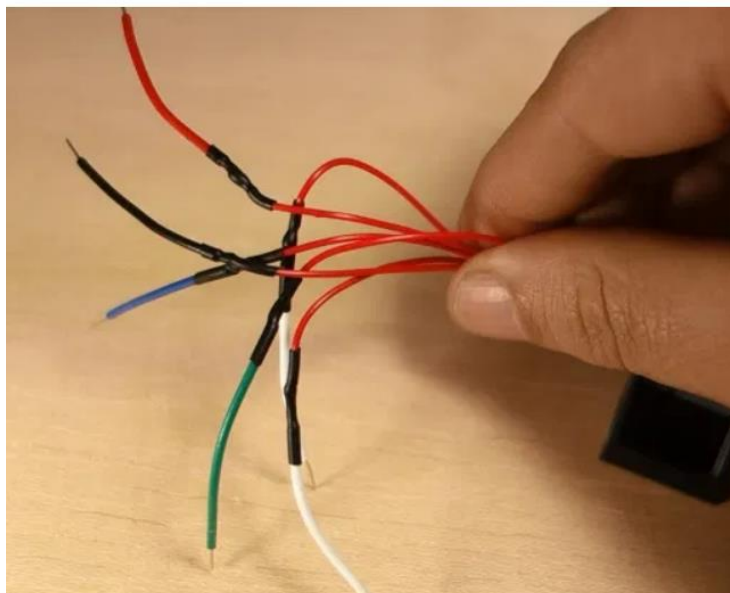


Рисунок 3.6 з'єднання проводів датчика відбитків пальців

3.3 Підключення РК дисплею

Далі підключаємо РК дисплей, так, як показано в таблиці 3.2

Таблиця 3.2 - Контакти з'єднання РКД і Arduino

РКД 12С	Arduino Atmega328P
GND	GND
VCC	5V
SDA	A4
SCL	A5

Для управління дверним замком знадобиться акумуляторне джерело від 7 до 12В – я використав три елементи 18650.

Схема підключення РКД зображена на рисунку 3.3

Зм.	Арк.	№докум.	Підпис	Дата

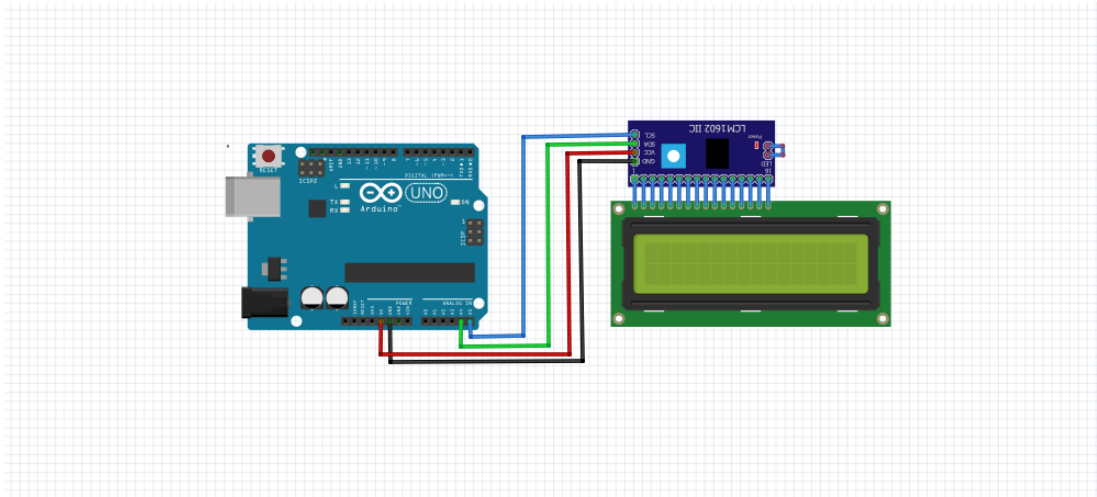


Рисунок 3.7 Схема підключення РК Дисплею

3.4 Підключення Електромагнітного дверного замка

Підключати електромагнітний замок слід так, як зазначено в таблиці 3.3

Таблиця 3.3 Контактні з'єднання під'єднання електромагнітного замка

Arduino Atmega328P	Одноканальний релейний модуль 5 В	
(+5V)	VCC	
GND	GND	
D12 Pin	IN1 input	
12V DC Adaptor	Електромагнітний замок	Одноканальний релейний модуль 5 В
		Normally Open
Positive		Common
	Positive Terminal	Normally Closed
Negative	Negative Terminal	

Потрібно підключити 5-вольтовий контакт Arduino до контакту VCC модуля реле.

З'єднати контакт GND Arduino з контактом GND модуля Relay.

Приєднати контакт Relay IN модуля Relay до контакту digital-12 Arduino, як показано вище.

Також потрібно підключити плюсовий провід джерела живлення постійного струму до іншого боку модуля реле, а мінусовий провід до електромагнітного замка, як показано.

З'єднати плюсовий провід електромагнітного замка з модулем реле. Тепер завантажити код на Arduino.

3.5 Підключення GSM-модуля

Це міні-версія серійної розробної плати GSM / GPRS на основі модуля GPRS A6. Він підтримує дводіапазонну мережу GSM/GPRS, доступну для дистанційної передачі даних GPRS та SMS.

Плата відрізняється компактними розмірами і низьким споживанням струму. Завдяки технології енергозбереження споживаний струм у сплячому режимі становить всього 3 мА.

Він зв'язується з мікроконтролером через порт UART, підтримує команди, включаючи GSM 07.07, GSM 07.05 і розширені AT-команди Ai-Thinker.

Технічні характеристики

Струм - 2 А (макс.)

Частота - 850 / 900 / 1800 / 1900 МГц

Довжина x ширина x висота - 22,8 мм x 16,8 мм x 2,2 мм

Робоча напруга - 4,5 В ~ 5,2 В

Швидкість даних GPRS, швидкість передачі даних Завантаження - 85,6 Кбіт/с, завантаження 42,8 Кбіт/с

Температурний діапазон - -30°C – +80°C

					КВРКІ 180230.18.02.07 ПЗ	Арк
Зм.	Арк.	№докум.	Підпис	Дата		51

Модуль А6 GA6-B GSM/GPRS — це мініатюрний GSM-модем, який можна інтегрувати у велику кількість IoT-проектів. Ви можете використовувати цей модуль, щоб виконати майже все, що може звичайний мобільний телефон; SMS-повідомлення, здійснювати та приймати телефонні дзвінки, підключатися до Інтернету через GPRS, TCP/IP тощо!

Крім того, модуль підтримує чотиридіапазонну мережу GSM/GPRS, що означає, що він працює практично в будь-якій точці світу.

Я підключив його до Arduino наступним чином: для початку підключив контакти U_TxD і U_RxD на модулі до цифрових контактів № 2 і № 4 на Arduino, оскільки ми будемо використовувати послідовне програмне забезпечення для спілкування з модулем. Слід підключити контакт VCC на модулі до контакту VCC 5 В на Arduino. Підключити контакт GND на модулі до контакту GND на Arduino. Нарешті, потрібно підключити антену, вставте повністю активовану картку Micro SIM в роз'єм. Контактні з'єднання можна побачити у таблиці 3.4.

