Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Швеця Валентина Руслановича

на здобуття ступеня вищої освіти Бакалавра

Біометричний термінал керування доступом в приміщення

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Комп'ютерна інженерія
Освітня програма Комп'ютерна інженерія

Шифр КРБКІ. 101007.21.01.08 ПЗ

Виконав студент 3 курсу група КІ1с-21-1 Валентин ШВЕЦЬ

Керівник канд. техн. наук, доцент Ігор МУЛЯР

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

15 06 2024 р.

Хмельницький, 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

Освітня програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Швецю Валентину Руслановичу

1 Тема роботи Біометричний термінал керування доступом в приміщення

Керівник роботи Муляр І.В.

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи завдання на кваліфікаційну роботу, специфікація мікроконтролера

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
дослідження предметної області та постановка задачі; обгрунтування базових положень щодо проектування пристрою контролю доступу; опис схем проектованої системи; опис алгоритму роботи системи

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Схема електрична структурна (Е1)», «Схема електрична функційа (Е2)»,

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

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	виконано
Ознайомлення з предметною областю	Лютий	виконано
Дослідження існуючих рішень	Лютий	виконано
Постановка задачі	Березень	виконано
Визначення загальних принципів рішення задачі	Березень	виконано
Деталізація принципів рішення задачі	Квітень	виконано
Розробка проєктних рішень	Квітень	виконано
Апробація проєктних рішень	Травень	виконано
Оформлення пояснювальної записки згідно вимог	Травень	виконано
Оформлення графічної частини	Червень	виконано
Захист КР	Червень	виконано

Студент Валентин ШВЕЦЬ

Керівник кваліфікаційної роботи Ігор МУЛЯР

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КРБКІ. 101007.21.01.08 ПЗ	Пояснювальна записка	65		
			Графічні матеріали			
2		КРБКІ. 101007.21.01.08 Е1	Схема електрична структурна	1		
3		КРБКІ. 101007.21.01.08 Е2	Схема електрична функційна	1		
4		КРБКІ. 101007.21.01.08 Е3	Схема електрична прнципова	1		
		КРБКІ. 101007.21.01.08 Е8	Алгоритм роботи	1		

КРБКІ.101007.21.01.08ВП

Зм	Арк	№ докум	Підпис	Дата
Розробив		Щвець		06.24
Перевір.		Муляр		06.24
Н. контр.		Мостовий		15.06.24
Затв.		Кльоц		06.24

Біометричний термінал керування доступом в приміщення

Відомість проекту

Літера	Аркуш	Аркушів
У	1	1

КІІС-21-1

АНОТАЦІЯ

Тема кваліфікаційної роботи: Біометричний термінал керування доступом в приміщення

Автор роботи: Валентин ШВЕЦЬ

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

Пояснювальна записка: 65 с., 28 рис., 3 табл., 2 дод., 45 джерел.

Графічна частина: 4 плакати.

СИСТЕМА КОНТРОЛЮВАННЯ ДОСТУПУ, ARDUINO

В рамках цієї роботи розглянуті різні біометричні методи, які можуть бути застосовані з використанням Arduino, а також розроблені апаратна і програмна частини системи для їх імплементації.

Основною метою є створення простої і доступної системи біометричної ідентифікації на базі Arduino, яка може знайти застосування в різних сферах, таких як безпека, контролювання доступу та інше.

Результатом є недорогий пристрій для відкривання дверного механізму за допомогою зчитування відбитка пальця, на платформі Arduino.

Підпис студента

30.05.2024
Дата

ЗМІСТ

Зм.	Арк.	№ докум.	Підпис	Дата	КРБКІ. 101007.21.01.08 ПЗ		
Розробив		Швець В.Р.		3.06.24	Біометричний термінал керування доступом в приміщення Пояснювальна записка	Літера	Аркуш 2 / Аркушів 65
Перевірив		Муляр І.В.		3.06.24		н	
Н.контр.		Мостовий С.В.		13.06.24		КІ1с-21-1	
Затвер.		Кльоц Ю.П.		13.06.24			

ВСТУП

Безумовно, розробка недорогих систем контролю доступу на базі Arduino та датчиків відбитків пальців є актуальною темою в наш час. Такі системи вирізняються своєю доступністю, гнучкістю та можливістю адаптації під різноманітні вимоги. Їхня реалізація не потребує значних фінансових витрат, оскільки компоненти, задіяні в проекті, мають відносно невисоку вартість. До того ж відкрита архітектура Arduino дозволяє легко модифікувати функціональність системи, змінювати алгоритми роботи чи додавати нові можливості.

Наявність системи контролю доступу з використанням біометричної ідентифікації за відбитками пальців додає приміщенню певного шарму та солідності. Такий замок одразу створює відчуття підвищеної безпеки та захищеності, попереджаючи потенційних зловмисників навіть замислюватися про несанкціоноване проникнення.

Метою цього дослідження є розробка підходів до біометричної ідентифікації для Arduino та визначення їх ефективності і точності. В рамках цієї роботи будуть розглянуті різні біометричні методи, які можуть бути застосовані з використанням Arduino, а також будуть розроблені апаратна і програмна частини системи для їх імплементації. Основною метою є створення простої і доступної системи біометричної ідентифікації на базі Arduino, яка може знайти застосування в різних сферах, таких як безпека, контроль доступу та інше.

В епоху стрімкого розвитку новітніх технологій ми маємо можливість і, я б навіть сказав, обов'язок впроваджувати передові рішення для забезпечення недоторканності наших осель та робочих приміщень. Безпека домівок і офісів завжди має бути пріоритетом номер один. І системи замків на основі відбитків пальців безсумнівно є одним з найбільш ефективних шляхів досягнення цієї мети [1].

З точки зору безпеки, застосування біометричного методу ідентифікації за відбитками пальців вважається більш надійним, аніж використання традиційних ключів або кодів доступу. Кожен відбиток є унікальним для конкретної особи, що ускладнює його підробку та забезпечує додатковий рівень захисту. Крім того, системи на основі Arduino характеризуються низьким енергоспоживанням, що робить їх економічними в експлуатації.

Варто відзначити також автономність роботи таких систем – їм не потрібне підключення до мережі чи зовнішніх серверів для функціонування. Це дозволяє використовувати їх у різноманітних приміщеннях, де необхідно забезпечити контроль доступу. Завдяки можливості програмування, системи можна налаштувати згідно зі специфічними вимогами певного об'єкта.

Загалом, створення недорогих механізмів контролювання доступу за відбитками пальців стає все більш популярним у навчальних та дослідницьких проектах технічних спеціальностей. Вони дають змогу студентам та розробникам отримати практичний досвід роботи з мікроконтролерами, датчиками, електронними компонентами та алгоритмами біометричної ідентифікації. Тому розробка програмно-апаратного пристрою контролювання доступу за допомогою Arduino та датчиків відбитків пальців є надзвичайно актуальним і своєчасним рішенням. Таке поєднання новітніх технологій з питаннями безпеки не лише забезпечить надійний захист, але й продемонструє наш крок у майбутнє, прогресивне мислення та турботу про недоторканність особистого чи робочого простору.

Дана робота присвячена розробці підходів до біометричної ідентифікації для Arduino. Arduino є популярною платформою для розробки електронних пристроїв, і використання його в біометричних системах відкриває нові можливості для розпізнавання особи за її фізичними характеристиками.

Актуальність даної теми полягає в потребі розвитку надійних, доступних і ефективних систем біометричної ідентифікації. В сучасному світі зростає популярність таких систем у зв'язку з необхідністю забезпечення високого

рівня безпеки і захисту інформації. Використання Arduino у біометричних системах може дозволити реалізувати біометричну ідентифікацію на рівні, який раніше був доступний лише високотехнологічним пристроям. Таким чином, розробка підходів до біометричної ідентифікації для Arduino має великий потенціал для подальшого розвитку біометричних технологій та їх впровадження у повсякденне життя.

Створення власної системи контролювання доступу – це водночас і виклик, і захоплюючий проект, який дозволить втілити передові технології в життя та підвищити рівень безпеки до нових стандартів.

1 ДОСЛІДЖЕННЯ ПІДХОДІВ ДО ПОБУДОВИ СИСТЕМ КОНТРОЛЮВАННЯ ДОСТУПУ

1.1 Загальна концепція та вимоги до проєктування

Сучасні системи контролювання доступу (СКД) є ключовим елементом безпеки організацій. Вони складаються з фізичних бар'єрів, технічних засобів, апаратного і програмного забезпечення. Грамотне проєктування та впровадження таких систем вимагає високого рівня знань і кваліфікації від системних інтеграторів, а їх ефективна експлуатація залежить від знань та навичок користувачів.

Державний стандарт незалежної України ДСТУ 4000-2000 «Системи тривожної сигналізації охоронні системи і системи контролювання доступу. Терміни та визначення», який був прийнятий у 2001 році, офіційно ввів термін «система контролювання доступу» в українську нормативну базу [2]. Цей стандарт встановлює термінологію для систем контролювання доступу, охоронних теле- і відеосистем, а також для систем тривожної сигналізації, забезпечуючи єдині стандарти для цих технологій на території України.

Впровадження цього стандарту мало на меті уніфікувати підхід до проектування, впровадження та експлуатації систем безпеки, в тому числі систем контролю доступу. Це сприяло підвищенню рівня безпеки об'єктів, забезпеченню сумісності різних компонентів системи та полегшенню їх інтеграції.

Згідно зі стандартом, система контролю доступу охоплює комплекс апаратних і програмних засобів, призначених для управління доступом на певні території або об'єкти. До складу таких систем входять фізичні бар'єри, зчитувачі, контролери, програмне забезпечення контролю доступу та інші компоненти, що забезпечують надійність і безпеку контролю доступу.

Актуальність даної теми полягає в необхідності розробки надійних, доступних та ефективних систем біометричної ідентифікації. У сучасному світі

популярність таких систем зростає через необхідність забезпечення високого рівня безпеки та захисту інформації. Використання Arduino в біометричних системах може дозволити реалізувати біометричну ідентифікацію на рівні, який раніше був доступний лише високотехнологічним пристроям. Таким чином, розробка підходів до біометричної ідентифікації для Arduino має великий потенціал для подальшого розвитку біометричних технологій та їх впровадження в повсякденне життя.

Високотехнологічні рішення не гарантують максимального рівня безпеки без належного налаштування та інтеграції з іншими системами безпеки, такими як відеоспостереження чи сигналізація [3]. Недооцінка людського фактора також є поширеною проблемою. Навіть найкраща техніка не може компенсувати помилки, що виникають через недостатню підготовку персоналу або порушення процедур. Регулярне навчання користувачів є обов'язковим елементом для успішного функціонування СКД.

Ще одна проблема полягає в ігноруванні важливості обслуговування та оновлення систем. Після встановлення системи необхідно регулярно проводити технічне обслуговування та оновлювати програмне забезпечення, щоб забезпечити безперебійне функціонування і захист від нових загроз. Міф про універсальні рішення також є поширеним: немає "універсальної" системи контролю доступу, яка підходить для всіх об'єктів та умов експлуатації. Кожна система має бути адаптована до специфічних вимог і ризиків конкретного замовника [4].

Недостатнє тестування та пілотні проекти також можуть призвести до проблем. Перед повним впровадженням системи важливо провести пілотні проекти та ретельне тестування, щоб виявити можливі слабкі місця та адаптувати систему до реальних умов експлуатації.

Таким чином, успішне впровадження та експлуатація систем контролю доступу залежить не лише від технічних характеристик обладнання, але й від належного проєктування, навчання персоналу та регулярного обслуговування системи.

В системах контролювання доступу всі компоненти є взаємопов'язаними та важливими, оскільки СКД базується на управлінні фізичними діями людей через певні логічні процеси. Відсутність другорядних складових означає, що кожен елемент виконує критичну роль у загальній функціональності системи [5].

Зчитувачі завжди працюють разом з ідентифікаторами СКД, такими як картки, брелоки, біометричні дані або мобільні пристрої. Вони забезпечують ідентифікацію користувача та передають інформацію до контролера. Контролери обробляють ці дані, приймають рішення про надання або обмеження доступу, керуючи відповідними фізичними бар'єрами, як-от двері чи турнікети [6, 7].

Рівень, складність та функціональність будь-якої СКД визначаються технічними характеристиками контролерів. Вони повинні відповідати вимогам конкретного об'єкта, мати необхідну обчислювальну потужність і підтримувати потрібні протоколи зв'язку. Сумісне з контролерами програмне забезпечення виконує функції управління та моніторингу системи, забезпечуючи інтерфейс для адміністраторів, ведення журналів подій, аналіз даних та інтеграцію з іншими системами безпеки.

Крім того, обрані замовниками технології СКД також відіграють важливу роль. Це можуть бути різні методи ідентифікації (RFID, біометрія, PIN-коди), методи передачі даних (провідні чи безпровідні мережі), а також додаткові функції, такі як інтеграція з системами відеоспостереження, пожежної сигналізації чи автоматизації будівель [8].

Таким чином, всі елементи СКД є невід'ємними частинами єдиної системи, і їх взаємодія визначає загальний рівень безпеки та ефективності системи. Це підкреслює важливість ретельного вибору і налаштування кожного компонента, щоб забезпечити надійне функціонування та відповідність потребам конкретного об'єкта чи організації.

1.2 Використання біометричної ідентифікації в системах контролювання доступу

Дверні замки з відбитком пальця є сучасною технологією контролю доступу, яка поєднує механічні та електронні компоненти для забезпечення високого рівня безпеки. Використання біометричних даних, таких як відбиток пальця, забезпечує унікальність і складність підробки, що робить ці замки більш захищеними від несанкціонованого доступу порівняно з традиційними ключами чи картками [9]. Такий підхід дозволяє власникам уникнути необхідності носити з собою ключі чи карти доступу, оскільки доступ можна отримати за допомогою простого дотику до сканера.

Безумовно, властивості відбитків пальців роблять їх ідеальним вибором для застосування в системах біометричної ідентифікації та автентифікації. Унікальність, незмінність протягом життя людини, універсальність та вічність - всі ці характеристики відбитків пальців забезпечують надійність їх використання. Кожен відбиток пальця складається з унікального візерунка папілярних ліній, хвиль та завитків, який формується випадковим чином під час ембріонального розвитку і не повторюється навіть у ідентичних близнюків.

Для зберігання відбитків пальців у цифровому вигляді використовуються різні підходи та формати. Найпоширенішим є зберігання у вигляді растрових зображень у форматах BMP, JPEG або TIFF, що дозволяє зберегти детальне зображення відбитка, проте потребує значного обсягу пам'яті [10, 11]. Більш ефективним є метод векторного зображення, коли замість повного растрового зображення зберігаються лише характерні точки та напрямки папілярних ліній у вигляді векторних координат. Цей підхід дозволяє істотно зменшити необхідний обсяг пам'яті при прийнятному рівні деталізації. Також можливе зберігання узагальненого шаблону відбитка, що містить лише основні характеристики, максимально скорочуючи розмір даних, проте можливо зі зниженням точності ідентифікації. Незалежно від обраного методу, для

економії місця дані можуть бути стиснуті за допомогою різних алгоритмів стиснення з втратами чи без втрат якості. Вибір оптимального способу зберігання визначається вимогами системи до точності, обсягу пам'яті та швидкодії.

Замки з відбитком пальця також мають перевагу в зручності використання. Процес налаштування та експлуатації зазвичай є інтуїтивно зрозумілим, що зменшує потребу в навчанні користувачів. Крім того, багато з цих замків зберігають журнали подій, дозволяючи відслідковувати, хто і коли використовував замок (рисунок 1.1).

Рисунок 1.1 - Смарт замок TTLOCK BOSS [12]

Однак, існують і певні недоліки та виклики. Деякі біометричні сенсори (рисунок 1.2) можуть мати проблеми з точністю в умовах забруднення, вологості або пошкодження шкіри на пальцях. Крім того, вартість біометричних замків зазвичай вища порівняно з традиційними механічними або картковими системами контролю доступу. Залежність від електроживлення

також є суттєвим фактором, оскільки для роботи біометричних сенсорів і електроніки потрібне стабільне електроживлення. У випадку збою або відключення електроенергії необхідно мати резервні методи доступу.

Рисунок 1.2 – Сканери відбитків пальців [13]

Питання приватності та безпеки даних також є важливими. Збір та зберігання біометричних даних викликають занепокоєння щодо їхньої безпеки та відповідності нормативним вимогам.

Дверні замки з відбитком пальця є ефективним і зручним рішенням для контролю доступу, яке забезпечує високий рівень безпеки завдяки використанню біометричних даних. Однак, вони мають деякі технічні та експлуатаційні обмеження, які необхідно враховувати при їх виборі та впровадженні. Зважаючи на їхні переваги та недоліки, такі замки можуть бути оптимальним вибором для різних застосувань, особливо в місцях, де важлива висока безпека і зручність користування.

ZKTeco є відомим виробником систем контролю доступу, зокрема дверних замків з відбитком пальця, і має ряд переваг, що робить їх продукцію популярною серед користувачів [14].

Однією з головних переваг ZKTeco є висока точність і надійність їхніх біометричних сенсорів. Завдяки передовим технологіям розпізнавання

відбитків пальців, їхні замки забезпечують швидке і точне ідентифікування користувачів, мінімізуючи ризик помилок або відмов.

Ще одна суттєва перевага полягає в багатофункціональності пристроїв. ZKTeco пропонує рішення, що поєднують різні методи ідентифікації, включаючи відбитки пальців, PIN-коди, RFID-картки та мобільні додатки. Це дозволяє користувачам обирати найбільш зручний і безпечний спосіб доступу відповідно до їхніх потреб (рисунок 1.3).

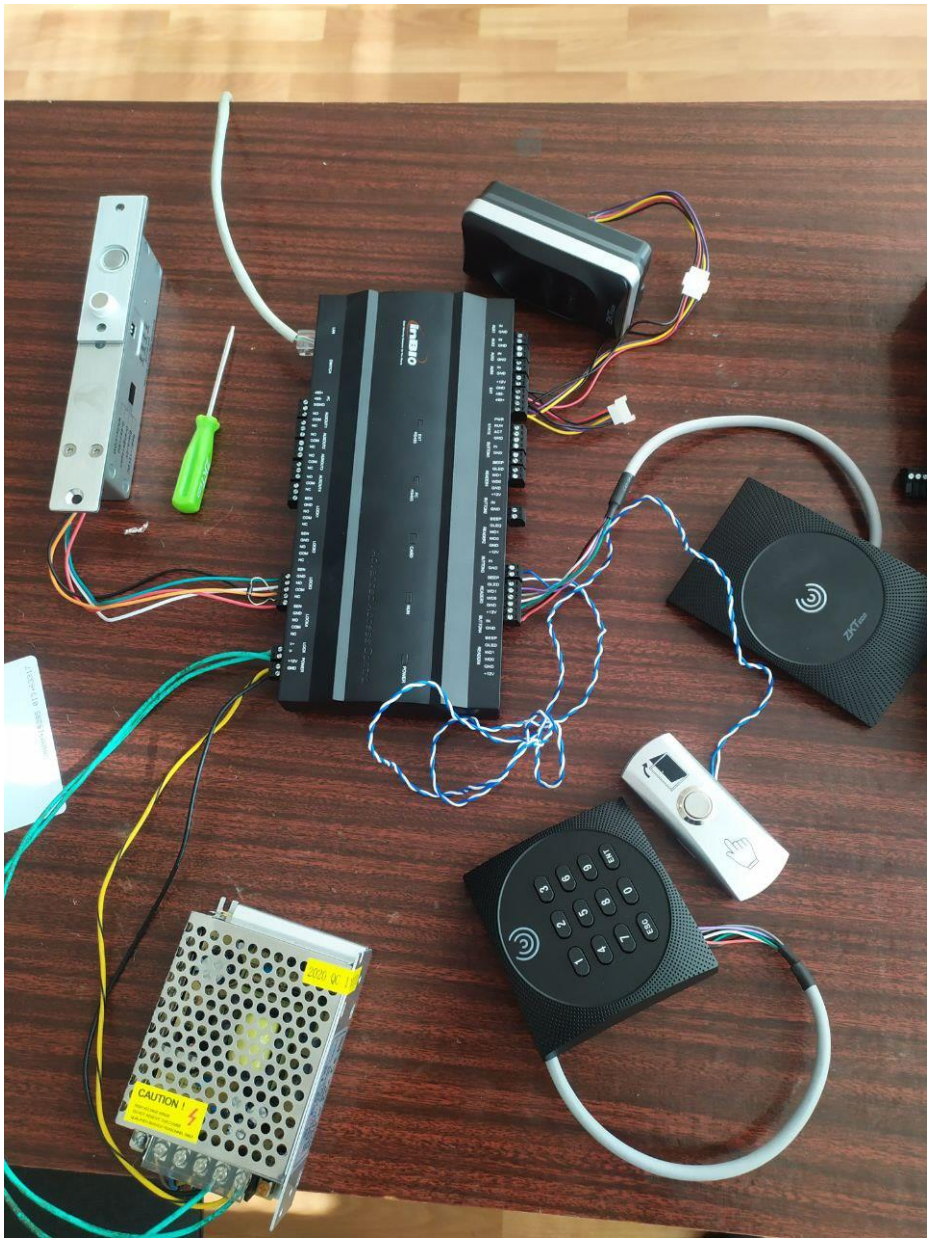


Рисунок 1.3 – Система контролювання доступу ZKTeco

ZKTeco також відома своєю гнучкістю і масштабованістю систем. В їхніх продуктах легко налаштовуються параметри доступу для різних користувачів і груп, а також інтеграція з іншими системами безпеки, такими як відеоспостереження та пожежна сигналізація. Це дозволяє створювати комплексні системи безпеки, які можна адаптувати до вимог різних об'єктів (рисунок 1.4).

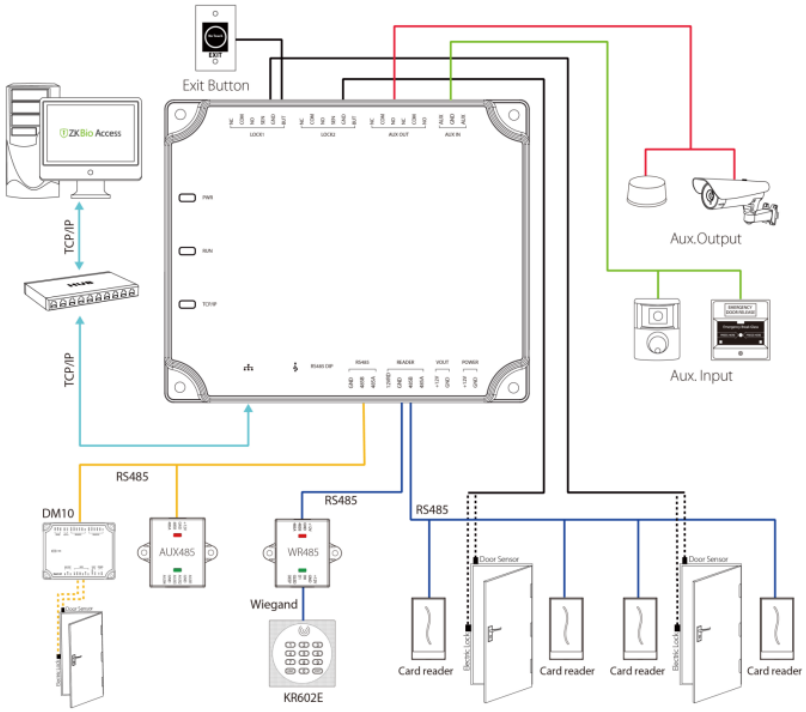


Рисунок 1.4 – Проєкт системи контролювання доступу [15]

Інтерфейс програмного забезпечення ZKTeco відрізняється зручністю і зрозумілістю, що спрощує процес налаштування і управління системою. Це важливо для адміністраторів, яким потрібно оперативно вносити зміни та контролювати доступ.

Додатковою перевагою є висока якість і довговічність продукції. Замки та інші пристрої ZKTeco виготовлені з високоякісних матеріалів, що забезпечує їхню стійкість до зносу і зовнішніх впливів. Це особливо важливо для пристроїв, які використовуються в умовах інтенсивної експлуатації.

ZKTeco також пропонує конкурентоспроможні ціни на свої продукти, що робить їх доступними для широкого кола користувачів, від малих підприємств до великих корпорацій. Економічна ефективність рішень ZKTeco

забезпечується не тільки завдяки помірним цінам, але й завдяки низьким експлуатаційним витратам [16].

Таким чином, переваги використання продукції ZKTeco в системах контролю доступу включають високу точність і надійність біометричних сенсорів, багатофункціональність, гнучкість і масштабованість систем, зручність програмного забезпечення, високу якість і довговічність продукції, а також економічну ефективність. Ці характеристики роблять ZKTeco одним з лідерів на ринку систем контролювання доступу.

1.3 Аналіз переваг та недоліків існуючих рішень

На сьогодні існує багато підходів до побудови систем контролювання доступу. Можна використовувати спеціалізованепромислове обладнання, але ,цікавіше реалізувати самостійно. Для керування системою доступу слід використовувати мікроконтролери. На сьогодні найбільш популярні це сімейства Arduino і Raspberry Pi.

Біометричний контроль доступу на базі Raspberry Pi має кілька суттєвих переваг. Raspberry Pi є потужною і компактною платформою, яка дозволяє інтегрувати різні біометричні датчики, такі як зчитувачі відбитків пальців, завдяки широкій підтримці периферійних пристроїв і протоколів [17]. Використання Raspberry Pi дозволяє розробникам створювати гнучкі та масштабовані рішення, адаптуючи систему до конкретних потреб завдяки великій кількості доступних бібліотек і програмного забезпечення з відкритим кодом.

Raspberry Pi забезпечує високу продуктивність і обробку даних у реальному часі, що важливо для швидкої та точної ідентифікації користувачів. Крім того, завдяки підтримці мережевих з'єднань, система може бути

інтегрована з іншими системами безпеки та базами даних, що дозволяє централізовано керувати доступом і зберігати журнали подій.

Також Raspberry Pi має низьку вартість, що робить його доступним рішенням для різних організацій, від малих підприємств до великих корпорацій (рисунок 1.5). Важливою перевагою є також простота налаштування та використання, що дозволяє швидко розгорнути систему контролю доступу без значних витрат часу та ресурсів.

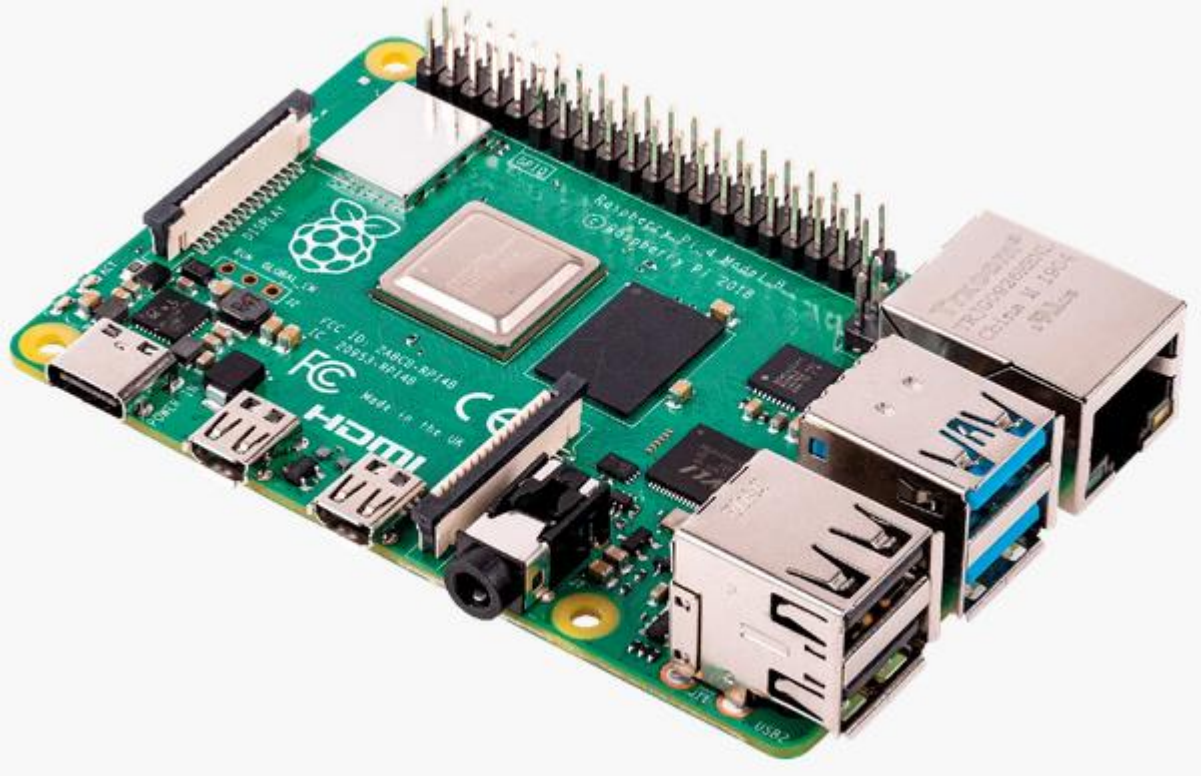


Рисунок 1.5 – Набір Raspberry Pi

Біометричний контроль доступу на базі Raspberry Pi має кілька недоліків. В нього обмежена потужність обробки даних порівняно з більш потужними комп'ютерами може впливати на швидкість і точність ідентифікації користувачів у системах з високим навантаженням або великою кількістю користувачів. Також обмежена кількість периферійних з'єднань на Raspberry Pi може обмежити кількість підключених біометричних датчиків або інших

необхідних пристроїв, що може вимагати додаткових компонентів або розширень.

І надійність системи може бути під питанням у випадку інтенсивного використання або в складних умовах, оскільки Raspberry Pi менш стійкий до фізичних впливів і екстремальних умов навколишнього середовища порівняно з промисловими рішеннями. Крім того, безпека системи може бути під загрозою, оскільки відкритість платформи та її програмного забезпечення може спрощувати спроби несанкціонованого доступу або втручання [18].

Іншим недоліком є залежність від зовнішніх модулів і компонентів, які можуть мати свої обмеження та вимагати додаткової інтеграції, налаштування та технічної підтримки. Нарешті, в деяких випадках відсутність офіційної технічної підтримки або гарантій може створювати проблеми при вирішенні технічних труднощів або несправностей. Ну і вартість розробки буде вищою в порівнянні з Arduino.

Дана робота присвячена розробці підходів до біометричної ідентифікації для Arduino. Arduino є популярною платформою для розробки електронних пристроїв, і використання його в біометричних системах відкриває нові можливості для розпізнавання особи за її фізичними характеристиками. У даному дослідженні будуть розглянуті підходи та розробки, які дозволять застосовувати Arduino для біометричної ідентифікації з використанням різних біометричних методів, таких як відбитки пальців, розпізнавання обличчя, розпізнавання радужної оболонки ока тощо.

Розробка системи контролювання доступу на базі платформи Arduino має багато переваг. Arduino є доступною і економічно ефективною платформою, що дозволяє придбати компоненти за розумними цінами. Багато сумісних датчиків і модулів доступні на ринку, що сприяє створенню недорогих рішень для контролю доступу.

Платформа Arduino відрізняється легкістю у вивченні та використанні. Завдяки інтуїтивно зрозумілому середовищу програмування та великій

кількості навчальних ресурсів, Arduino підходить як для новачків, так і для професіоналів. Активна спільнота підтримує користувачів через форуми, відеоуроки і документацію, що спрощує процес розробки.

Arduino також забезпечує високу гнучкість і масштабованість. Є можливість створювати індивідуальні рішення, які відповідають конкретним потребам вашого проекту. Легкість додавання нових функцій і інтеграції різних компонентів, таких як RFID-зчитувачі, клавіатури, біометричні сенсори або бездротові модулі, дозволяє створювати системи контролю доступу будь-якої складності.

Платформа Arduino ідеально підходить для швидкого прототипування. Ви можете легко збирати і тестувати різні конфігурації системи, вносячи зміни в апаратне і програмне забезпечення на льоту. Це дозволяє оперативно знаходити оптимальні рішення і скорочувати час розробки.

Arduino підтримує численні протоколи зв'язку, такі як I2C, SPI, UART, а також бездротові технології, як-от Wi-Fi, Bluetooth і LoRa [19]. Це полегшує інтеграцію системи контролю доступу з іншими системами безпеки або автоматизації, забезпечуючи комплексний підхід до управління об'єктом.

Платформа Arduino має велику і активну спільноту розробників, які діляться своїми проектами, кодами та ідеями. Це означає, що ви можете знайти багато готових рішень і прикладів, які допоможуть у розробці власної системи контролю доступу.

Arduino також дозволяє легко додавати нові функції і можливості до вашої системи. Ви можете інтегрувати камери для відеоспостереження, датчики руху або датчики диму, створюючи більш комплексні системи безпеки. Завдяки широкій підтримці і різноманітним ресурсам, після розробки системи ви зможете легко підтримувати та оновлювати її, реагуючи на нові вимоги або вдосконалюючи функціональність.

Таким чином, використання Arduino для розробки системи контролювання доступу пропонує доступність, гнучкість, легкість у

використанні та інтеграції, що робить його чудовим вибором як для навчальних проектів, так і для комерційних застосувань.

Використання мікроконтролера Atmega328P у розробці системи контролю доступу має кілька вагомих переваг. Цей мікроконтролер є серцем популярної платформи Arduino Uno, що робить його добре підтримуваним і легко інтегрованим у різні проекти (рисунок 1.6).

Рисунок 1.6 – Мікроконтролер Atmega328P [20]

По-перше, Atmega328P є досить доступним за ціною, що дозволяє створювати економічно ефективні рішення для контролю доступу. Він широко доступний на ринку, що спрощує його придбання та заміну в разі потреби.

По-друге, Atmega328P має достатньо ресурсів для виконання більшості завдань, пов'язаних із контролем доступу. Мікроконтролер оснащений 32 КБ флеш-пам'яті для зберігання програми, 2 КБ оперативної пам'яті SRAM і 1 КБ EEPROM для зберігання налаштувань або журналів подій. Це дозволяє розробляти досить складні програми і зберігати необхідну інформацію для роботи системи [20].

По-третє, Atmega328P підтримує різноманітні протоколи зв'язку, включаючи UART, SPI і I2C. Це робить його дуже гнучким для інтеграції з різними периферійними пристроями, такими як RFID-зчитувачі, клавіатури, датчики та модулі бездротового зв'язку. Завдяки цьому ви можете створювати

складні системи контролювання доступу, які відповідають конкретним потребам вашого проекту.

Плата на базі мікроконтролера Atmega328P може працювати від зовнішнього джерела живлення, яке забезпечує напругу в діапазоні від 6 до 20 вольт. Однак є деякі особливості щодо оптимального діапазону напруги, які слід враховувати для забезпечення стабільної роботи.

Якщо напруга живлення менша за 7 вольт, на виході стабілізатора напруги може подаватися менше 5 вольт, що може призвести до нестабільної роботи плати. Це може викликати збої в роботі мікроконтролера та інших компонентів, що підключені до плати. Тому використання напруги нижче 7 вольт не рекомендується.

При використанні напруги вище 12 вольт регулятор напруги на платі може перегріватися. Перегрів може призвести до виходу плати з ладу, оскільки надмірне нагрівання може пошкодити регулятор або інші компоненти. Таким чином, напруга живлення більше 12 вольт також не є оптимальною для роботи плати.

Рекомендований діапазон напруги живлення для стабільної роботи плати становить від 7 до 12 вольт. У цьому діапазоні плата працює стабільно і без ризику перегріву регулятора напруги.

На відміну від попередніх плат, які використовували мікросхему драйвера FTDI USB-to-serial для зв'язку з комп'ютером, Atmega328P оснащена мікроконтролером Atmega8U2 (або Atmega16U2 у деяких версіях), який запрограмований як перетворювач USB-послідовний порт. Це забезпечує більш швидкий і надійний зв'язок між платою та комп'ютером, а також дозволяє оновлювати прошивку мікроконтролера без додаткового обладнання. Використання Atmega8U2 замість FTDI дозволяє зменшити вартість плати та спрощує її конструкцію.

Мікроконтролер також відомий своєю енергоефективністю. Atmega328P має різні режими енергозбереження, що дозволяє зменшити споживання енергії

під час простою. Це важливо для систем контролю доступу, які повинні працювати безперервно і часто використовують резервне живлення.