Таблиця 3.4 Контактні з'єднання Arduino I GSP-модуля

Arduino	A6_mini GA6-B GSM
5V	VCC
GND	G
D2	U_TX
U4	U_RX

3.6 Збирання пристрою

Після завершення перевірки точності процесу ідентифікації були складені ретельні принципові схеми, які документували всі з'єднання початкового прототипу. Потім коробку розрізали, а всі компоненти закріпили всередині корпусу. Далі, використовуючи ці схеми, я переробив усі з'єднання, використовуючи мініатюрну макетну плату, прикріплену до основи коробки. Інтер'єр остаточного прототипу можна побачити на рисунку 3.8.



Рисунок 3.8- Складання всієї схеми в коробку-корпус

Щоб зробити систему ще більш зручною для користувачів, до кожного перемикача були додані ярлики, щоб чітко вказувати, хто має зареєструвати нового користувача, а який ідентифікувати користувача, З і Р відповідно. Остаточний прототип, який бачать користувачі, можна побачити на рисунку 3.9.



Рисунок 3.9- Остаточний вигляд прототипу

Зм.	Арк.	№докум.	Підпис	Дата

3.7 Схеми до пристрою та оцінка їх вартості

Загальна схема пристрою зображена на рисунку 3.10

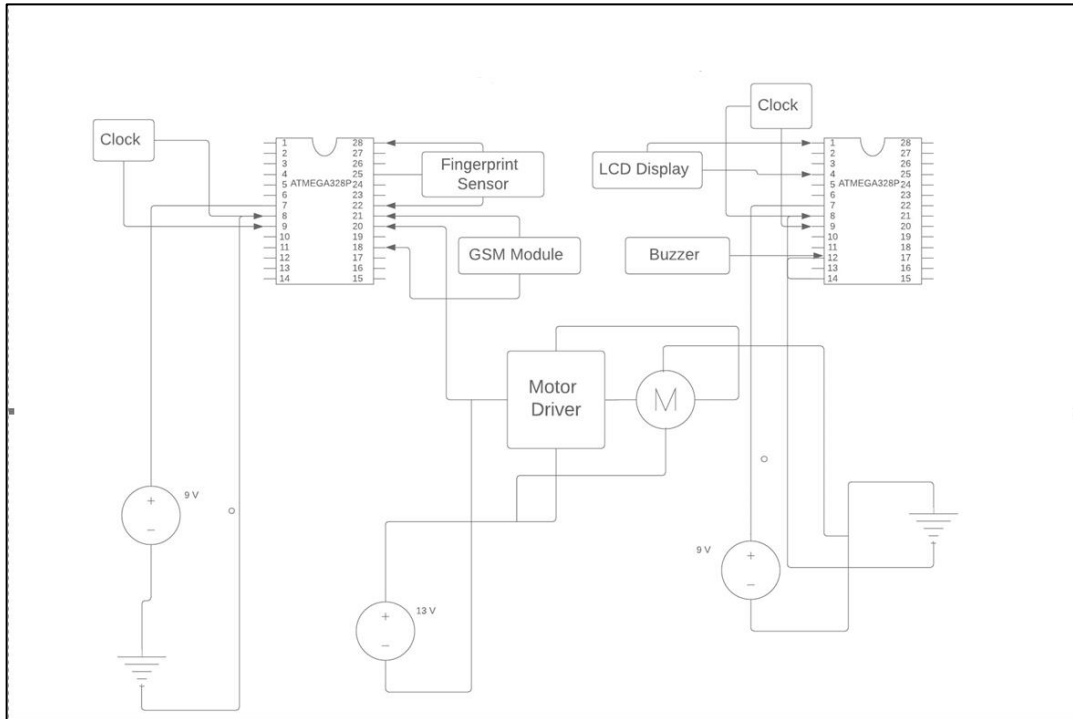


Рисунок 3.10- Загальна електрична схема пристрою

Зм.	Арк.	№докум.	Підпис	Дата

Блок схема роботи пристрою зображена на рисунку 3.11

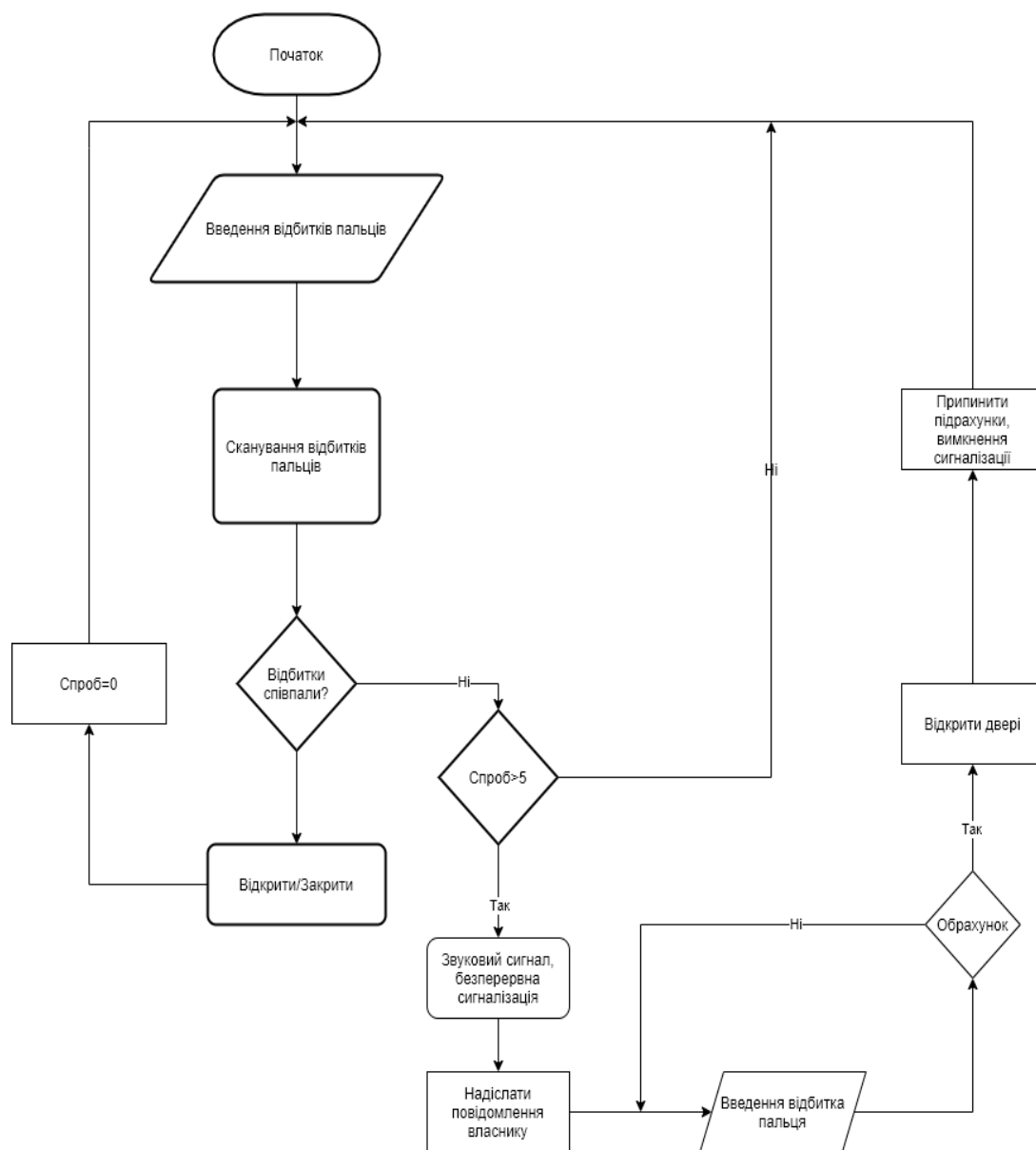


Рисунок 3.11- Блоксхема роботи пристрою

Повна вартість пристрою наведена в таблиці 3.5

Таблиця 3.5- Таблиця вартості пристрою

Назва	Модель	Кількість	Ціна (грн)	Вартість (грн)
1	2	3	4	5
Оптичний сканер відбитка пальця	R307	1	2300	2300
Плата	Arduino Atmega328P	2	297	594
Мотор редуктора	DC Gear Motors	2	196	392
Драйвер крокового двигуна	L298N	1	30	30
GPRS-Модуль	GA6-B mini	1	226	226
Перетворювач	RS485 TTL FTDI	2	155	310
Перемикач	Перемикач увімкнення/вимкнення корпусу тримача акумулятора 9 В	1	100	100
Тримач для батарейок типу AA	Корпус 4 камерний	1	100	100
Кристалічний генератор	16 МГц – кристалічні генератори	2	85	170

Зм.	Арк.	№докум.	Підпис	Дата

КВРКІ 180230.18.02.07 ПЗ

Арк

56

Кінець таблиці 3.5

1	2	3	4	5
Конденсатор	Керамічний конденсатор 104 (100 нФ кожен)	2	5	10
Конденсатор	Керамічний конденсатор 220	1	5	5
Зумер	Зумер	1	10	10
Макетні дошки	МВ-102	3	200	600
SIM-карта	Micro sim	1	66	66
Дисплей	РК-дисплей LCD 1602	1	113	113
Батарейки	Батарейки АА	3	9	27
Загальна вартість пристрою- 5053 грн				

3.8 Висновок

У даному розділі було продемонстровано реалізацію схеми і показано засоби підключення необхідних елементів розумного замка з відбитком пальця один до одного. Було реалізовано загальну макетну. Перед збиранням пристрою по контролю доступу в приміщення було куплено необхідні деталі і елементи конструкції проведено їх оцінка.

ВИСНОВКИ

У ході реалізації даного проекту було теоретично розглянуто основи досліджуваної проблеми, проведено аналіз предметної області і виявлення наявних проблем і завдань, здійснено порівняльний аналіз переваг та недоліків існуючих та відомих моделей і рішень, а також було знайдено різні методологічні підходи до вирішення задачі за темою дослідження.

Отже, було чітко визначено основні етапи для реалізації поставленої задачі з побудови розумного замка з сканером відбитків пальців, обрано найбільш підходящі методи для підключення необхідних компонентів одне до одного для сформування готового пристрою. Дане дослідження дозволить не допустити критичних недоліків у проекті та допоможе усунути їх, якщо вони виникнуть під час експлуатації розумного замка.

Попередні дослідження стали відправною точкою у конструюванні замка з сенсором відбитків пальців. І уже на наступному етапі було створено схему з'єднань компонентів дверного замка. Також моделювання підключення елементів, допомогло все зробити в майбутньому в реальному часі. Оцінка вартості всіх компонентів необхідних для конструювання смарт-замка допомогли довести те, що пристрій є не надто дорогим у реалізації.

					КВРКІ 180230.18.02.07 ПЗ	Арк
Зм.	Арк.	№докум.	Підпис	Дата		58

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Блог Allo URL: <https://blog.allo.ua/ua/rozumni-dverni-zamki-shho-tse-take-ta-yak-vibrati> (дата звернення: 13.03.22)
2. A. Jain and S. Pankanti, "Fingerprint Classification and Matching" Handbook for Image and Video Processing, A. Bovik (ed.), Academic Press, April 2013.
3. ACS Lock. URL: <https://www.acslocks.com/fingerprint-door-lock/> (дата звернення: 13.03.22)
4. Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology Special Issue on Image and Video Based Biometrics*, vol. 14, no. 1, 2018.
5. Anil K. Jain, Jianjiang Feng and Karthik Nandakumar, "Matching Fingerprints", *IEEE Computer*, vol. 43, no. 2, pp. 36-44, 2019.
6. Arduino Duemilanove;
<http://www.arduino.cc/en/Main/ArduinoBoardDuemilanove>
7. Carroll S., Kalaitzakis M., Vitzilaios N. UAS Sensor Deployment and Retrieval to the Underside of Structures. *In 2021 International Conference on Unmanned Aircraft Systems (ICUAS)*. 2021. Pp. 895-900.
8. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, "FVC2002: Fingerprint Verification Competition. Proceedings of International Conference on Pattern Recognition (ICPR)", pp. 744-747, August 2020.
9. D. Vinod kumar and M R K Murthy, "Fingerprint Based ATM Security by using ARM7" in IOSR Journal of Electronics and Communication Engineering(IOSRJECE), vol. 2, no. 5, pp. 26-28, October 2019.
10. Emartee. URL: <http://www.emartee.com/> (дата звернення 9.04.22)
11. Faisal I. A., Purboyo T. W., Ansori A. S. R. A Review of accelerometer sensor and gyroscope sensor in IMU sensors on motion capture. *J. Eng. Appl. Sci.* 2019. Pp. 826-829.