Ще однією перевагою є простота програмування та наявність великої кількості бібліотек і прикладів коду. Мікроконтролер Atmega328P підтримується середовищем розробки Arduino IDE, яке пропонує зручний інтерфейс для написання, компіляції та завантаження програм. Величезна спільнота користувачів Arduino активно ділиться кодами, проектами та ідеями, що значно полегшує процес розробки.

Atmega328P також відрізняється високою надійністю і стабільністю в роботі. Він широко використовується у багатьох комерційних і промислових додатках, що підтверджує його надійність і здатність працювати в різних умовах.

Використання Atmega328P для розробки системи контролювання доступу забезпечує економічну ефективність, гнучкість, енергоефективність і простоту програмування. Цей мікроконтролер є відмінним вибором як для новачків, так і для досвідчених розробників, що дозволяє створювати надійні і функціональні системи контролю доступу

1.4 Постановка задачі

Метою цього дослідження є розробка підходів до біометричної ідентифікації для Arduino та визначення їх ефективності і точності. В рамках цієї роботи будуть розглянуті різні біометричні методи, які можуть бути застосовані з використанням Arduino, а також будуть розроблені апаратна і програмна частини системи для їх імплементації. Основною метою є створення простої і доступної системи біометричної ідентифікації на базі Arduino, яка може знайти застосування в різних сферах, таких як безпека, контроль доступу

та інше. Для досягнення поставленої задачі потрібно вирішити наступня завдання:

– система повинна забезпечувати ідентифікацію користувачів за відбитком пальця;

– доступ до приміщення має надаватися лише авторизованим користувачам;

– система повинна вести журнал подій, що включає інформацію про час ідентифікації та статус доступу (дозволено/заборонено);

– система повинна мати можливість додавання та видалення користувачів через інтерфейс користувача;

– індикація успішної та невдалої ідентифікації повинна здійснюватися за допомогою світлодіодів та звукового сигналу;

– керуючий мікроконтролер - плата arduino uno на базі ATMEGA328p;

– електронний замок - реле або соленоїдний замок для керування доступом до дверей;

– програмне забезпечення для arduino, написане на мові програмування c++ з використанням середовища розробки Arduino IDE;

– бібліотеки для роботи зі зчитувачем відбитків пальців та іншими компонентами.

Таким чином, технічне завдання на побудову системи контролю доступу в приміщення за відбитком пальця на основі платформи Arduino визначає основні функціональні та технічні вимоги, апаратні та програмні компоненти, а також етапи виконання проєкту.

2 ПРОЄКТУВАННЯ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ

2.1 Обгрунтування вибору системи керування

Метою даного проекту є розробка та впровадження системи контролю доступу в приміщення, яка використовує біометричну ідентифікацію за відбитком пальця. Система повинна забезпечити надійний контроль доступу, ведення журналу подій та можливість керування через інтерфейс користувача. Для цього використовуються два мікроконтролери Atmega328P.

У нашій розробці системи контролювання доступу в якості центрального елементу використано мікроконтролер Atmega328P (рисунок 2.1). Оскільки Atmega328P має обмежену кількість контактів (всього 28, по 14 з кожного боку), для реалізації всіх необхідних функцій ми вирішили використовувати два мікроконтролери Atmega328P. Це дозволило нам збільшити кількість доступних вхідних і вихідних контактів та ефективно розподілити завдання між двома мікроконтролерами, забезпечуючи більш високу продуктивність та гнучкість системи.

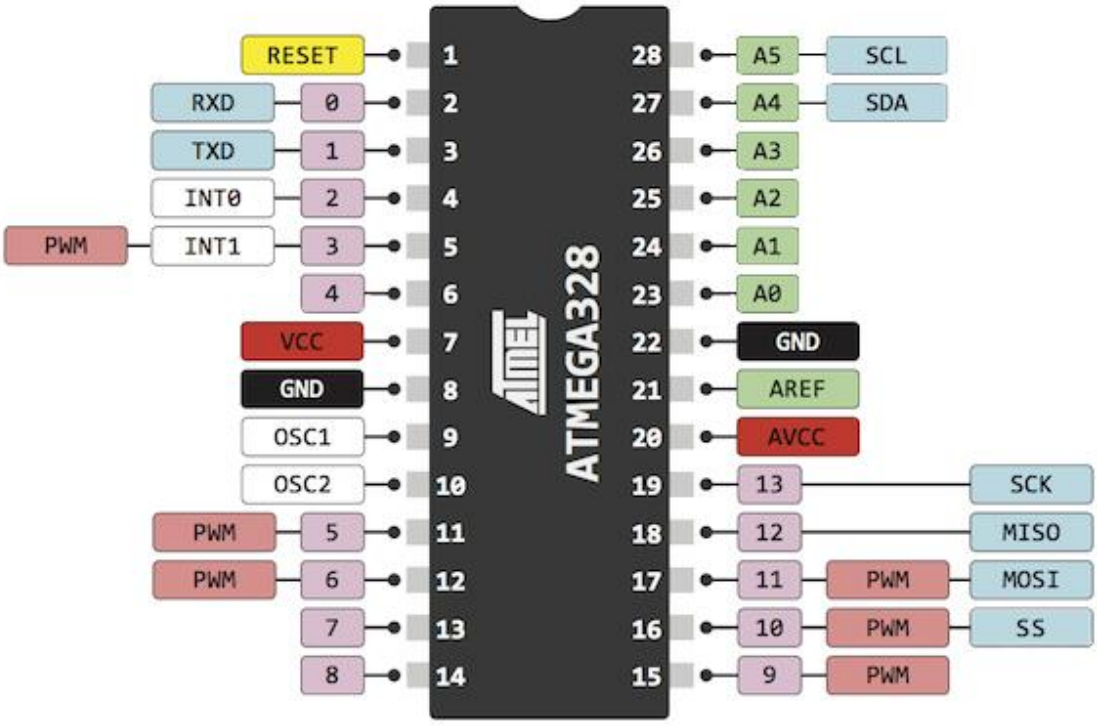


Рисунок 2.1 – Контакти Atmega328P [21]

Напруга живлення подається на виводи мікроконтролера VCC і GND і не повинна перевищувати значення, зазначене в технічній документації. Для ATmega328P верхня межа рекомендованої напруги живлення становить 5,5 В, абсолютний максимум – 6 В. Тривала робота при такій напрузі може вивести мікроконтролер з ладу.

Для придушення високочастотних перешкод у ланцюзі живлення рекомендується встановлювати керамічний конденсатор ємністю 0,1 мкФ між VCC і GND. Причому розташовувати його слід якнайближче до живлячих виводів мікроконтролера для мінімізації паразитної індуктивності та опору підвідних провідників.

Для з’єднання двох Atmega328p між собою використовуємо схему, зображену на рисунку 2.2.

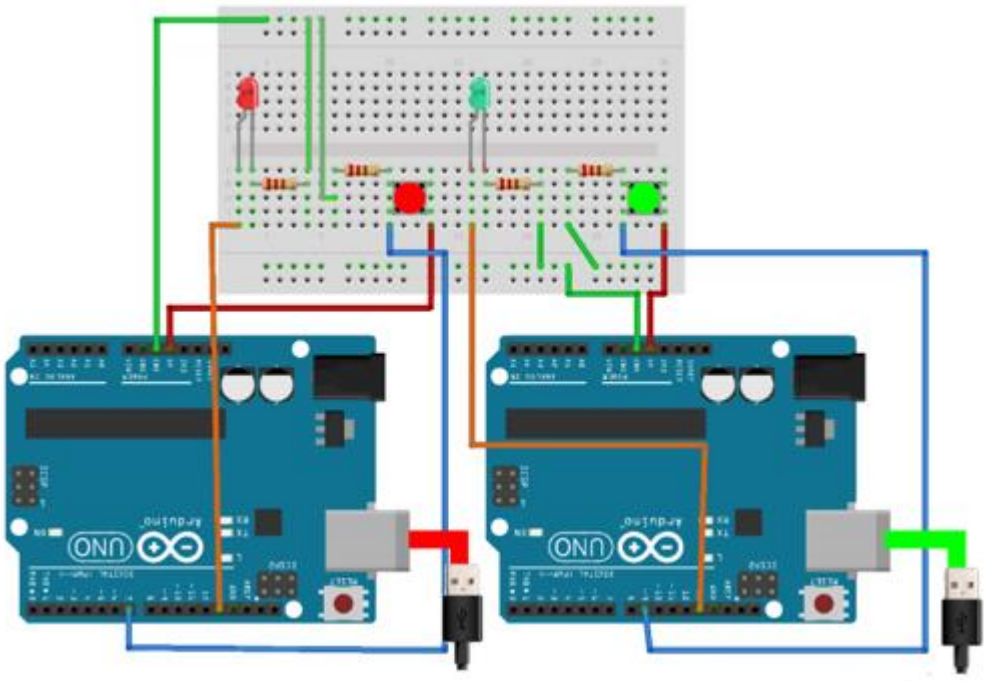


Рисунок 2.2 – Зєднання двох мікроконтролерів [22]

ATmega328P має подвійне живлення: виводи VCC і GND (виводи 7 і 8) використовуються для живлення цифрових схем мікроконтролера; AVCC і GND (виводи 20 і 22) – для живлення аналого-цифрового перетворювача. Навіть якщо ви не збираєтеся використовувати АЦП, до нього повинно бути

підведено живлення: з'єднайте виводи VCC з AVCC, а цифрову землю з аналоговою. Якщо ж ви плануєте використовувати АЦП, то в ланцюг живлення слід додати фільтр для зменшення перешкод. У даташиті рекомендується з'єднати AVCC з VCC через індуктивність 10 мкГн і з GND через ємність 0,1 мкФ. Однак ця рекомендація не виконується навіть у платах Arduino, і вивід AVCC на них просто з'єднаний з VCC.

2.2 Загальна структура системи

В структурній схемі розробленого пристрою компоненти представлені у спрощеному вигляді за допомогою графічних позначень у формі довільних прямокутників. Всередині кожного прямокутника, що символізує певний функціональний блок системи, міститься коротка назва, яка описує його призначення [23].

Вибір конкретних компонентів для включення до структурної схеми здійснювався з урахуванням використання сучасних, ефективних та новітніх мікроелектронних елементів, які відповідають визначеним у технічному завданні вимогам до системи. Врахування поставлених перед пристроєм завдань є необхідним для забезпечення його належного функціонування.

Основна мета структурної схеми - відображення загальної структури пристрою, його основних блоків, вузлів, деталей та зв'язків між ними. Завдяки цьому можна зрозуміти принципи роботи пристрою в його основних режимах та взаємодію між компонентами. При розробці структурної схеми електричної системи допускається використання довільних позначень для елементів, проте слід дотримуватися загальноприйнятих правил оформлення схем.

Таким чином, структурна схема дає уявлення про загальну архітектуру та взаємозв'язки основних складових частин пристрою, що сприяє кращому розумінню його конструкції та принципів функціонування, використовуючи

сучасні компоненти, підібрані з урахуванням вимог технічного завдання (рисунок 2.3). Схема також наведена в додатку Б.

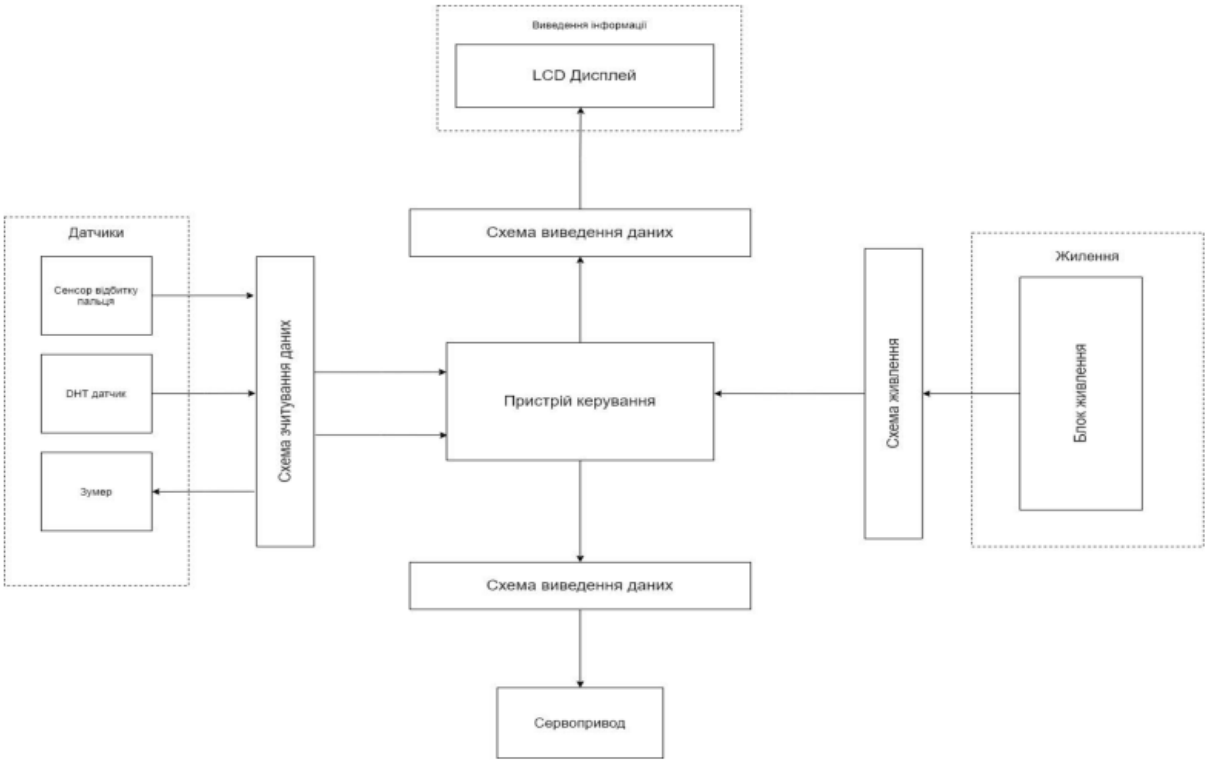


Рисунок 2.3 – Схема електрична структурна

Базуючись на функціях та завданнях, визначених у технічному завданні, можна виокремити ключові модулі системи. Відповідно до цих завдань, система була розділена на окремі блоки, кожен з яких виконує специфічні функції та взаємодіє з іншими блоками. Такий підхід дозволяє забезпечити ефективну роботу системи в цілому та виконання поставлених перед нею функціональних вимог.

Розділення системи на модулі сприяє кращому розумінню її структури та організації, а також полегшує процеси розробки, тестування та внесення змін до окремих компонентів. Крім того, модульний підхід забезпечує більшу гнучкість та масштабованість системи у випадку, якщо виникне необхідність її розширення чи модернізації. Тепер перейдемо до розгляду основних складових запропонованої електричної структурної схеми.

Модульна організація дозволяє чітко визначити функціональні обов'язки кожного блока, що спрощує процес проектування та впровадження. Водночас, зв'язки між модулями забезпечують їхню узгоджену взаємодію для досягнення загальної мети системи. Такий структурований підхід є ключовим для створення складних систем, особливо у сфері електроніки та автоматизації.

Загалом, розподіл системи на модулі на основі технічного завдання є ефективним способом організації її структури та функціонування. Це дозволяє розробникам зосередитись на окремих компонентах, водночас зберігаючи цілісність та ефективність системи в цілому.

В якості пристрою керування використано два мікроконтролери Atmega328P. Керуючий модуль виконує такі функції:

- управляє всіма компонентами системи;
- обробляє дані з біометричного модуля;
- керує індикацією та звуковим сигналізатором;
- відповідає за управління електронним замком;
- взаємодіє з клавіатурою і дисплеєм.

Один мікроконтролер обробляє зчитування відбитків пальців, перевіряє їх та надсилає результати ідентифікації до другого мікроконтролера.

Інший мікроконтролер приймає дані ідентифікації, керує замком, веде журнал подій, обробляє введення з клавіатури та відображає інформацію на дисплеї.

Зчитувач відбитків пальців виконує кілька ключових функцій для забезпечення ідентифікації користувачів у системі контролю доступу. Основною функцією є захоплення зображення відбитка пальця за допомогою оптичного або ємнісного сенсора. Після цього зображення піддається попередній обробці, щоб покращити його якість і виділити ключові характеристики відбитка.

Далі зчитувач виконує процес екстракції ознак, що включає визначення унікальних точок на відбитку, таких як кінцеві точки та розгалуження ліній. Ці ознаки використовуються для створення математичної моделі відбитка пальця.

Після екстракції ознак, зчитувач проводить порівняння отриманої моделі з вже збереженими в базі даних відбитками. Це дозволяє визначити, чи відповідає поточний відбиток зареєстрованому користувачу. Якщо відбиток розпізнано, зчитувач передає сигнал про успішну ідентифікацію до системи контролю доступу, що дозволяє користувачу отримати доступ.

Зчитувач також може забезпечувати зберігання нових відбитків у базі даних під час процесу реєстрації нових користувачів. Крім того, він може мати функції для видалення відбитків і управління базою даних користувачів. Важливою функцією є також забезпечення безпеки зберігання та передачі даних відбитків, щоб запобігти несанкціонованому доступу або втраті даних.

Дисплей у системі контролю доступу виконує кілька важливих функцій для інформування користувачів та адміністраторів. Основна функція дисплея полягає в наданні зворотного зв'язку користувачам під час процесу аутентифікації, наприклад, повідомлення про успішний або невдалий доступ, запит на повторне сканування відбитка пальця або введення додаткових даних. Дисплей також використовується для відображення інструкцій і повідомлень, що робить систему більш зрозумілою та зручною для користувачів.

Крім того, дисплей може показувати інформацію для адміністраторів, таку як журнали подій, списки зареєстрованих користувачів і статус системи. Це дозволяє здійснювати моніторинг і управління системою безпосередньо з пристрою. У режимі налаштування дисплей допомагає в конфігурації системи, надаючи можливість вибору різних опцій і параметрів через зручний інтерфейс.

Дисплей також може використовуватися для показу часу та дати, що є корисним для реєстрації подій у реальному часі. Загалом, дисплей є важливим компонентом системи контролю доступу, забезпечуючи зручний інтерфейс для взаємодії з користувачами та адміністраторів.