					КВРКІ 180230.18.02.07 ПЗ	Арк
Зм.	Арк.	№докум.	Підпис	Дата		59

12. Fernando L. Podio, "Personal authentication through biometric technologies", *Proceedings 2002 IEEE 4th International Workshop on Networked Appliances (Cat. No.02EX525) Gaithersburg*, pp. 57-66, 2015.
13. García J., Molina J. M., & Trincado J. Real evaluation for designing sensor fusion in UAV platforms. *Information Fusion*. 2020. Pp. 136-152.
14. Giernacki W., Horla D., Saska M. In-flight Efficient Controller Auto-tuning using a Pair of UAVs. In 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). 2020. Pp. 1300-1307.
15. Global Security; URL:<http://www.globalsecurity.org/security/systems/biometrics-history.htm> (дата звернення: 09.05.22).
16. GlobalSecurity; <http://www.globalsecurity.org/security/systems/biometrics-history.htm>, 2007.
17. Gunawan T. S., Yahya W. A., Sulaeman E., Kartiwi M., Janin Z. Development of control system for quadrotor unmanned aerial vehicle using LoRa wireless and GPS tracking. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2020. Pp. 2674-2681.
18. Hou A. S., Lin C. E. Uas Delivery Multi-Rotor Autopilot Based on ArduPilot Framework Using S-Bus Protocol. In 2021 Integrated Communication, *Navigation and Surveillance Conference (ICNS)*. 2022. Pp. 1-10.
19. K. Karu and A.K. Jain, "Fingerprint Classification", *Pattern Recognition*, Vol. 29, No. 3, pp. 389-404, 1996
20. Lourde R Mary and Khosla Dushyant, "Fingerprint Identification in Biometric Security Systems", *International Journal of Computer and Electrical Engineering*, vol. 2, no. 5, October 2020.
21. MAX232 Serial Level Converter; <http://sodoityourself.com/max232-serial-level-converter>
22. Mehta P., Gupta R., & Tanwar S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Computer Communications*. 2020. Pp. 518-538.

23. Mendoza-Mendoza J. A., Gonzalez-Villela V., Sepulveda-Cervantes G., Mendez-Martinez, M., Sossa-Azuela H. ArduPilot Working Environment. *In Advanced Robotic Vehicles Programming*. 2020. Pp. 19-46.

24. Nikhil N., Shreyas S. M., Vyshnavi G., Yadav, S. Unmanned aerial vehicles (UAV) in disaster management applications. *In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*. 2020. Pp. 140-148.

25. Nitgen: RS-232C serial protocol for Stand-Alone Fingerprint Recognition Device

26. Psilias D., Milidonis A., Voyiatzis I. Architecture for Secure UAV Systems. *In 24th Pan-Hellenic Conference on Informatics*. 2020. Pp. 99-102.

27. R. P. Wildes, "Iris recognition: an emerging biometric technology", *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348-1363, September, 2017.

28. R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, and A.W. Senior, Guide to Biometrics. Springer Science+Business Media, LLC. 2016, New York..

29. Raffaele Cappelli, Alessandra Lumini, Dario Maio and Davide Maltoni, "Fingerprint Image Reconstruction from Standard Templates", *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489-1503, September 2007.

30. Ross J. Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems" in , New York, NY, USA:John Wiley & Sons, 2016.

31. RS-232 Signals and RS232 voltage levels; http://www.radioelectronics.com/info/telecommunications_networks/rs232/signals-voltages-levels.php

32. Sparkfun Electronics; <http://www.sparkfun.com/> Indra W. A., Industrial S. G. H., Zamzam N. S., bin Hassim Fakulti N., Zuska F. Development of A Guided Drone Powered by Radio Frequency Energy Harvesting. *In 2021 IEEE International Conference in Power Engineering Application (ICPEA)*. 2021. Pp. 127-131.

33. Sparkfun Tutorials; <http://www.sparkfun.com/tutorials/104>

34. The Keyless Lock Store; <http://www.nokey.com/biomaccon.html>, 2015.

35. Union College Human Subjects Review Committee;.

					КВРКІ 180230.18.02.07 ПЗ	Арк
						61
Зм.	Арк.	№докум.	Підпис	Дата		

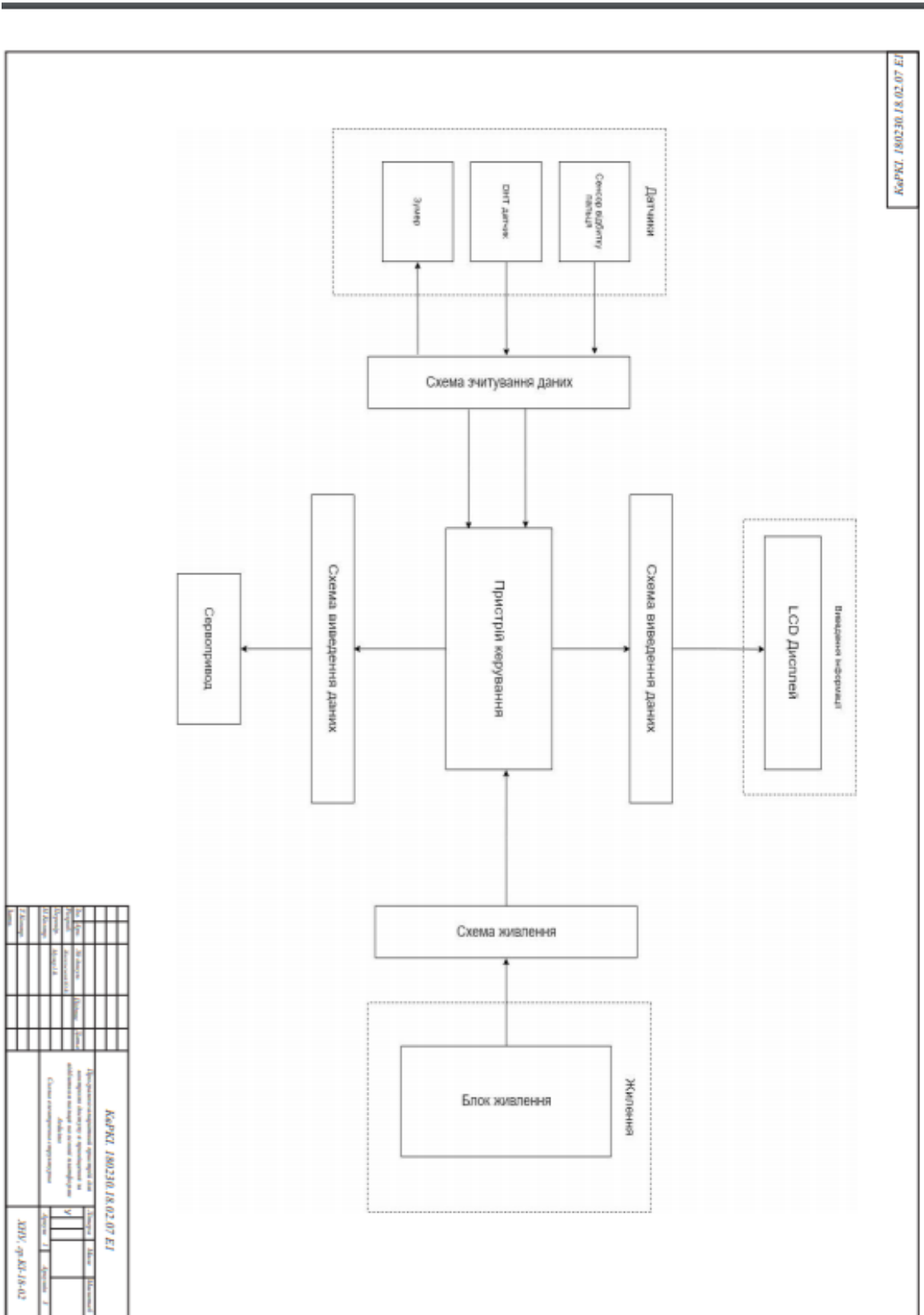
36. Yoon K., Park D., Yim Y., Kim K., Yang S. K., Robinson M. Security Authentication System Using Encrypted Channel on UAV Network. *First IEEE International Conference on Robotic Computing (IRC)*. 2017. Pp. 393-398.

37. Yu-Chih Huang, "Secure Access Control Scheme of RFID System Application", *Fifth International Conference on Information Assurance and Security*, 2018.

38. Zevdin Pala and Nihat Inanc, "Smart Parking Applications Using RFID Technology", *1st Annual RFID Eurasia Istanbul*, pp. 1-3, 2013.

					КВРКІ 180230.18.02.07 ПЗ	Арк
Зм.	Арк.	№докум.	Підпис	Дата		62

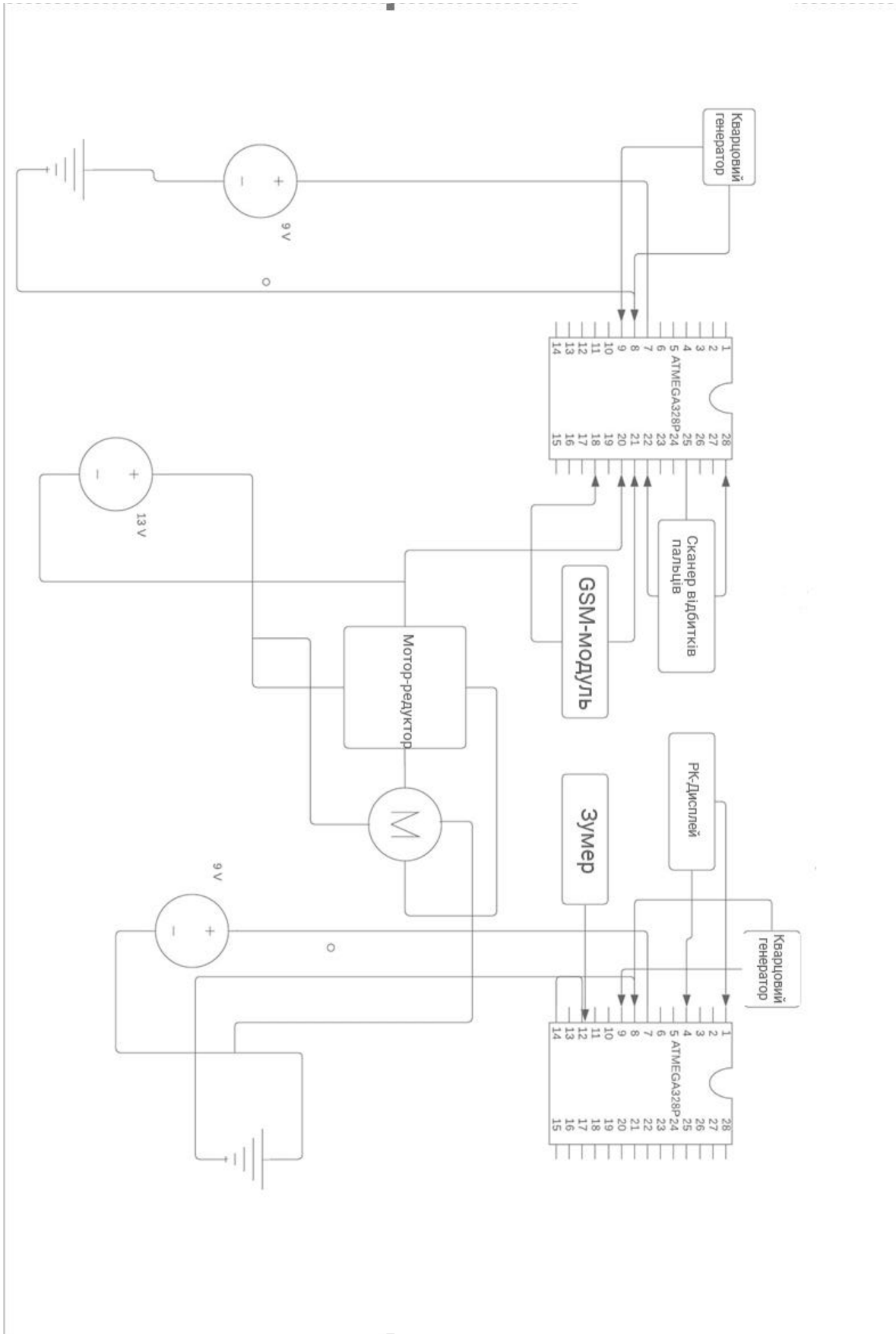
Додаток А
(обов'язковий)
Копія креслення «Схема електрична структурна»



КЕР.К.180230.18.02.07.E1		Керівник проектування	М.П.	М.П.
№ документа	Змін	Дата	Відомості	Відомості
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				
35				
36				
37				
38				
39				
40				
41				
42				
43				
44				
45				
46				
47				
48				
49				
50				
51				
52				
53				
54				
55				
56				
57				
58				
59				
60				
61				
62				
63				
64				
65				
66				
67				
68				
69				
70				
71				
72				
73				
74				
75				
76				
77				
78				
79				
80				
81				
82				
83				
84				
85				
86				
87				
88				
89				
90				
91				
92				
93				
94				
95				
96				
97				
98				
99				
100				

Додаток Б
(обов'язковий)

Копія креслення «Схема електрична Функційна»



Додаток Д

Лістинг коду для керування безпілотним апаратом

```
#include "dht.h"
#define dht_apin 2 // Analog Pin sensor is connected to
dht DHT;
#include<LiquidCrystal.h>
LiquidCrystal lcd(13,12,6,7,9,8);
#include <SoftwareSerial.h>
SoftwareSerial fingerPrint(10, 11);
#include<Servo.h>
Servo myServo;

#include <Adafruit_Fingerprint.h>
uint8_t id;
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&fingerPrint);
#define rabin A8
#define enroll A0
#define del A1
#define up A2
#define down A3
#define openLight 3
#define closeLight 4
#define servoPin 5

void setup()
{
  delay(1000);
  myServo.attach(servoPin);
  myServo.write(180);
  pinMode(enroll, INPUT_PULLUP);
  pinMode(up, INPUT_PULLUP);
  pinMode(down, INPUT_PULLUP);
  pinMode(del, INPUT_PULLUP);
  pinMode(rabin, INPUT_PULLUP);
  pinMode(openLight, OUTPUT);
  pinMode(closeLight, OUTPUT);
  lcd.begin(16,2);
  DHT.read11(dht_apin);

  lcd.setCursor(0,0);
  lcd.print(" MANMOHAN ");
  lcd.setCursor(0,1);
  lcd.print("POLYTECHNIC COLLAGE");
  lcd.scrollDisplayLeft();
  delay(1000);
  lcd.scrollDisplayLeft();
  delay(1000);
```

```

lcd.scrollDisplayLeft();
delay(1000);
lcd.scrollDisplayLeft();
delay(5000);
lcd.clear();
finger.begin(57600);
Serial.begin(9600);
lcd.clear();
lcd.print(" Finding Module ");
lcd.setCursor(0,1);
delay(2000);
if (finger.verifyPassword())
{
  Serial.println("Found fingerprint sensor!");
  lcd.clear();
  lcd.print(" Module Found ");
  delay(2000);
}
else
{
  Serial.println("Did not find fingerprint sensor :(");
  lcd.clear();
  lcd.print("Module Not Found");
  lcd.setCursor(0,1);
  lcd.print("Check Connections");
  while (1);
}
}

void loop()
{
  lcd.setCursor(0,0);
  lcd.print("HUMI =");
  lcd.print(DHT.humidity);
  lcd.print("% ");
  lcd.setCursor(0,1);
  lcd.print("TEMP =");
  lcd.print( DHT.temperature);
  lcd.println("C ");
  delay(5000);
  lcd.clear();
  lcd.setCursor(0,0);
  lcd.print(" Press Match ");
  lcd.setCursor(0,1);
  lcd.print("To Start System");
  digitalWrite(closeLight, HIGH);
  if(digitalRead(up)==0 || digitalRead(down)==0)
  {