GSM модуль у системі контролювання доступу виконує кілька важливих функцій, що забезпечують зв'язок та моніторинг системи на відстані. Він дозволяє системі надсилати текстові повідомлення або робити телефонні дзвінки для інформування користувачів або адміністраторів про різні події, такі як успішний або невдалий доступ, спроби несанкціонованого проникнення, або інші критичні ситуації. Це забезпечує підвищену безпеку та контроль, оскільки адміністратори можуть отримувати сповіщення в режимі реального часу незалежно від їхнього місця знаходження.

GSM модуль також дозволяє віддалено керувати системою контролю доступу через SMS-команди або дзвінки. Це може включати можливість відкриття дверей, додавання або видалення користувачів, або зміни налаштувань системи. Така функціональність особливо корисна для великих об'єктів або в ситуаціях, коли фізичний доступ до системи обмежений.

Крім того, GSM модуль може використовуватися для двостороннього зв'язку між системою контролювання доступу та зовнішніми серверами або хмарними платформами, що дозволяє зберігати журнали подій, здійснювати резервне копіювання даних та інтегрувати систему з іншими безпековими рішеннями. Це значно розширює можливості моніторингу та управління системою.

Таким чином, GSM модуль забезпечує мобільність, оперативність та додаткову безпеку системи контролювання доступу, роблячи її більш гнучкою та ефективною у використанні [24].

Реле у системі контролювання доступу виконують критичні функції, пов'язані з фізичним управлінням замками та іншими механізмами, які забезпечують доступ до приміщення [25].

Реле виконує роль електронного перемикача, який дозволяє мікроконтролеру або іншому низьковольтному електронному компоненту керувати високовольтними або високострумовими пристроями, такими як електромагнітні замки. Коли система визначає, що доступ дозволено, реле

активується, замикаючи або розмикаючи ланцюг, що живить замок, тим самим відкриваючи або закриваючи його.

Мотор-редуктор у системі контролювання доступу використовується для забезпечення руху механізмів із підвищеною точністю та контролем, особливо коли потрібне сильне зусилля при низькій швидкості. Його основне призначення — передавати потужність від електродвигуна до механічного навантаження з одночасним зниженням швидкості обертання і збільшенням крутного моменту. Це дозволяє мотор-редуктору ефективно переміщати важкі механізми, такі як замки, ворота, шлагбауми або інші пристрої, що вимагають великої сили для роботи [25].

Мотор-редуктор забезпечує плавний і стабільний рух механічних частин, що важливо для забезпечення надійного доступу та запобігання пошкодженню системи. Завдяки редукції швидкості обертання, мотор-редуктор може точніше контролювати позицію та рух, що є критичним у системах, де важлива висока точність і повторюваність дій, таких як автоматичні двері або бар'єри.

Використання мотор-редуктора також допомагає зменшити навантаження на сам двигун, продовжуючи його термін служби та підвищуючи ефективність роботи системи. Це досягається за рахунок оптимального розподілу потужності та зусиль, що дозволяє мотору працювати в оптимальному режимі навіть при високих навантаженнях.

Бузер, або звуковий сигналізатор, у системі контролювання доступу відповідає за надання звукових сповіщень користувачам. Він використовується для індикації різних станів системи, таких як успішне або невдале зчитування відбитка пальця. Коли користувач успішно проходить ідентифікацію, бузер може видавати короткий сигнал, що підтверджує надання доступу. У разі невдалого зчитування або відмови у доступі бузер видає інший звуковий сигнал, зазвичай довший або більш інтенсивний, щоб привернути увагу користувача до проблеми.

Крім індикації доступу, бузер може використовуватися для інших сповіщень, наприклад, попереджень про помилки в системі або необхідності обслуговування. У разі, якщо система вимагає додаткової взаємодії від користувача, бузер може сигналізувати про це, наприклад, при необхідності повторного сканування відбитка пальця або введення пароля.

Бузер також може бути корисним для адміністративного персоналу, оскільки звукові сповіщення допомагають швидко реагувати на події, такі як несанкціоновані спроби доступу або інші аномалії в роботі системи. Звукові сигнали від бузера сприяють покращенню зручності використання системи, забезпечуючи швидкий та зрозумілий зворотний зв'язок у різних ситуаціях.

Схема управління даними в системі контролювання доступу виконує роль центральної нервової системи, організовуючи потоки інформації та процеси прийняття рішень, що мають вирішальне значення для забезпечення безпеки та ефективності. Після отримання потоку даних система здійснює процес аналізу та перевірки.

2.3 Обгрунтування обраних компонентів системи

Цифровий зчитувач відбитків пальців - це пристрій, призначений для ідентифікації особи за унікальними характеристиками її пальця. Цей зчитувач використовує спеціальні датчики для сканування поверхні пальця, збираючи деталі його фізичної структури, такі як лінії, виступи та впадини. Після сканування, отримані дані перетворюються на цифровий шаблон за допомогою спеціальних алгоритмів обробки. Цей шаблон використовується для подальшого порівняння з іншими шаблонами, які зберігаються у базі даних. При порівнянні відбитка пальця зі збереженими шаблонами, система визначає, чи відповідає відбиток певному користувачеві. Такий процес ідентифікації

може бути використаний для надання доступу до приміщень, комп'ютерних систем або інших об'єктів, які потребують автентифікації користувача [26, 27].

Сканер відбитків пальців R307 є популярним модулем для застосування в системах біометричної ідентифікації та контролю доступу [28]. Цей пристрій має низку переваг та характеристик, які роблять його привабливим вибором для розробників:

– використовує оптичний сенсор для зчитування відбитків пальців, що забезпечує високу якість зображень, що підвищує точність розпізнавання;

– має роздільну здатність 508 dpi, що гарантує детальне відтворення дрібних деталей відбитка пальця;

– розміри області сканування 16х24 мм дозволяють зчитувати повний відбиток великого пальця;

– здатний зчитувати відбитки за 0,5-0,8 секунди, забезпечуючи зручність та оперативність використання;

– оснащений потужним процесором для обробки та порівняння відбитків, що знижує навантаження на головний контролер системи;

– здатний виявляти підроблені або фальшиві відбитки завдяки використанню спеціальних алгоритмів;

– підтримує популярні інтерфейси зв'язку, такі як UART та USB, що полегшує його підключення до різних систем;

– сконструйований із використанням міцних матеріалів і здатний витримувати понад 10 мільйонів сканувань;

– має омпактний розмір та низьке енергоспоживання, що робить його придатним для вбудованих і портативних застосувань.

Загалом, R307 (рисунок 2.4) є потужним і водночас простим у використанні сканером відбитків пальців, що забезпечує високу точність розпізнавання при відносно невисокій ціні. Ці характеристики роблять його відмінним вибором для систем контролювання доступу та інших проектів, де потрібна надійна біометрична ідентифікація.

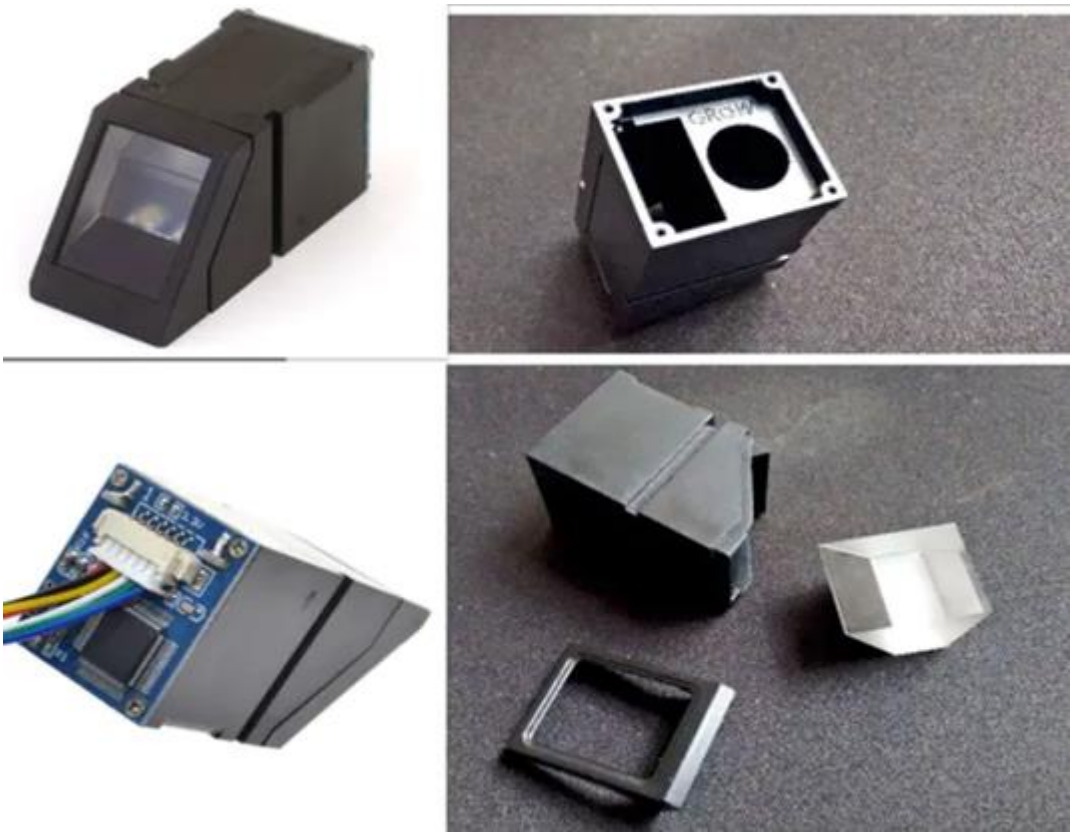


Рисунок 2.4 - Сенсор зчитування відбитків пальців [28]

Для того, щоб система мала змогу ідентифікувати користувачів та надавати їм доступ, необхідно попередньо зареєструвати їхні відбитки пальців у базі даних пристрою. Під час процесу реєстрації користувач сканує свій відбиток на датчику сканера. Зображення відбитка оцифровується, обробляється для виділення унікальних ознак візерунка папілярних ліній, а отриманий цифровий шаблон зберігається в базі даних у зв'язці з присвоєним цьому користувачеві ідентифікатором. Ідентифікатором може бути числовий код, кодове ім'я тощо. Процес реєстрації повторюється для всіх користувачів, яким буде надано дозвіл на доступ [29].

Після завершення реєстрації система готова до роботи в режимі ідентифікації. Коли користувач підносить палець до сканера, пристрій зчитує поточний відбиток, обробляє його і отримує цифровий шаблон. Далі відбувається порівняння цього шаблону з усіма зареєстрованими шаблонами в базі за допомогою спеціальних алгоритмів. Якщо знаходиться збіг з одним із

шаблонів з певним ступенем достовірності, система ідентифікує користувача через його ідентифікатор. Базуючись на результаті ідентифікації, система або надає доступ користувачеві, розблокувавши, наприклад, електричний замок дверей, або відмовляє йому у доступі.

Отже, попередня реєстрація відбитків пальців авторизованих користувачів із присвоєнням унікальних ідентифікаторів є критично важливим і невід'ємним етапом для належного функціонування біометричної системи контролювання доступу на основі відбитків пальців. Внутрішня будова сенсору наведена на рисунку 2.5.

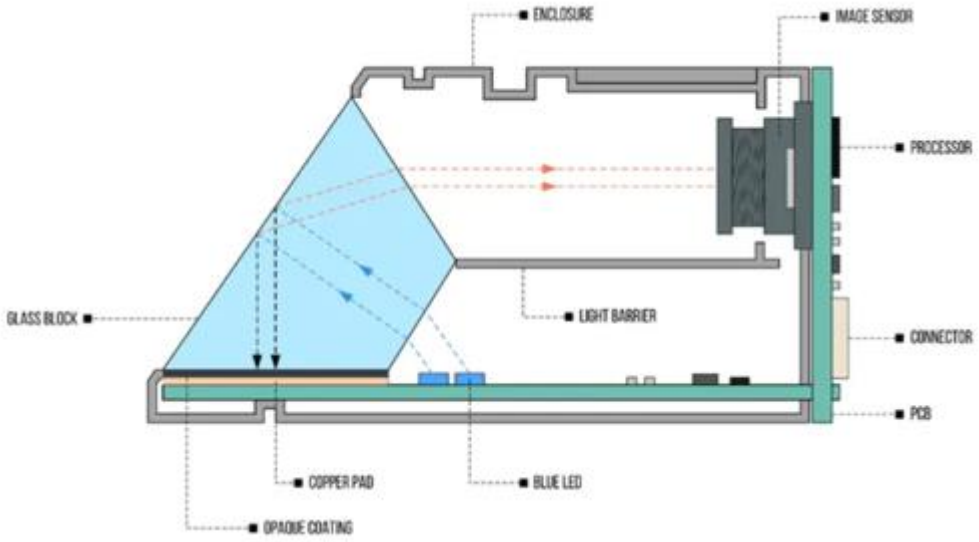


Рисунок 2.5 – Будова сенсору [30]

Рідкокристалічний символьний дисплей є типом екрану, який відображає текстову інформацію за допомогою символів і графічних символів. Він складається з матриці пікселів, де кожен символ представлений певним набором точок або "пікселів". Ці пікселі формують символи, які можуть бути відображені на екрані [31].

Цей тип дисплея зазвичай використовується для відображення простого тексту та графіки у вбудованих системах, промислових пристроях, а також у приладах споживчого призначення. Однією з його ключових особливостей є те,

що він може виводити обмежену кількість символів у кожному рядку, що робить його ідеальним для використання у пристроях з обмеженим простором екрану.

Щодо управління, рідкокристалічні символьні дисплеї дисплеї можуть працювати через різні інтерфейси зв'язку, такі як паралельний або послідовний, що дозволяє їм легко підключатися до мікроконтролерів або інших пристроїв. Вони зазвичай мають простий інтерфейс для виведення тексту та керування освітленням екрану.

Основними перевагами рідкокристалічн символьних дисплеїв є їх низька вартість, простота використання та надійність. Вони також мають досить невеликі розміри, що робить їх ідеальними для використання в пристроях з обмеженим простором. Однак їх можливості у відображенні графічної інформації обмежені, оскільки вони призначені переважно для виведення тексту.

Рідкокристалічн дисплей 16x2 є одним з найпоширеніших типів дисплеїв. Він складається з двох рядків, кожен з яких має по 16 прямокутних областей або символів для відображення текстової інформації. Кожен символ може бути відображений у вигляді 5x8 пікселів, що дозволяє відтворювати текст із 16 символів у кожному рядку [32].

Цей тип дисплея є дуже популярним у вбудованих системах, електронних пристроях і промислових застосуваннях через свою простоту використання та надійність. Він часто використовується для виведення статусних повідомлень, даних сенсорів, або будь-якої іншої інформації, яка може бути відображена у вигляді тексту.

Основні характеристики рідкокристалічн дисплея 16x2 включають його зручний розмір, простоту підключення до мікроконтролерів або інших пристроїв, а також низьку вартість. Його можна легко інтегрувати в різноманітні проекти завдяки великій підтримці бібліотек та простим інтерфейсам зв'язку.

Рідкокристалічний дисплей 16x2 має 16 контактів, які використовуються для підключення до мікроконтролера або іншого джерела живлення. Перший контакт, який знаходиться зліва, є контактом заземлення (GND), що забезпечує земляне підключення для дисплея. Другий контакт - це VCC, який приймає напругу живлення і зазвичай підключений до 5-вольтового вихідного контакту на платі Arduino або іншого мікроконтролера.

Наступний контакт, позначений як Vo, призначений для підключення потенціометра, який дозволяє регулювати контрастність дисплея. Це дозволяє налаштувати яскравість та чіткість відображення символів на екрані для оптимального комфорту при перегляді.

Інші контакти дисплея використовуються для підключення до мікроконтролера і передачі даних, управління підсвіткою та іншими функціями. Ці контакти дозволяють мікроконтролеру керувати виведенням тексту та графіки на дисплей, створюючи таким чином відповідний візуальний інтерфейс для користувача (рисунок 2.6).

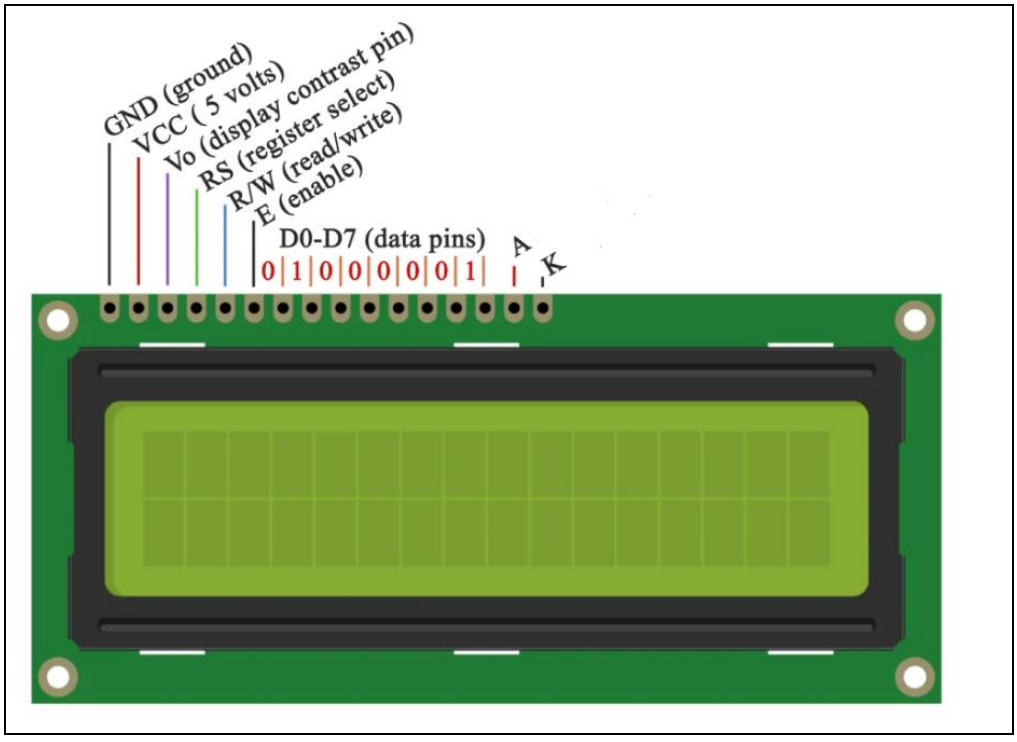


Рисунок 2.6 – Контакти дисплею [32]

Контакт RS або контакт вибору регістра визначає, чи надсилаються до РК-дисплея команди або дані. Коли контакт RS встановлено на низький рівень (нуль вольт), це означає, що ми надсилаємо команди на дисплей. Ці команди використовуються для управління діями дисплея, такими як переміщення курсора, очищення екрану або вмикання/вимикання дисплея.

У той час, якщо контакт RS встановлено на високий рівень (5 вольт), це означає, що ми надсилаємо дані або символи на дисплей. Ці дані відображаються на екрані як текст або графіка, що відображається користувачу.

Схема підключення дисплею зображена на рисунку 2.7

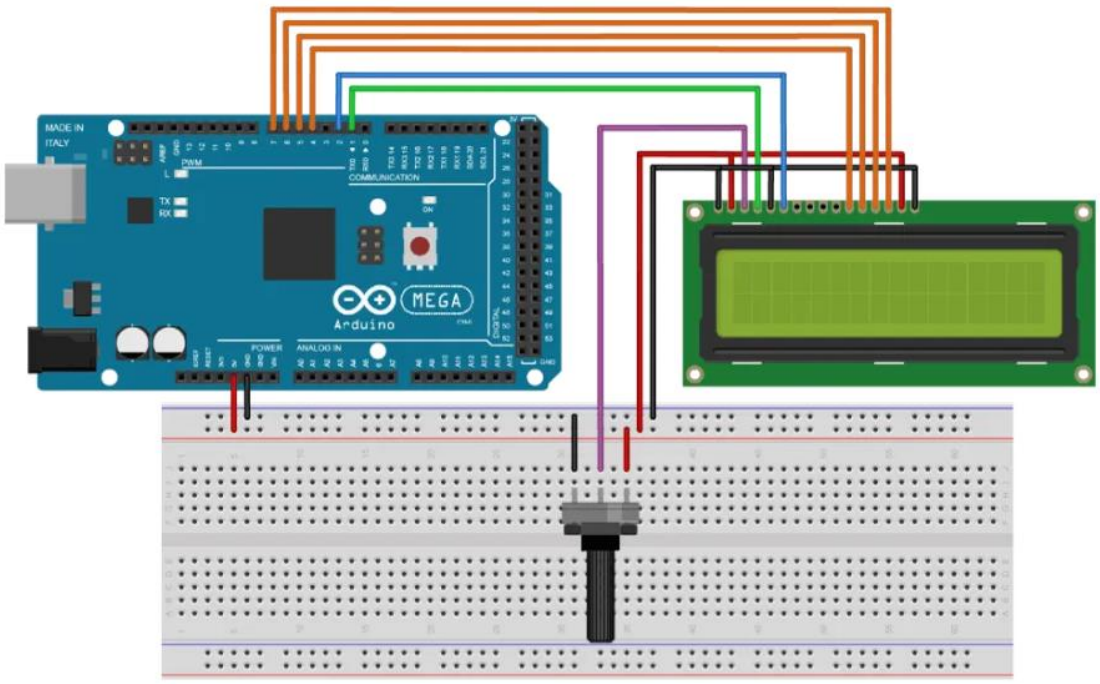


Рисунок 2.7 – Схема підключення дисплею [33]

Такий механізм вибору регістра дозволяє мікроконтролеру керувати виведенням різних типів інформації на РК-дисплей, надаючи йому можливість відображати як текстову інформацію, так і графічні символи за необхідності.

Дверний замок, який керується електромагнітним соленоїдом, може виконувати функцію застібки, що відкривається або зачиняється за допомогою електромагнітного поля (рисунок 2.8). Це може бути спеціально розроблене

кріплення для дверних замків, що робить його схожим на традиційний механічний замок, який керується ключем.

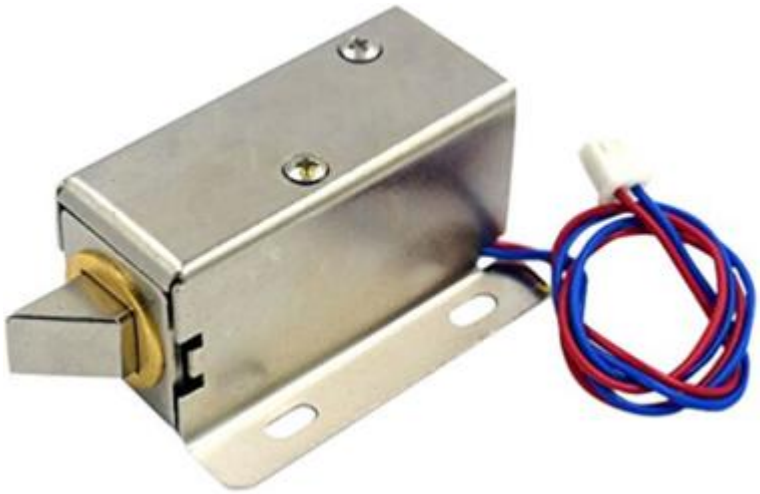


Рисунок 2.8 – Електромагнітний замок [34]

Функція соленоїда при використанні замка полягає в тому, щоб керувати механічним замком або засувкою. Соленоїд - це пристрій, що перетворює електричний сигнал в механічний рух. Коли соленоїд отримує електричний струм, він створює магнітне поле, що призводить до руху механічного стержня або штифта [34]. Цей рух може бути використаний для відкриття або закриття замка, залежно від його конструкції.

Основна різниця полягає в тому, що електромагнітний соленоїд додається до механічної конструкції замка, дозволяючи відкривати або закривати його за допомогою електричного сигналу. Це може бути виконано через альтернативне керування, таке як кнопка або ключовий перемикач.

Коли соленоїд активується, він створює магнітне поле, яке викликає переміщення застібки, що відкриває двері. Після деактивації соленоїда, застібка повертається до початкового положення, що дозволяє закрити двері.

Такий тип дверного замка може бути використаний для управління доступом у приміщення, де ручка буде утримуватися до тих пір, поки не буде активовано електричне керування або кнопка. Цей метод застосовується як для

внутрішніх, так і для зовнішніх дверей з метою забезпечення безпеки та контролювання доступу.

Коли на електромагніт подається живлення, струм, що проходить через нього, створює магнітний потік, що викликає притягнення пластини якоря до електромагніту. Це називається блокуючою дією електромагніту, і вона застосовується для закриття або блокування механізму дверного замка. Схема підключення навдена на рисунку 2.9.

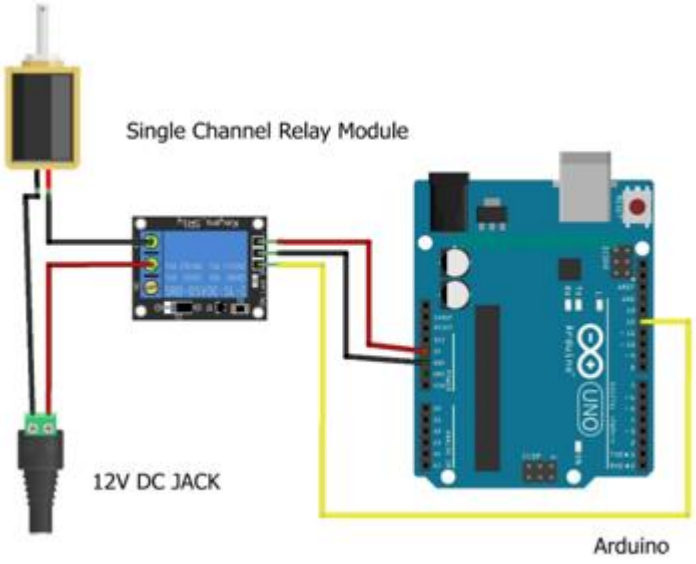


Рисунок 2.9 – Схема підключення [33]

Коли живлення електромагніта вимикається, магнітний потік перестає генеруватися, і пластина відпускається від електромагніту. Це називається відкриваючою дією електромагніту, і вона використовується для відкриття або розблокування механізму, такого як дверний замок.

Такий принцип роботи електромагніта дозволяє керувати рухом механізму, забезпечуючи можливість блокування та розблокування дверей, воріт, шаф та інших пристроїв у системах безпеки та управління доступом.

При виборі GSM-модулю для використання з Arduino, важливо звернути увагу на кілька ключових характеристик.

Спочатку, потрібно переконатися, що модуль сумісний з Arduino і має TTL-виходи, що узгоджуються з логікою та рівнями напруги Arduino. Це дозволяє легко підключати модуль та використовувати його у проекті.

Далі важливо врахувати підтримку GSM мереж. Модуль повинен працювати з мережами, які доступні у вашому регіоні, і підтримувати необхідні стандарти.

Функціональність модуля також важлива. Він повинен мати можливість надсилання та отримання SMS повідомлень, а також передачі даних через GSM мережу.

Обов'язково слід звернути увагу на інтерфейс зв'язку модуля з Arduino. Різні модулі можуть мати різні інтерфейси, такі як UART, SPI або I2C, і вибір залежить від вашої потреби та доступних портів на Arduino [36].

Нарешті, надійність і підтримка модуля також грають важливу роль. Важливо вибрати модель від надійного виробника з достатньою технічною підтримкою та документацією для спрощення розробки та вирішення можливих проблем.

Модуль A6 GSM вибирається для проектів з Arduino з декількох причин. По-перше, він має простий інтерфейс, який легко підключається до Arduino через UART, що спрощує використання для проектів, що потребують зв'язку через GSM мережу. Функціональність модуля також вражає: він підтримує надсилання та отримання SMS, передачу даних через GPRS і можливість здійснювати дзвінки [35, 36]. Завдяки широкій доступності на ринку, модуль A6 можна придбати в багатьох магазинах електроніки та інтернет-магазинах. Його вартість також є привабливою для багатьох, що робить його вигідним вибором для бюджетних проектів. Таким чином, модуль A6 GSM відмінно підходить для використання у проектах з Arduino завдяки своїй простоті, функціональності, доступності та вартості (рисунок 2.10).

Рисунок 2.10 – A6 GSM

Для підключення модуля A6 GSM до Arduino вам знадобиться з'єднати їх за допомогою UART-з'єднання. Ви можете використовувати три порти Arduino для цього: RX (прийом), TX (відправка) та GND (земля). Для під'єднання модуля A6 GSM до Arduino за допомогою методу послідовного зв'язку через цифрові контакти використовується бібліотека SoftwareSerial. Цей метод дозволяє використовувати будь-які цифрові контакти Arduino для зв'язку з модулем, навіть якщо вони не підтримують протокол UART за замовчуванням.

Для цього обрані контакти 9 і 10, які підтримують ШІМ на Arduino. Ці контакти будуть використовуватися для обміну даними з модулем A6. Щоб це зробити, ви можете підключити TX модуля A6 до піну 10 (вихідний сигнал), а RX - до піну 9 (вхідний сигнал) (рисунок 2.11).

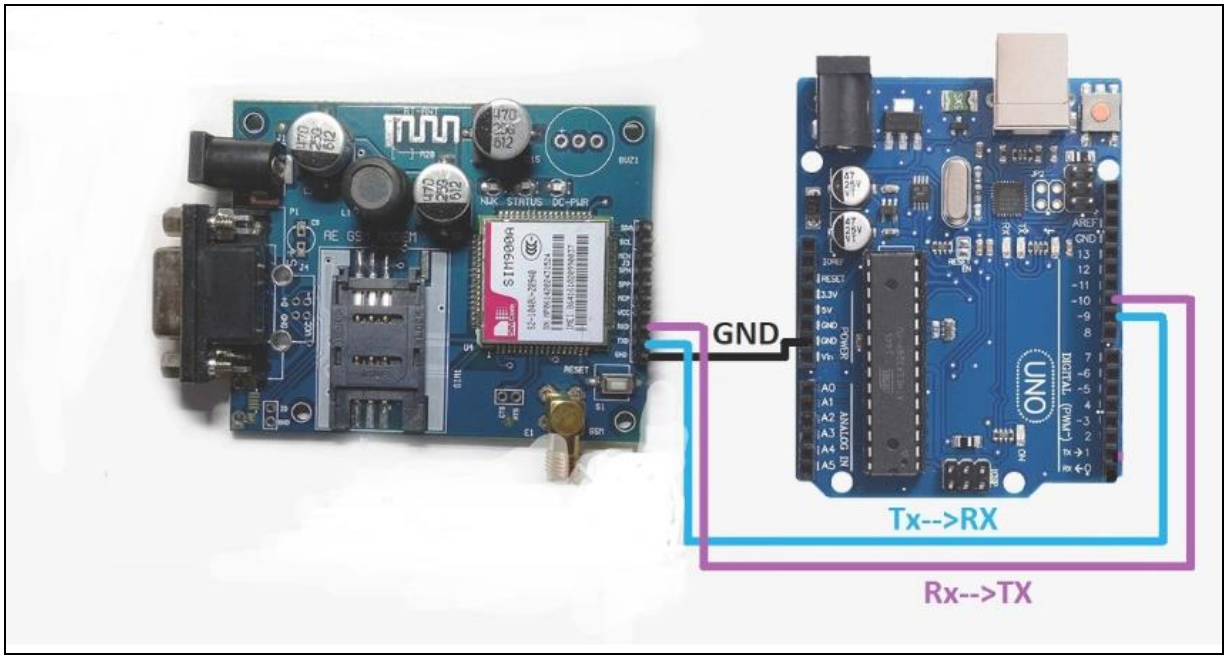


Рисунок 2.11 – Схема підключення A6 GSM [37]

Після налаштування з'єднання за допомогою SoftwareSerial Library ви зможете взаємодіяти з модулем A6 GSM через ці цифрові контакти Arduino [38]. Таким чином, ви зможете відправляти SMS, здійснювати дзвінки та працювати з GSM мережею, користуючись простотою та гнучкістю цього методу підключення.

2.4 Висновок

Розглянувши всі блоки та компоненти проекту, можна відзначити, що у кваліфікаційній роботі передбачено використання біометричного сканера відбитків пальців для ідентифікації особи, яка намагається отримати доступ до приміщення. Arduino виступає як центральний мікроконтролер, керуючи всією системою та взаємодіючи з іншими компонентами. Зчитувач відбитків пальців сканує відбитки пальців та забезпечує ідентифікацію особи.

Для відображення інформації про стан системи або повідомлень для користувача використовується рідкокристалічн символьний дисплей. Бузер слугує для аудіового сповіщення про стан системи або інші події.

GSM модуль відповідає за надсилання SMS-повідомлень адміністратору або виконання інших дій через мобільну мережу. Дверний замок, який може бути змонтований як електромагнітний соленоїд або реле, контролює відкриття та закриття дверей у відповідь на валідний вхід.

Додатково, можуть бути використані й інші компоненти, наприклад, датчики температури та вологості, для додаткового контролю або звітування про умови у приміщенні.

Усі ці компоненти працюють разом, створюючи комплексну систему контролювання доступу, яка забезпечує безпеку та зручність управління доступом до приміщення.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ПРИСТРОЮ

3.1 Проєктування схеми електричної функціональної

Електрична функціональна схема є ключовим етапом у розробці системи управління. Вона визначає роль кожного компонента та їх взаємозв'язок, розкриваючи природу процесів, що відбуваються у пристрої. Функціональна схема дозволяє відобразити функції окремих частин пристрою та встановити їх параметри.

Графічні позначення, використані на схемі, дозволяють зрозуміти елементи з'єднання та задати їх технічні характеристики. Важливо керуватися послідовністю функціональних процесів при побудові схеми.

Функціональні схеми пояснюють процеси у функціональних ланцюгах пристрою, використовуючи їх для вивчення принципів роботи та налагодження пристрою. Вони дозволяють більш детально розкрити функції компонентів та зв'язки між ними, що надає повнішу інформацію про роботу пристрою порівняно з принциповою схемою.

Така схема є важливим інструментом для розуміння та пояснення роботи пристрою, а також для його подальшого розвитку та вдосконалення.

Схема електрична структурна послужила основою для розробки електричної функціональної схеми, яка надана на рисунку 3.1 та у Додатку Б. На основі цієї функціональної схеми розкрито функціональні зв'язки між різними компонентами та їх роль у системі управління. Кожен елемент і підсистема отримали своє місце та функціональне призначення в контексті роботи пристрою в цілому.

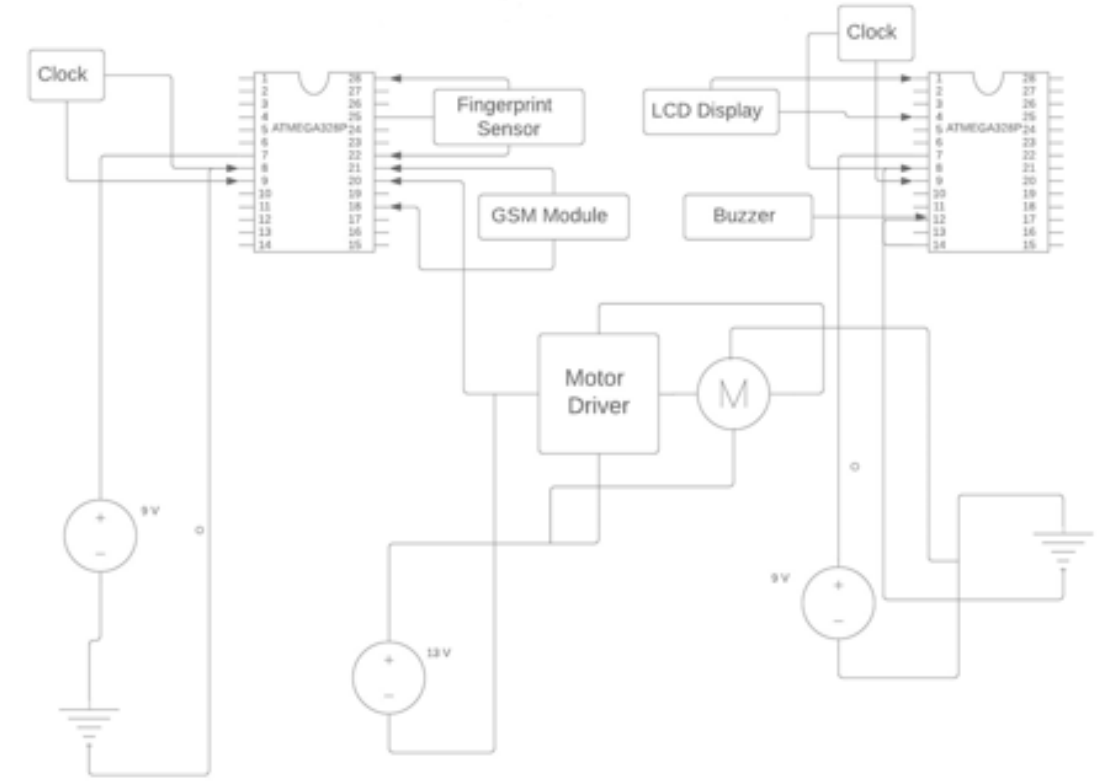


Рисунок 3.1 – Схема електрична функціональна

Мікроконтролер аналізує отримані дані та виконує відповідні дії, які були запрограмованіі над цими даними. ATmega328P має два входи живлення, які служать для різних функцій пристрою. Перший вхід, позначений як VCC, призначений для живлення цифрових логічних схем мікроконтролера. Другий вхід, позначений як AVCC, призначений для живлення аналого-цифрового перетворювача (АЦП).