```

```

for(int i=0;i<5;i++) { lcd.clear(); lcd.print("Place Finger"); delay(2000); int result=getFingerprintIDez();
if(result>=0)
{
digitalWrite(openLight, HIGH);
digitalWrite(closeLight, LOW);
lcd.clear();
lcd.print(" Allowed ");
lcd.setCursor(0,1);
lcd.print(" Gate Opened ");
myServo.write(0);
delay(5000);
myServo.write(180);
digitalWrite(closeLight, HIGH);
digitalWrite(openLight, LOW);
lcd.setCursor(0,1);
lcd.print(" Gate Closed ");
return;
}
}
}
checkKeys();
delay(2000);
if( currentposition==0 && digitalRead(rabin) == 0)
{
displayscreen();

}
int l ;
char code=keypad.getKey();
if(code!=NO_KEY)
{
lcd.clear();
lcd.setCursor(0,0);
lcd.print("PASSWORD:");
lcd.setCursor(7,1);
lcd.print(" ");
lcd.setCursor(7,1);
for(l=0;l<=currentposition;++l)
{

lcd.print("*");
keypress();
}

if (code==password[currentposition])
{
++currentposition;
if(currentposition==4)
{

```

```

unlockdoor();
currentposition=0;

}

}

else
{
++invalidcount;
incorrect();
currentposition=0;

}
if(invalidcount==5)
{

++invalidcount;
torture1();

}
if(invalidcount==8)
{
torture2();
}
}

void checkKeys()
{
if(digitalRead(enroll) == 0)
{
lcd.clear();
lcd.print("Please Wait");
delay(2000);
while(digitalRead(enroll) == 0);
Enroll();
}

else if(digitalRead(del) == 0)
{
lcd.clear();
lcd.print("Please Wait");
delay(2000);
delet();
}
}

void Enroll()

```

```

{
  int count=0;
  lcd.clear();
  lcd.print("Enroll Finger ");
  lcd.setCursor(0,1);
  lcd.print("Location:");
  while(1)
  {
    lcd.setCursor(9,1);
    lcd.print(count);
    if(digitalRead(up) == 0)
    {
      count++;
      if(count>25)
      count=0;
      delay(500);
    }

    else if(digitalRead(down) == 0)
    {
      count--;
      if(count<0) count=25; delay(500); } else if(digitalRead(del) == 0) { id=count; getFingerprintEnroll();
return; } else if(digitalRead(enroll) == 0) { return; } } void delet() { int count=0; lcd.clear();
lcd.print("Delete Finger "); lcd.setCursor(0,1); lcd.print("Location:"); while(1) { lcd.setCursor(9,1);
lcd.print(count); if(digitalRead(up) == 0) { count++; if(count>25)
  count=0;
  delay(500);
}

else if(digitalRead(down) == 0)
{
  count--;
  if(count<0)
  count=25;
  delay(500);
}
else if(digitalRead(del) == 0)
{
  id=count;
  deleteFingerprint(id);
  return;
}

else if(digitalRead(enroll) == 0)
{
  return;
}
}
}

```

```

uint8_t getFingerprintEnroll()
{
  int p = -1;
  lcd.clear();
  lcd.print("Finger ID:");
  lcd.print(id);
  lcd.setCursor(0,1);
  lcd.print("Place Finger");
  delay(2000);
  while (p != FINGERPRINT_OK)
  {
    p = finger.getImage();
    switch (p)
    {
      case FINGERPRINT_OK:
        Serial.println("Image taken");
        lcd.clear();
        lcd.print("Image taken");
        break;
      case FINGERPRINT_NOFINGER:
        Serial.println("No Finger");
        lcd.clear();
        lcd.print("No Finger");
        break;
      case FINGERPRINT_PACKETRECEIVEERR:
        Serial.println("Communication error");
        lcd.clear();
        lcd.print("Comm Error");
        break;
      case FINGERPRINT_IMAGEFAIL:
        Serial.println("Imaging error");
        lcd.clear();
        lcd.print("Imaging Error");
        break;
      default:
        Serial.println("Unknown error");
        lcd.clear();
        lcd.print("Unknown Error");
        break;
    }
  }

  // OK success!

  p = finger.image2Tz(1);
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image converted");

```

```

    lcd.clear();
    lcd.print("Image converted");
    break;
case FINGERPRINT_IMAGEMESS:
    Serial.println("Image too messy");
    lcd.clear();
    lcd.print("Image too messy");
    return p;
case FINGERPRINT_PACKETRECEIVEERR:
    Serial.println("Communication error");
    lcd.clear();
    lcd.print("Comm Error");
    return p;
case FINGERPRINT_FEATUREFAIL:
    Serial.println("Could not find fingerprint features");
    lcd.clear();
    lcd.print("Feature Not Found");
    return p;
case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Could not find fingerprint features");
    lcd.clear();
    lcd.print("Feature Not Found");
    return p;
default:
    Serial.println("Unknown error");
    lcd.clear();
    lcd.print("Unknown Error");
    return p;
}

```

```

Serial.println("Remove finger");
lcd.clear();
lcd.print(" Remove Finger ");
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
    p = finger.getImage();
}
Serial.print("ID "); Serial.println(id);
p = -1;
Serial.println("Place same finger again");
lcd.clear();
    lcd.print(" Place Finger ");
    lcd.setCursor(0,1);
    lcd.print(" 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;
}
}

// 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_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!
Serial.print("Creating model for #"); Serial.println(id);

p = finger.createModel();
if (p == FINGERPRINT_OK) {
    Serial.println("Prints matched!");
} else if (p == FINGERPRINT_PACKETRECEIVEERR) {
    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!");
    lcd.clear();
    lcd.print("Stored!");
    delay(2000);
} 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;
}
}