Така подвійна система живлення дозволяє окремо керувати живленням цифрових і аналогових компонентів мікроконтролера. Це важливо для забезпечення стабільної роботи аналогових схем, таких як АЦП, які можуть бути чутливими до сплесків напруги в живленні.

Для коректної роботи мікроконтролера в обох режимах, рекомендується підключити обидва входи живлення до одного джерела напруги, але також можна використовувати різні джерела, якщо це потрібно для функціонування конкретної системи.

Розглянемо детальніше підключення основних елементів системи. Перш за все, для взаємодії з датчиком відбитків пальців, ми використовуємо мікроконтролер Atmega328P. Цей мікроконтролер відповідає за збір, обробку та передачу інформації від датчика до інших компонентів системи.

Датчик відбитків пальців підключається до мікроконтролера для зчитування відбитків пальців користувача. Використовуючи вбудовані алгоритми обробки, мікроконтролер аналізує зчитані дані і приймає рішення щодо доступу або блокування системи [39].

Для відображення інформації користувачеві та відображення стану системи використовується рідкокристалічний дисплей. Цей дисплей підключається до мікроконтролера та відображає необхідну інформацію, таку як результат сканування відбитку пальця або повідомлення про статус системи.

Для контролювання доступу до приміщення ми будемо використовувати електромагнітну засувку. Ця засувка підключена до керуючого мікроконтролера, який вмикатиме її у випадку успішної аутентифікації користувача за його відбитком пальця.

Також, для попередження про неправильні або спроби несанкціонованого доступу, у системі використовується бузер або звуковий сигналізатор, який підключається до мікроконтролера та спрацьовує у випадку невірного введення відбитка пальця.

Для надсилання повідомлень про події у системі, такі як спроби несанкціонованого доступу, використовується GSM-модуль. Цей модуль підключений до мікроконтролера та надсилає повідомлення на визначений номер у випадку спрацювання тривоги або інших важливих подій.

Ці елементи взаємодіють між собою, створюючи комплексну систему контролювання доступу, яка забезпечує безпеку та зручність управління доступом до приміщення.

Біометричний датчик відбитків пальців є ідеальним рішенням для створення системи доступу, що забезпечує високий рівень захисту за

допомогою аналізу відбитка пальця. Цей пристрій працює за послідовним протоколом, тому його можна легко інтегрувати з будь-яким мікроконтролером (наприклад, Arduino) або картою розробки.

Біометричний датчик може зберігати до 162 відбитків пальців у внутрішній флеш-пам'яті. Індикатор світлодіода пристрою загоряється кожного разу, коли датчик знімає відбитки пальців, що полегшує процес реєстрації та використання [40].

Датчик відбитків пальців, який ми використовуємо, є оптичним типом. Існують також ємнісні та ультразвукові типи датчиків, але вони дорожчі і менш поширені. Оптичний датчик працює за принципом знімку відбитку пальців, після чого використовується спеціальний алгоритм для порівняння зі збереженими даними та визначення відповідності.

Батареї на дев'ять вольт зазвичай використовуються в пристроях, де потрібна велика енергія і стабільна робота протягом тривалого часу. Їх можна знайти в різних пристроях домашнього та професійного використання, таких як електронні іграшки, вимірювальні прилади, акустичні системи та інші електронні пристрої, які потребують надійного джерела живлення.

3.2 Проєктування схеми електричної принципової

Принципова схема є ключовим етапом у розробці будь-якого електричного пристрою. Вона представляє собою повну електричну схему пристрою, яка включає всі необхідні елементи та з'єднання між ними.

На схемі використовуються різні типи елементів, такі як інтегральні схеми різного рівня інтеграції, дискретні елементи та з'єднувальні компоненти. Графічні позначення на схемі дозволяють ідентифікувати кожен елемент та з'єднання між ними.

Принципова схема дозволяє розкрити всі аспекти роботи пристрою та встановити взаємозв'язки між його складовими частинами. Це важливий інструмент для розуміння та аналізу роботи пристрою, а також для подальшої розробки та вдосконалення.

Використання принципової схеми дозволяє розробникам створювати індивідуальні схеми підключення та вузли з'єднання, що відповідають конкретним потребам проекту. Це дозволяє оптимізувати роботу системи, забезпечуючи оптимальний рівень функціональності та надійності.

Схема електрична принципова, наведена на рисунку 3.2 та в додатку Б, є ключовим інструментом у розробці та аналізі проекту. Вона дозволяє отримати повне уявлення про електричні зв'язки та взаємодію компонентів системи.

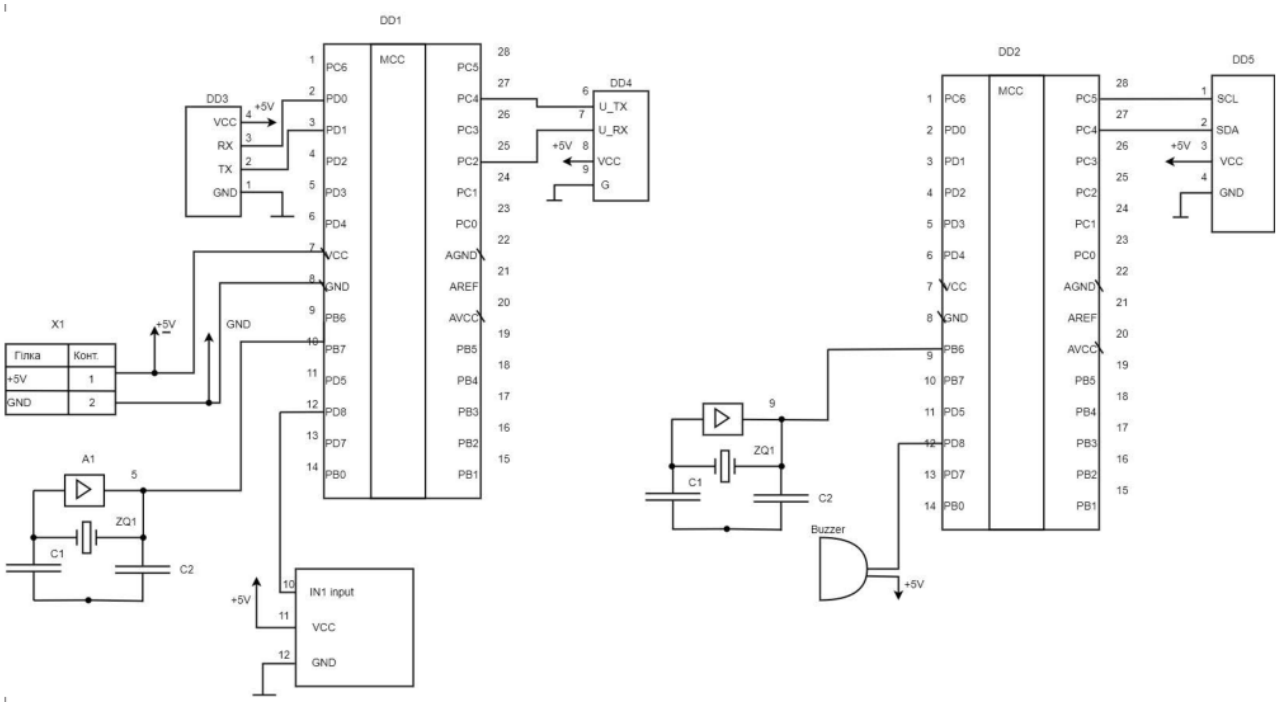


Рисунок 3.2 – Схема електрична принципова

Вихід датчика підключається до цифрового входу мікроконтролера, Деякі датчики можуть вимагати підключення до аналогового входу для зчитування відбитків пальців.

Схема підключення давача відбитків пальців до Arduino наведена на рисунку 3.3.

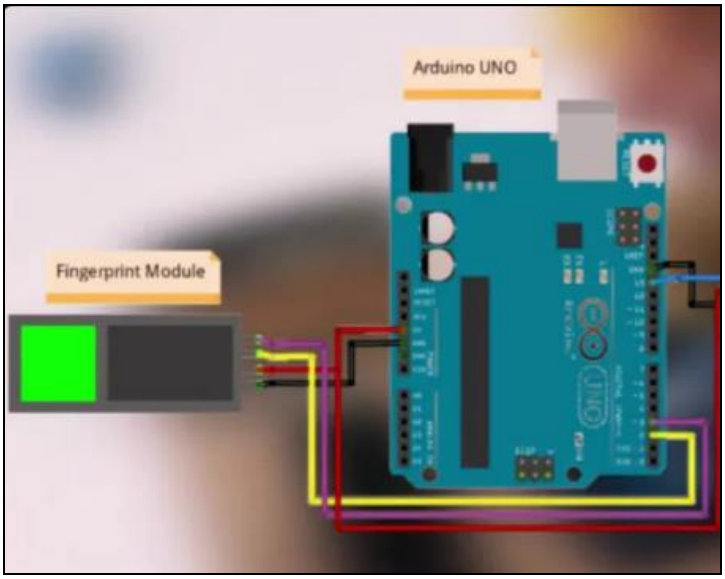


Рисунок 3.3 – Схема підключення сенсора [41]

Підключаємо сенсор відбитку пальця згідно таблиці 3.1.

Таблиця 3.1- Контакти з’єднання сенсора відбитків пальців та Arduino

Сенсор відбитка пальця	Arduino Atmega328P
VCC	5V
GND	GND
RX	Pin2
TX	Pin3

Зазвичай, для підключення датчика відбитків пальців до Arduino використовуються цифрові виходи для передачі та прийому даних. При підключенні датчика важливо дотримуватися правильної полярності та правильного підключення кожного проводу до відповідного входу або виходу Arduino (рисунок 3.4).

Результат роботи системи, яка використовує датчик відбитків пальців, може бути відображений на РК-дисплеї або переданий через GSM-модуль для віддаленого моніторингу або керування.

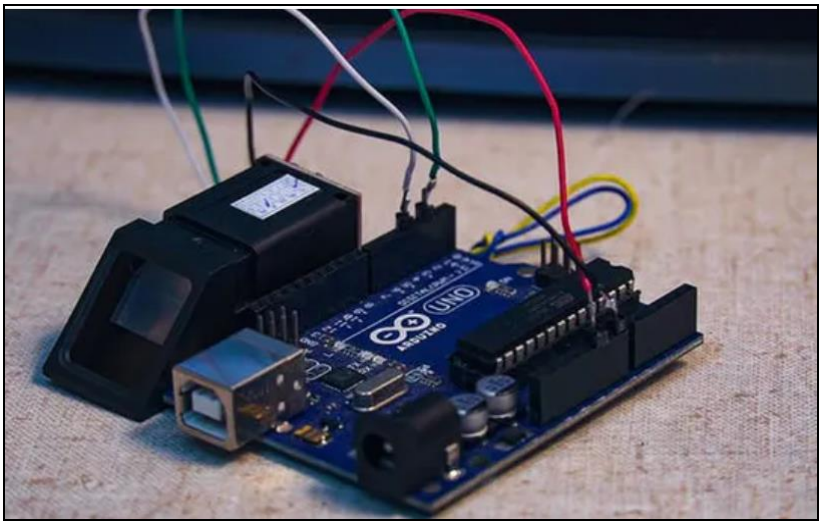


Рисунок 3.4 - Підключення сканера відбитків пальців

Різні кольори допоможуть легко ідентифікувати кожен з'єднувальний провід та спростять підключення. Наступні кольори рекомендовано використовувати для кожної функції:

– DNC (Do Not Connect) - білий провід;

– TX (Вихід даних) - синій провід;

– VCC (Живлення) - червоний провід;

– Земля (GND) - чорний провід.

– RX (Вхід даних) - зелений провід.

Далі підключаємо рідкокристалічний дисплей. Детальні вимоги до з’єднань показано в табличці 3.2

Таблиця 3.2 - Контакти з’єднання дисплею та Arduino

Дисплей	Arduino Atmega328P
SDA	A4
SCL	A5
VCC	5V
GND	GND

Для управління дверним замком з використанням біометричних технологій, дійсно потрібно стабільне джерело живлення. Використання трьох акумуляторних елементів 18650 є розумним рішенням, оскільки ці батареї мають високу ємність і здатні забезпечити необхідний діапазон напруги від 7 до 12 вольт.

Кожен елемент 18650 має номінальну напругу 3.7 В і максимальну напругу близько 4.2 В, коли повністю заряджений. Три елементи в серії забезпечують загальну напругу від 11.1В до 12.6 В. Це ідеально підходить для більшості електронних замків, які потребують напруги в межах 7-12 В.

Схема підключення рідкокристалічного дисплею зображена на рисунку 3.5

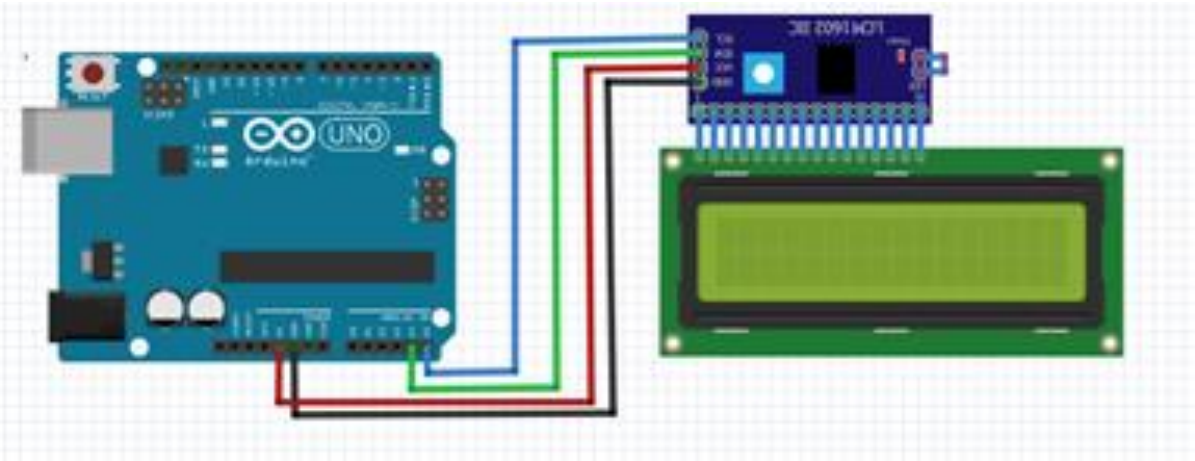


Рисунок 3.5 Схема підключення рідкокристалічного дисплею [41]

Підключення електромагнітного дверного замка до Arduino дозволяє створити систему контролю доступу з використанням різних методів аутентифікації, таких як RFID, клавіатура, біометрія тощо [42]. Для підєднання електромагнітного замка необхідно з’єднати контакт Arduino на 5В та контакт VCC модуля реле. Пієднати контакт GND модуля реле GND Arduino до контакту. Приєднати контакт IN модуля та цифовий контакт 12 Arduino, як показано на рисунку.

Також необхідно з’єднати плюсовий провід блоку живлення постійного струму до одного контакту модуля реле, а мінусовий контакт до

електромагнітного замка, як показано на схемі. Потім підключіть плюсовий провід електромагнітного замка до іншого контакту модуля реле. Після цього завантажте код на Arduino.

GPRS-модуль A6 - це компактний комунікаційний модуль, який підтримує GPRS та GSM-зв'язок. Модуль працює в різних діапазонах (850 / 900 / 1800 / 1900 МГц), що дозволяє використовувати його в будь-яких мережах. Підтримка передачі даних включає GPRS Class 10, що забезпечує максимальну швидкість передачі даних до 85,6 Кбіт/с.

Модуль A6 використовує протоколи HTTP та TCP/IP для передачі даних через Інтернет. Це робить його придатним для використання в різних проектах IoT (інтернету речей) [42]. Зв'язок з контролером здійснюється через UART (послідовний) інтерфейс, що дозволяє легко інтегрувати модуль з Arduino.

Модуль A6 споживає до 500 мА під час передачі даних, і близько 5 мА в режимі очікування.

Фізичні розміри модуля компактні, що дозволяє використовувати його в проектах з обмеженим простором. Модуль має роз'єм для підключення антени, що забезпечує стабільний сигнал навіть в умовах поганого покриття мережі. Крім того, модуль підтримує підтримує команди, включаючи GSM 07.07, GSM 07.05, та AT-команди для конфігурації та управління зв'язком, що полегшує його програмування та інтеграцію в різні проекти.

Завдяки технології енергозбереження споживаний струм у сплячому режимі становить всього 3 мА.

Підключення та керування GPRS модулем A6 з Arduino вимагає правильного з'єднання компонентів та написання відповідного коду для обміну даними.

Ми підключили його до контролера Arduino наступним чином: для початку підключив піни U_TxD та U_RxD на модулі до пінів 2 і 4 на Arduino. Далі потрібно підключити пін VCC на модулі до піну VCC на Arduino і так само з’єднати контакти GND. Далі потрібно вставити активовану картку Micro

SIM в роз’єм і підключити антену. Інформація про підключення наведена у таблиці 3.3.

Таблиця 3.3 - Підключення Arduino I GSP-модуля

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

Використовуючи макетну плату, прикріплену до основи корпусу було зібрано пристрій. Вигляд остаточного прототипу можна побачити на рисунку 3.6.

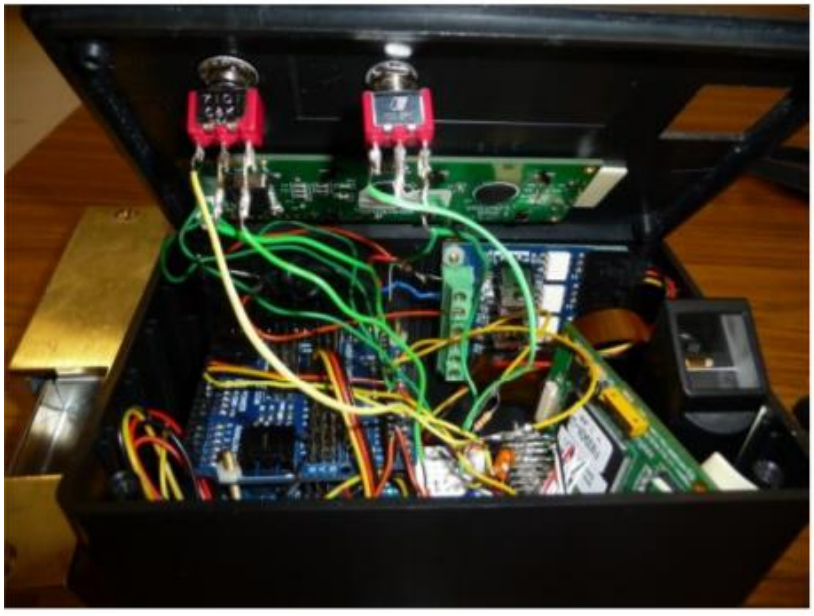


Рисунок 3.6 – Внутрішній вигляд корпусу

На макетній платі було розміщено всі необхідні компоненти, включаючи Arduino, GPRS модуль A6, джерело живлення та з'єднувальні дроти. Всі з'єднання були виконані відповідно до схеми, щоб забезпечити коректну роботу пристрою.

Arduino було підключено до GPRS модуля через серійний інтерфейс, використовуючи пін 7 для прийому даних (RX) та пін 8 для передачі даних (TX). Електромагнітний замок був підключений до модуля реле, що дозволяє Arduino контролювати його увімкнення та вимкнення.

Після завершення збірки пристрій був протестований для перевірки коректності всіх з'єднань та роботи програмного забезпечення. Завантажений на Arduino код дозволяв керувати замком та обмінюватися даними з GPRS модулем, забезпечуючи віддалений контроль доступу.

3.3 Алгоритм роботи системи

Алгоритм роботи пристрою починається з подачі живлення на всі компоненти. Після цього Arduino ініціалізує серійний зв'язок з GPRS модулем A6, встановлюючи швидкість передачі даних. Модуль A6 перевіряє наявність мережевого сигналу та підключається до мережі за допомогою SIM-карти.

Коли система готова до роботи, Arduino відправляє AT-команди до GPRS модуля для налаштування з'єднання. Якщо модуль успішно відповідає на команди, Arduino переходить до основного циклу роботи.

Для реєстрації відбитків пальців в системі контролю доступу з використанням біометричного датчика та Arduino, необхідно виконати кілька кроків: підключити біометричний датчик до Arduino, написати код для зчитування та зберігання відбитків пальців, а також налаштувати систему для розпізнавання зареєстрованих відбитків.

Для налаштування системи розпізнавання зареєстрованих відбитків пальців, спочатку необхідно зберегти зареєстровані відбитки пальців разом з їх унікальними ідентифікаторами в пам'яті датчика.

Коли приходить команда на відкриття або закриття замка, Arduino обробляє її та керує модулем реле. Реле, у свою чергу, підключає або відключає

електромагнітний замок від джерела живлення, змушуючи його відкриватися або закриватися (рисунок 3.7).

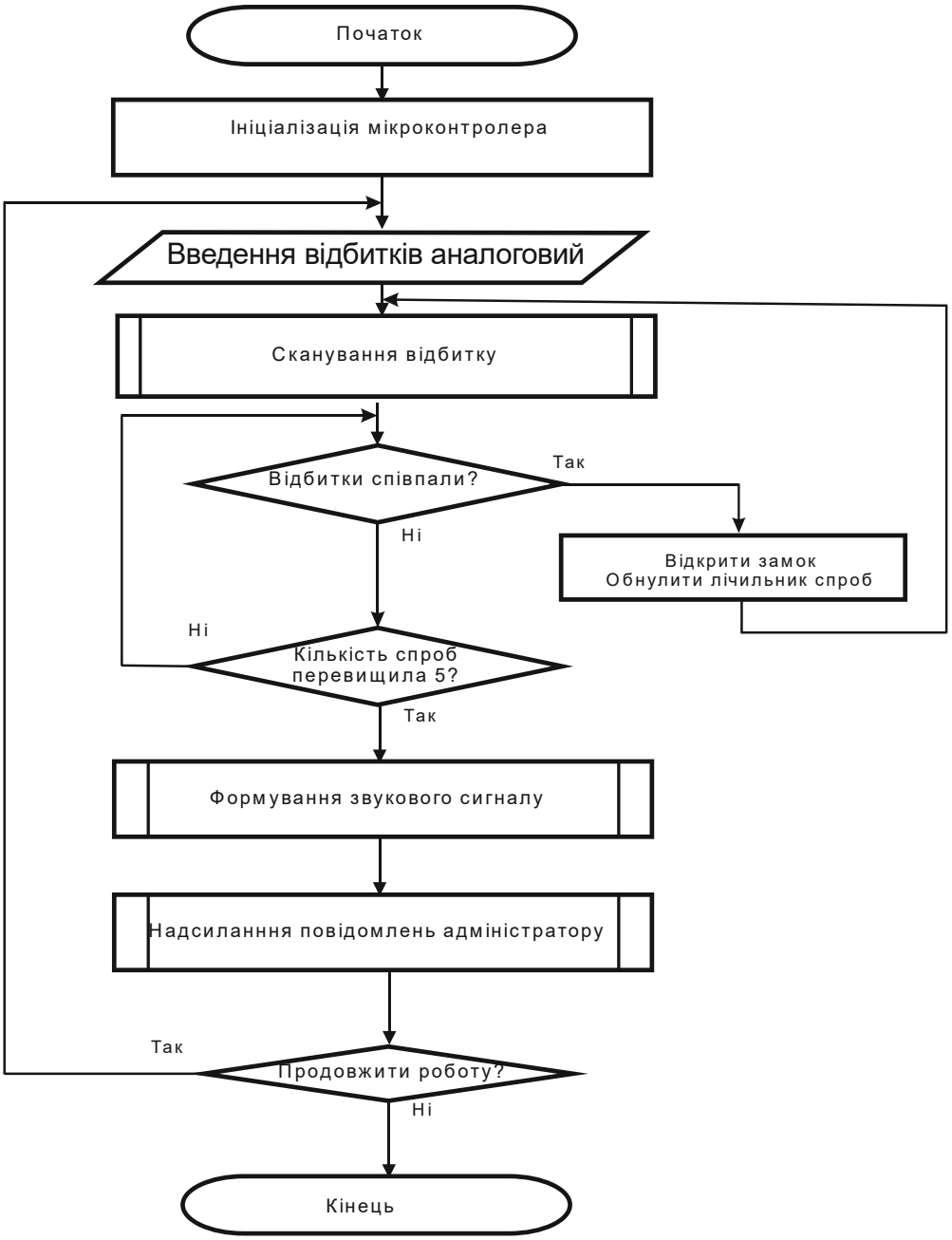


Рисунок 3.7 – Алгоритм роботи системи

У даній системі, коли користувач вводить свій відбиток пальця у сканер відбитків, який з'єднаний з дверною засувкою через мікроконтролер, система перевіряє цей відбиток у своїй базі даних. Якщо відповідний відбиток

знайдено, засувка відкривається, а двері дозволяються пройти. Те ж саме відбувається, коли користувач бажає заблокувати двері: правильний відбиток пальця приводить до того, що засувка закривається, запираючи двері.

У випадку, якщо поданий відбиток пальця не правильний, система генерує звуковий сигнал та виводить повідомлення на РК-дисплеї "Спробуйте ще раз". Якщо зловмисник намагається безперервно проникнути всередину і надає 5 або більше неправильних відбитків, система переходить у захищений режим. У цьому режимі вона активує тривожний сигнал та виводить повідомлення "Режим паніки" на дисплеї. Власнику надходить повідомлення про спробу злому через GSM-модуль.

Ця система забезпечує надійний контроль доступу та повідомляє про спроби несанкціонованого доступу, забезпечуючи безпеку та захист об'єкта.

Таким чином, пристрій забезпечує безперервний контроль доступу, реагуючи на команди користувача та відправляючи звіт про стан замка.

Під час роботи пристрою Arduino постійно моніторить стан з'єднання з GPRS модулем та відправляє дані про стан замка власнику. У випадку втрати зв'язку, Arduino автоматично намагається відновити підключення.

3.4 Програмна реалізація

Arduino Integrated Development Environment (IDE) - це інтегроване середовище розробки, призначене для програмування мікроконтролерів Arduino [43]. Ось опис цього середовища без використання списків:

Arduino IDE - це спеціальна програма, яка надає зручний інтерфейс для написання, компіляції та завантаження програмного коду на платформу Arduino. Вона працює на різних операційних системах, таких як Windows, macOS та Linux.

Arduino IDE - це потужний інструмент для розробки вбудованого програмного забезпечення для платформи Arduino. Він надає зручність та простоту використання, що робить його популярним серед початківців та досвідчених розробників одночасно.

У цьому проєкті використовується бібліотека SoftwareSerial для встановлення серійного зв'язку через будь-які цифрові піни Arduino. SoftwareSerial - це бібліотека для Arduino, яка дозволяє створювати додаткові послідовні порти за допомогою програмного забезпечення. Вона дозволяє вам зв'язувати Arduino з іншими пристроями через UART, коли апаратний послідовний порт вже використовується або відсутній на вашій платі.

Ця бібліотека дозволяє створювати додаткові послідовні порти на будь-яких цифрових входах/виходах Arduino. Ви можете налаштувати ці порти для зчитування та передачі даних через UART, що робить їх корисними для зв'язку з іншими мікроконтролерами, сенсорами або модулями.

Хоча SoftwareSerial має обмеження щодо швидкості передачі даних та часу відповіді, вона є корисним інструментом для взаємодії з пристроями, якщо апаратні послідовні порти недоступні або вже використовуються для інших завдань.

У функції setup() відкривається серійна комунікація з ПК і з модулем GPRS, після чого відправляється AT команда для перевірки зв'язку з модулем. У функції loop() дані, що надходять від ПК, передаються до модуля GPRS, і навпаки. Це дозволяє налагодити зв'язок між Arduino та GPRS модулем A6 і передавати команди та дані між ними.

Для ефективної роботи рідкокристалічного дисплею використовується LiquidCrystal.h - це бібліотека в Arduino IDE, яка дозволяє керувати символьними LCD-дисплеями з рідкою кристалічною підсвіткою [44]. Ця бібліотека дозволяє виводити текст, цифри та інші символи на LCD-дисплей, керувати позицією курсора та налаштовувати параметри відображення, такі як контрастність та підсвічування.

Після цього встановлюємо бібліотеку Adafruit's Fingerprint в Arduino IDE, натиснувши на "Sketch", "Include Library", далі "Manage Libraries..." та встановивши потрібну бібліотеку.

Потім відкриємо приклад програми для біометричного сканера відбитків пальців у Arduino IDE, знаходячись в "File", "Examples", "Adafruit Fingerprint", "enroll". У цьому прикладі ми бачимо код для реєстрації відбитків пальців.

Внесемо зміни до коду, щоб налаштувати кількість та спосіб реєстрації відбитків пальців, враховуючи ваші потреби.

Після внесення змін скомпілюэмо код та завантажимо його на наш контролер Arduino.

Запускаємо програму на Arduino та слідуємо інструкціям у консолі або на дисплеї, щоб зареєструвати відбитки пальців. Обераємо ідентифікатор пальця та слідуємо інструкціям щодо кількості та способу реєстрації.

Вас попросять два рази прикласти той самий палець до сенсора. Якщо відбитки збігаються, то реєстрація пройшла успішно.

Перевіряємо реєстрацію, використовуючи приклади програми для перевірки реєстрації відбитків. Для цього перевіряємо, чи вдалося зберегти відбитки пальців у EPROM сенсорного модуля.

Ці кроки допоможуть нам успішно зареєструвати відбитки пальців у вашому біометричному сканері відбитків пальців за допомогою бібліотеки Adafruit's Fingerprint в Arduino IDE.

Бібліотека Servo.h в Arduino IDE призначена для керування сервоприводами [45]. Вона дозволяє легко керувати положенням сервоприводів, що використовуються для рухомих механізмів, наприклад, в моделях або роботах. Завдяки цій бібліотеці можна задавати кут повороту сервопривода і контролювати швидкість руху.

Програмний код наведено в додатку Б.

3.5 Висновок

Проеєт включає в себе компоненти апаратного та програмного забезпечення, такі як сканер відбитків пальців, мікроконтролер Arduino, електромагнітний дверний замок, LCD-дисплей та звуковий сигналізатор.

Система працює наступним чином: користувач вводить свій відбиток пальця в сканер, який перевіряє його у базі даних. Якщо відбиток знайдено і він відповідає, двері відкриваються. У випадку невідповідності або неправильного введення, система виводить повідомлення на дисплей та активує звуковий сигнал. Крім того, система має захист від зламу: при спробі неправильного введення відбитка пальця п'ять або більше разів підряд, система переходить у захищений режим і повідомляє власника про можливий злам.

Завдяки використанню Arduino та відповідних бібліотек, проект стає доступним для реалізації навіть для початківців у світі робототехніки. Він може бути застосований у різних сферах, від офісів та домашніх установок до комерційних приміщень та об'єктів зі зберіганням даних або цінних речей. Розроблений проект демонструє можливості сучасних систем безпеки, забезпечуючи ефективний та зручний механізм контролювання доступу.

ВИСНОВКИ

У ході виконання даного проекту були проведені наступні етапи: теоретичний аналіз основ проблеми, вивчення предметної області з метою виявлення існуючих проблем і завдань, порівняльний аналіз переваг і недоліків існуючих рішень, а також дослідження різних методологічних підходів для вирішення поставленої задачі.

Це дозволило чітко визначити основні кроки для реалізації проекту з побудови розумного замка зі сканером відбитків пальців та обрати найбільш підходящі методи для підключення компонентів між собою для створення готового пристрою. Дане дослідження допоможе уникнути критичних помилок у проекті та виявити їх, якщо вони виникнуть під час експлуатації розумного замка.

Попередні дослідження стали важливим етапом у конструюванні замка з використанням сканера відбитків пальців. На наступних етапах була розроблена схема з'єднання компонентів дверного замка, а також моделювання підключення елементів допомогло у віртуальній перевірці їх взаємодії. Оцінка вартості всіх необхідних компонентів дозволила визначити, що пристрій є відносно доступним у реалізації.

У підсумку, розроблений проект є комплексною системою контролю доступу, яка використовує сканер відбитків пальців для ідентифікації користувачів. Проект включає в себе теоретичний аналіз, вивчення предметної області, порівняльний аналіз існуючих рішень, а також дослідження методологічних підходів.

Результатом цих досліджень є реалізація розумного замка зі сканером відбитків пальців, який забезпечує надійний контроль доступу та безпеку. Проект передбачає виявлення та вирішення можливих проблем ще на етапі розробки, що дозволяє уникнути критичних помилок у майбутньому.

Використання Arduino та відповідних бібліотек робить проект доступним для реалізації навіть для початківців, а його можливе застосування розширюється від домашнього використання до комерційних об'єктів.

Розроблений проект вирішує актуальну задачу контролю доступу за допомогою інноваційних технологій, що дозволяє забезпечити високий рівень безпеки та зручності використання.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. A. Jain and S. Pankanti, “Fingerprint Classification and Matching” Handbook for Image and Video Processing, A. Bovik (ed.), Academic Press, April 2013.

2. ДСТУ 4000-2000 Системи тривожної сигналізації охоронні теле(відео) системи і системи контролювання доступу. Терміни та визначення URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=27277 (дата звернення: 22.05.2024)

3. Romanowich J., Chin D., Lento T. Smart Video Security Handbook: A Practical Guide for Catching Intruders Before They Act. New York: McGraw-Hill, 2020. 240 c.

4. A. C. Losada-Gutiérrez. Smart Video Surveillance System Based on Edge Computing. 2021. C. 2958-2975.

5. Проєктування комплексних систем захисту інформації: підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.

6. Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка, П. М. Шпатар - Чернівці: Чернівецький національний університет, 2018. - 252 с

7. Fundamentals of InformationSystems Security / Editors : David Kim, Michael G. Solomon. – Burlington, Massachusetts : Jones & Bartlett Learning, 2018. – 548 p.

8. Anil K. Jain, Jianjiang Feng and Karthik Nandakumar, "Matching Fingerprints", IEEE Computer, vol. 43, no. 2, pp. 36-44, 2019.

9. Блог Allo URL: https://blog.allo.ua/ua/rozumni-dverni-zamki-shho-tse-take-ta-yak-vibrati (дата звернення: 13.03.24)

10. 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.

11. 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.

12. Смарт замок TTLOCK BOSS URL: https://locksmith.com.ua/product/ttlock-boss-uk/ (дата звернення: 15.03.24)

13. Сканер відбитків пальців ZK8500R URL: https://zktecoua.com/ua/products/scanner-zkteco-zk8500r/ (дата звернення: 15.03.24)

14. ZKTeco URL: https://zktecoua.com/ua/products/ (дата звернення: 14.03.24)

15. Контроль доступа URL: https://diviks.com.ua/ua/kontrol-dostupa.html (дата звернення: 17.03.24)

16. ZKTeco Technology URL: https:// https://zkteco.technology/ (дата звернення: 18.03.24)

17. Камери і об’єктиви для мікрокомп’ютерів | Raspberry Pi | Arduino. 2021. URL: https://botland.com.ua/uk/14-kamery-i-ob-yektyvy-dlya-mikrokompyuteriv (дата звернення: 19.02.2024)

18. S. S. Patil, S.S. Kulkarni. Raspberry Pi Based Smart Surveillance System. 2018. URL: https://www.ijircce.com/upload/2018/march/181_Raspberry.pdf (дата звернення: 22.02.2024)

19. Cyber Security for Cyber Physical Systems / Saqib Ali, Taiseera Al Balushi, Zia Nadir, Omar Khadeer Hussain. – Cham, Switzerland : Springer, 2018. – 174 p.