```

```

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

    if (p != FINGERPRINT_OK)
        return -1;

    p = finger.image2Tz();
    if (p != FINGERPRINT_OK)
        return -1;

    p = finger.fingerFastSearch();
    if (p != FINGERPRINT_OK)
    {
        lcd.clear();
        lcd.print("Finger Not Found");
        lcd.setCursor(0,1);
    }
}

```

```

    lcd.print("Try Later");
    delay(2000);
    return -1;
}
// found a match!
Serial.print("Found ID #");
Serial.print(finger.fingerID);
return finger.fingerID;
}

uint8_t deleteFingerprint(uint8_t id)
{
    uint8_t p = -1;
    lcd.clear();
    lcd.print("Please wait");
    p = finger.deleteModel(id);
    if (p == FINGERPRINT_OK)
    {
        Serial.println("Deleted!");
        lcd.clear();
        lcd.print("Figer Deleted");
        lcd.setCursor(0,1);
        lcd.print("Successfully");
        delay(2000);
    }

    else
    {
        Serial.print("Something Wrong");
        lcd.clear();
        lcd.print("Something Wrong");
        lcd.setCursor(0,1);
        lcd.print("Try Again Later");
        delay(2000);
        return p;
    }
}

void unlockdoor()
{
    delay(900);

    lcd.setCursor(0,0);
    lcd.println(" ");
    lcd.setCursor(1,0);
    lcd.print("Access Granted");
    lcd.setCursor(4,1);
    lcd.println("WELCOME!!");
    lcd.setCursor(15,1);
    lcd.println(" ");
}

```

```

lcd.setCursor(16,1);
lcd.println(" ");
lcd.setCursor(14,1);
lcd.println(" ");
lcd.setCursor(13,1);
lcd.println(" ");
unlockbuzz();

for(pos = 180; pos>=0; pos-=5) // goes from 180 degrees to 0 degrees
{
myservo.write(pos); // tell servo to go to position in variable 'pos'
delay(5); // waits 15ms for the servo to reach the position
}
delay(2000);

delay(1000);
counterbeep();

delay(1000);

for(pos = 0; pos <= 180; pos +=5) // goes from 0 degrees to 180 degrees
{ // in steps of 1 degree
myservo.write(pos); // tell servo to go to position in variable 'pos'
delay(15);

int currentposition=0;

lcd.clear();
displayscreen();

}
}

//*****WRONG CODE
FUNCTION*****//

void incorrect()
{
delay(500);
lcd.clear();
lcd.setCursor(1,0);
lcd.print("CODE");
lcd.setCursor(6,0);
lcd.print("INCORRECT");
lcd.setCursor(15,1);
lcd.println(" ");

```

```

lcd.setCursor(4,1);
lcd.println("GET AWAY!!!");

lcd.setCursor(13,1);
lcd.println(" ");
Serial.println("CODE INCORRECT YOU ARE UNAUTHORIZED");
digitalWrite(redled, HIGH);
digitalWrite(buzz, HIGH);
delay(3000);
lcd.clear();
digitalWrite(redled, LOW);
digitalWrite(buzz,LOW);
displayscreen();
}
//***** CLEAR THE SCREEN!!!*****//
void clearscren()
{
lcd.setCursor(0,0);
lcd.println(" ");
lcd.setCursor(0,1);
lcd.println(" ");
lcd.setCursor(0,2);
lcd.println(" ");
lcd.setCursor(0,3);
lcd.println(" ");
}
//*****KEYPRESS*****//
void keypress()
{

digitalWrite(buzz, HIGH);
delay(50);
digitalWrite(buzz, LOW);
}
//*****DISPALAY
FUNCTION!!!*****//
void displayscreen()
{

lcd.setCursor(0,0);
lcd.println("*ENTER THE CODE*");
lcd.setCursor(1 ,1);

lcd.println("TO _/_ (OPEN)!!");
}

```

```

//***** ARM
SERVO*****/
/
void armservo()
{

for (pos=180;pos<=180;pos+=50)
{
myservo.write(pos);
delay(5);
}
delay(5000);

for(pos=180;pos>=0;pos-=50)
{
myservo.write(pos);
}

}
//*****UNLOCK BUZZ*****//
void unlockbuzz()
{

digitalWrite(buzz, HIGH);
delay(80);
digitalWrite(buzz, LOW);
delay(80);
digitalWrite(buzz, HIGH);
delay(80);
digitalWrite(buzz, LOW);
delay(200);
digitalWrite(buzz, HIGH);
delay(80);
digitalWrite(buzz, LOW);
delay(80);
digitalWrite(buzz, HIGH);
delay(80);
digitalWrite(buzz, LOW);
delay(80);
}

//*****COUNTER
BEEP*****//
void counterbeep()
{
delay(1200);

lcd.clear();

```

```

digitalWrite(buzz, HIGH);

lcd.setCursor(2,15);
lcd.println(" ");
lcd.setCursor(2,14);
lcd.println(" ");
lcd.setCursor(2,0);
delay(200);
lcd.println("GET IN WITHIN::");

lcd.setCursor(4,1);
lcd.print("5");
delay(200);
lcd.clear();
lcd.setCursor(2,0);
lcd.println("GET IN WITHIN:");
digitalWrite(buzz,LOW);
delay(1000);
//2
digitalWrite(buzz, HIGH);
lcd.setCursor(2,0);
lcd.println("GET IN WITHIN:");
lcd.setCursor(4,1); //2
lcd.print("4");
delay(100);
lcd.clear();
lcd.setCursor(2,0);
lcd.println("GET IN WITHIN:");
digitalWrite(buzz,LOW);
delay(1000);
//3
digitalWrite(buzz, HIGH);
lcd.setCursor(2,0);
lcd.println("GET IN WITHIN:");
lcd.setCursor(4,1); //3
lcd.print("3");
delay(100);
lcd.clear();
lcd.setCursor(2,0);
lcd.println("GET IN WITHIN:");
digitalWrite(buzz,LOW);
delay(1000);
//4
digitalWrite(buzz, HIGH);
lcd.setCursor(2,0);
lcd.println("GET IN WITHIN:");
lcd.setCursor(4,1); //4
lcd.print("2");
delay(100);

```



```

//*****TORTURE1*****//
void torture1()
{
  delay(1000);
  lcd.clear();
  lcd.setCursor(2,0);
  lcd.print("WAIT FOR ");
  lcd.setCursor(5,1);
  lcd.print("15 SECONDS");
  digitalWrite(buzz, HIGH);
  delay(15000);
  digitalWrite(buzz, LOW);
  lcd.clear();
  lcd.setCursor(2,0);
  lcd.print("LOL..");
  lcd.setCursor(1,1);
  lcd.print(" HOW WAS THAT??");
  delay(3500);
  lcd.clear();

}
//*****TORTURE2*****//
void torture2()
{
  delay(1000);
  lcd.setCursor(1,0);
  lcd.print(" ");
  lcd.setCursor(2,0);
  lcd.print("EAR DRUMS ARE");
  lcd.setCursor(0,1);
  lcd.print(" PRECIOUS!! ");
  delay(1500);
  lcd.clear();
  lcd.setCursor(1,0);
  lcd.print(" WAIT FOR");
  lcd.setCursor(4,1);
  lcd.print(" 1 MINUTE");
  digitalWrite(buzz, HIGH);
  delay(55000);
  counterbeep();
  lcd.clear();
  digitalWrite(buzz, LOW);
  lcd.setCursor(2,0);
  lcd.print("WANT ME TO");
  lcd.setCursor(1,1);
  lcd.print("REDICULE MORE??");
  delay(2500);
  lcd.clear();
  lcd.setCursor(2,0);