20. Мікроконтролер ATMEGA328P URL: https://arduino.ua/prod15-mikrokontroller-atmega328p (дата звернення: 21.03.2024)

21. Мікроконтролер ATMEGA328P-PU із завантажувачем Arduino Uno URL: https://www.mini-tech.com.ua/ua/atmega328p-pu-s-zagruzchikom-arduino-uno (дата звернення: 24.03.2024)

22. Connect multiple Arduinos to one computer URL: https://www.hackster.io/Zigster/connect-multiple-arduinos-to-one-computer-5a0722 (дата звернення: 25.03.2024)

23. Паламар М.І., Стрембіцький М.О., Паламар А.М. Проектування комп’ютеризованих вимірювальних систем та комплексів. Навчальний посібник. Тернопіль: ТНТУ. 2019. 150 с.

24. Глобальна система мобільного зв'язку URL: https://uk.wikipedia.org/wiki/GSM (дата звернення: 25.03.2024)

25. Датчики і приводи в IoT – забезпечення промислової автоматизації URL: https://www.telesphera.net/blog/datchiki–i–privodi–v–iot.html (дата звернення: 18.05.2024)

26. Відеоспостереження та системи відеонагляду: захист і безпека 24/7 від VidiMost. 2020 URL: https://vidimost.com.ua/ (дата звернення: 16.02.2024)

27. 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.

28. Сканер відбитків пальців R307 URL: http://www.kosmodrom.com.ua/el.php?name=R307-FRS (дата звернення: 16.02.2024)

29. Сканери відбитків пальців та id-паспортів URL: https://expertsolution.com.ua/uk/equipments/skaneri/ (дата звернення: 15.04.2024)

30. HIGH-QUALITY FINGERPRINT ACQUISITION URL: https://mantraidentity.com/Authentication-Scanner/Fingerprint-Scanner-MFS500 (дата звернення: 16.04.2024)

31. Safeguarding the Information Systems in an Organization through Different Technologies, Policies, and Actions/ Hend K. Alkahtani. – Computer and Information Science. – Vol. 12, No. 2; 2019. – Published by Canadian Center of Science and Education. – P. 117-125.

32. LCD 1602 символьний дісплей 16x2 URL: https://arduino.ua/prod169-lcd-1602-simvolnii-displei-16x2-sinii (дата звернення: 18.04.2024)

33. 6 Simple Arduino UNO Projects URL: https://encrypted-tbn2.gstatic.com/images?q=tbn:ANd9GcTsAHMSxiLI8l0UHyTXf0GmJeBtNj-N8PcEwWi_8VTBU2xG8ISO (дата звернення: 18.04.2024).

34. Електрозасувки URL: https://ualock.com.ua/ua/g2413400-elektrozaschelki (дата звернення: 18.04.2024)

35. GSM/GPRS Модуль A6 Pro URL: https://ardushop.in.ua/arduino/gsm-gprs-module-a6-pro (дата звернення: 19.04.2024)

36. Модуль GSM A6 mini GPRS/GSM URL: https://www.mini-tech.com.ua/ua/gsm-gprs-module-a6 (дата звернення: 21.04.2024)

37. Send and Receive SMS with Sim900 & Arduino URL: https://www.ee-diary.com/2021/09/send-and-receive-sms-with-sim900-arduino.html (дата звернення: 21.04.2024)

38. SoftwareSerial Library URL: https://www.arduino.cc/en/Reference/softwareSerial (дата звернення: 22.04.2024)

39. 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.

40. R307 Optical Fingerprint Reader Sensor Module Good Quality URL: https://techiesms.com/product/r307-optical-fingerprint-reader/ (дата звернення: 22.04.2024)

41. Проєкти на Arduino URL: https://habr.com/ru/sandbox/115592/ (дата звернення: 28.04.2024)

42. Бездротовий інтернет – що це таке, види, швидкість URL: https://mobitech.com.ua/ua/articles/besprovodnoi–internet (дата звернення: 22.05.2024)

43. Arduino Integrated Development Environment (IDE) v1 URL: https://www.arduino.cc/en/Guide/Environment (дата звернення: 24.05.2024)

44. LiquidCrystal URL: https://doc.arduino.ua/ru/prog/LiquidCrystal (дата звернення: 24.05.2024)

45. Servo URL: https://www.arduino.cc/en/reference/servo (дата звернення: 25.05.2024)

ДОДАТОК А

(обов'язковий)

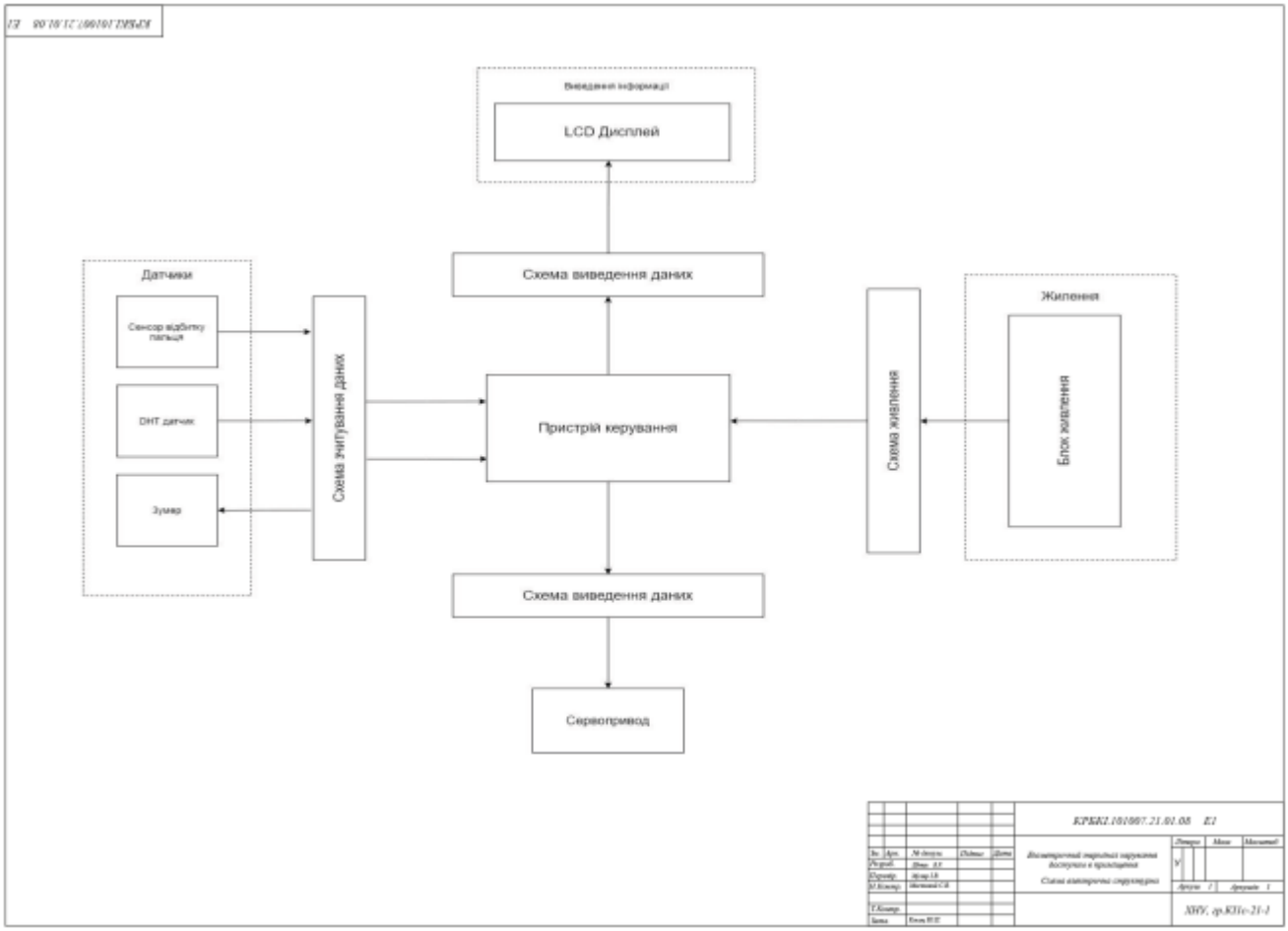
Код програми для Arduino

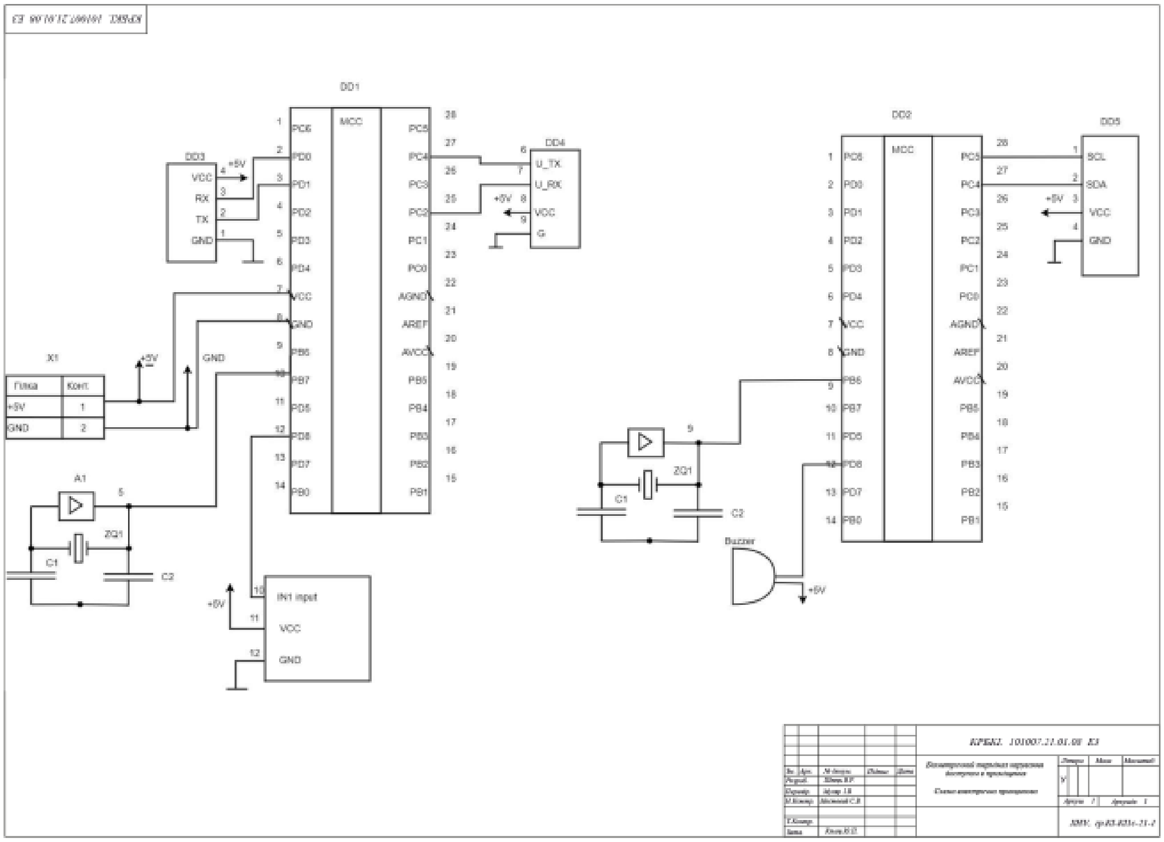
```
#include "dht.h"
#define dht_apin 2 // Analog Pin sensor is connected to
dht DHT;
#include<LiquidCrystal.h>
LiquidCrystal lcd(13,12,6,7,9,8);
#include <SoftwareSerial.h>
SoftwareSerial fingerPrint(10, 11);
#include<Servo.h>
Servo myServo;

#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);

}
```

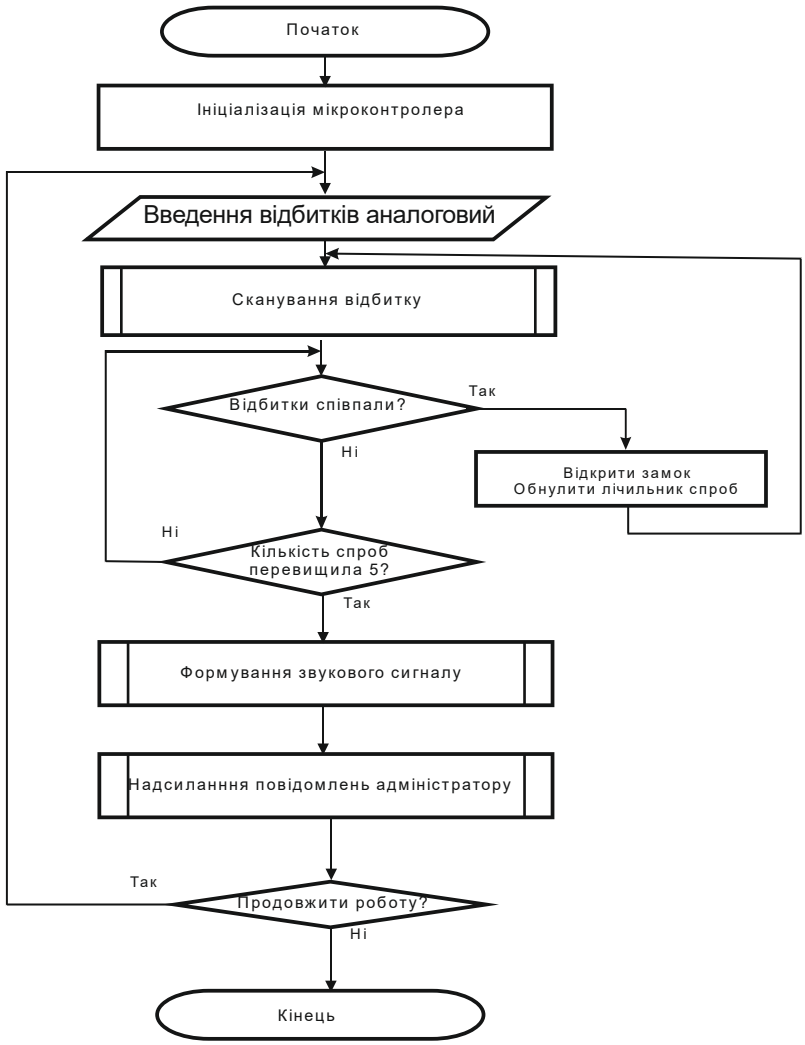
ДОДАТОК Б

(обов’язковий)

Копія графічної частини




DD1
MCC
PC6
PD0
PD1
PD2
PD3
PD4
VCC
GND
PB6
PB7
PD5
PD6
PD7
PB0
PC5
PC4
PC3
PC2
PC1
PC0
AGND
AREF
AVCC
PB5
PB4
PB3
PB2
PB1
DD3
DD4
U_TX
U_RX
RX
TX
+5V
X1
A1
ZQ1
C1
C2
IN1 input
DD2
DD5
SCL
SDA
Buzzer
КРБКЛ. 101007.21.01.08 Э3



					КРБКІ. 101007.21.01.08 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Біометричний термінал керування доступом в приміщення Алгоритм роботи	Літера	Маса	Масштаб
Розроб.		Шишуй В.Р						
Перевір.		Мулар І.В.				Аркуш	Аркушів	
Т.Контр.								
Н.Контр.		Мостовий С.В.				ХНУ, КІ1с-21-1		
Затв.		Ключ Ю.П.						

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Швеця Валентина Руслановича
ПІБ здобувача вищої освіти

Студента ФІТ, 3 курсу, групи КІ1с-21-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

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

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

3.06.2024
дата

підпис

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 6%**

ID: 131415 Назва: Біометричний термінал керування доступом в приміщення Додано в БД: 2024-06-18 Автора: Швець В.Р. Керівники: Муляр І.В. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	68743	1027	1359 (2%)	16 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

Дата перевірки:
18.06.2024 22:26:34 EEST

Дата звіту:
18.06.2024 22:32:56 EEST

ID перевірки:
1016373399

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100008300

Назва документа: **Швець КвРБ КІ 2024 на палагіат**

Кількість сторінок: **60** Кількість слів: **10247** Кількість символів: **79149** Розмір файлу: **1.45 MB** ID файлу: **1016180880**

3.95%
Схожість

Найбільша схожість: **1.08% з Інтернет-джерелом** (http://ir.nmu.org.ua/bitstream/handle/123456789/158701/%d0%92%d0.

2.66% Джерела з Інтернету | 100 ..... Сторінка 62

1.96% Джерела з Бібліотеки | 45 ..... Сторінка 62

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Біометричний термінал керування доступом в приміщення

Автор: Швець Валентин Русланович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Муляр Ігор Володимирович, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 96,05%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Ігор МУЛЯР

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Дипломник Швець Валентин Русланович
Тема Біометричний термінал керування доступом в приміщення
Спеціальність 123 Комп'ютерна інженерія

Обсяг кваліфікаційної роботи:

кількість листів креслень 4 ; кількість сторінок записки 65
1. Короткий зміст роботи та прийнятих рішень В кваліфікаційній роботі розроблено програмно-апаратний пристрій для контролю доступу в приміщення за відбитком пальця на основі платформи Arduino

2 Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині.
3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому, теоретичному, розділі роботи 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 роботи. У наступному розділі було здійснено проектування з'єднання елементів між собою, детально розглянуто можливості з'єднань цих елементів. У основній проектній частині було реалізована сучасними методами та рішеннями прибор, якмй 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 роботи Кваліфікаційна робота відповідає сучасним вимогам до проектування програмно-апаратних пристроїв та містить ряд рішень, що відповідають умовам сучасності. Побудований пристрій має хороший рівень захисту від незаконого проникнення в приміщення, та надсилає повідомлення власнику, у випадку, коли хтось намагається проникнути без відома власника.

5. Негативні сторони проекту Розроблений пристрій досить громіздкий

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до поставленого завдання. 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 роботу в цілому Кваліфікаційна робота 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)
Підченко Сергій Костянтинович, завідувач кафедри ТМІТ, доктор технічних наук, професор

« 17 » 06 2024 р. (підпис)