```

```
lcd.print("Ha Ha Ha Ha");  
delay(1700);  
lcd.clear();  
}
```

Кодом. познач.	Найменування	Кільк.	Примітка
<u>Конденсатори</u>			
C4	K50-35-10 В – 47 мкФ +50-20 % ОЖО 463. 19 ТУ	1	
C3	K10-73-M47-100 пФ ±10% ОЖО 460. 043 ТУ	1	
<u>Мікросхеми</u>			
DD1	Atmega328P	2	мікроконтролер
<u>Модуль</u>			
DD4	GA6-B mini	1	GSM-модуль
<u>Світлодіод</u>			
HL1	АЛ307ГМ	1	
<u>Реле</u>			
DD6	L298N	2	
<u>Датчик відбитка пальця</u>			
BL1	R307	1	
<u>Кварцовий резонатор</u>			
Z1	104 (100 нФ)	2	
<u>Дисплей</u>			
DD5	LCD 1602	1	РКД

КвРКІ.180230.18.02.07 ПЕ

Арк.	№ докум.	Підпис	Дата
Розроб.	Жигальський	<i>[Signature]</i>	16.06.23
Перевір.	Муляр І.В.	<i>[Signature]</i>	16.06.23
Н.контр.	Мостовий С.В.	<i>[Signature]</i>	16.06.23
Затверд.	Кльоц Ю.П.	<i>[Signature]</i>	16.06.23

Програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino

Перелік елементів

Літера	Аркуш	Аркушів
У	1	3

ХНУ, КІ-18-2

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 2.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 10%**

ID: 105378 Название: Програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino Добавлено в БД: 2022-06-14 Авторы: Жигальський Юрій Вікторович Руководители: Муляр І.В. Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	60352	577	2447 (4%)	39 (7%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

Ім'я користувача:
Кафедра кібербезпеки

Дата перевірки:
14.06.2022 21:34:12 EEST

Дата звіту:
14.06.2022 21:37:33 EEST

ID перевірки:
1011581122

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100008300

Назва документа: Дипломна Жигальський Юрій

Кількість сторінок: 88 Кількість слів: 13283 Кількість символів: 107523 Розмір файлу: 7.28 MB ID файлу: 1011450669

19.4% Схожість

Найбільша схожість: 14.5% з Інтернет-джерелом (<https://electronicsworkshops.com/2020/09/12/fingerprint-door-based...>)

16.5% Джерела з Інтернету

2

Сторінка 90

2.93% Джерела з Бібліотеки

1

Сторінка 90

0.24% Цитат

Цитати

2

Сторінка 91

Не знайдено жодних посилань

6.04% Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 2%)

3.48% Вилучення з Інтернету

385

Сторінка 92

2.63% Вилученого тексту з Бібліотеки

172

Сторінка 95

Модифікації

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

Замінені символи

2

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ
КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА СИСТЕМНОГО ПРОГРАМУВАННЯ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino

Автор: Ю.В. Жигальський

Спеціальність: 123 – Комп'ютерна інженерія та програмування

Освітня програма: Комп'ютерна інженерія

Науковий керівник: І.В. Муляр, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

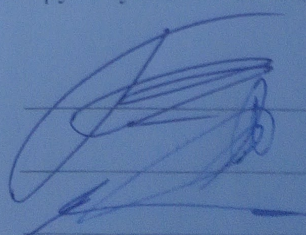
- 1) запозичення розміщені в розділах аналізу існуючих аналогів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
- 2) усі запозичення фрагментарні, або мають належним чином оформлені посилання;
- 3) окремі виявлені збіги є загальноживаними шаблонами, що використовуються при оформленні текстової документації, а саме шаблони рамок
- 4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту, використання абревіатур.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 19.4% і адресується до 3 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи

Гарант ОП

Завідувач кафедри КбКСМ



І.В. Муляр

С.М. Лисенко

Ю.П. Кльоц

РЕЦЕНЗІЯ НА ДИПЛОМНИЙ ПРОЕКТ

Дипломник Жигальський Юрій Вікторович

Тема Програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino

Спеціальність 123 Комп'ютерна інженерія

Обсяг дипломного проекту:

кількість листів креслень 4; кількість сторінок записки 86

1. Короткий зміст ДП та прийнятих рішень В рамках дипломного проекту програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino

2. Висновок про відповідність ДП дипломному завданню Дипломний проект у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині даного проекту.

3. Характеристика виконання кожного розділу проекту, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому, теоретичному, розділі дипломного проекту якісно та в повній мірі розглянуті методи вирішення поставленої задачі, розглянуто існуючі аналоги пристрою, виявлено їхні переваги і недоліки, був проаналізований кожен аспект, який стосується теми дипломного проекту. У наступному розділі було здійснено проектування з'єднання елементів між собою, детально розглянуто можливості з'єднань цих елементів. У основній проектній частині диплому було реалізована сучасними методами та рішеннями прибор, який надає доступ в приміщення шляхом зчитування біометричних даних. Спроектований пристрій дозволить задовольнити потреби споживачів, та допоможе захистити їх приміщення, будинки, офіси, тощо.

4. Позитивні сторони проекту Дипломний проект відповідає сучасним вимогам до проектування програмно-апаратних пристроїв та містить ряд рішень, що відповідають умовам сучасності. Побудований пристрій має хороший рівень захисту від незаконного проникнення в приміщення, та унаслідок повідомлення власнику, у випадку, коли хтось намагається проникнути без відома власника.

5. Негативні сторони проекту Громіздкий, займає багато місця.

6. Оцінка графічного оформлення та пояснювальної записки проекту Графічне оформлення виконане відповідно до суті дипломного проекту. На першому кресленні відображено електрично структурну схему, на другому кресленні відображено електрично функційну схему, на третьому кресленні відображено електричну структурну схему. В загальному графічне оформлення виконане на належному рівні. Пояснювальна записка відповідає задекларованим нормам для її оформлення.

7. Відгук про проект в цілому Дипломний проект вирішує поставлену задачу і детально описує її вирішення.

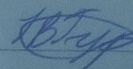
8. Інші зауваження

9. Оцінка дипломного проекту Розглянувши позитивні та негативні сторони представленого дипломного проекту, можна зробити висновок, що він заслуговує оцінку «добре».

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

Турчан Іван Васильович доцент кафедри інженерії програмного забезпечення

« 16 » червня 2022 р.



(підпис)