

Міністерство освіти і науки України
Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та охоронних систем
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

АПАРАТНО-ПРОГРАМНА РЕАЛІЗАЦІЯ КОНТРОЛЮ
ДОСТУПУ ЗА ВІДБИТКОМ ПАЛЬЦЯ

HARDWARE AND SOFTWARE IMPLEMENTATION OF
FINGERPRINT ACCESS CONTROL

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-42
Кензерський Владислав Сергійович

(підпис)

Керівник:
к.т.н., доцент
Терлецький Тарас Володимирович

(підпис)

Кваліфікаційну роботу
допущено до захисту
« ____ » _____ 2026 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних та інформаційних технологій

Кафедра комп'ютерної інженерії та безпеки

Ступінь вищої освіти: бакалавр

Галузь знань: 12 Інформаційні технології

Спеціальність: 123 Комп'ютерна інженерія

Освітня програма: «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри

доц. Т. Терлецький

« 23 » 12 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Кензерському Владиславу Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Апаратно-програмна реалізація контролю доступу за відбитком пальця

Керівник роботи к.т.н., доцент Терлецький Тарас Володимирович

затверджені наказом закладу вищої освіти від «20» грудня 2025 року № 536/01-02

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 28.05.2026р.

3. Вихідні дані до роботи: джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
вступ, технічна характеристика та службове призначення об'єкту розроблення, аналіз існуючих аналогів, обґрунтування теми кваліфікаційної роботи бакалавра та постановка задачі на проектування, розробка структурної схеми системи, обґрунтування вибору апаратної складової системи, практична реалізація системи, висновки.

5. Перелік графічного (ілюстративного) матеріалу:
набір слайдів презентації кваліфікаційної роботи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада Консультанта	Підпис	
		завдання видав	завдання прийняв
<i>Аналітичний стан предметної області</i>	<i>Терлецький Т.В., доцент</i>		
<i>Огрунтування складових системи</i>	<i>Терлецький Т.В., доцент</i>		
<i>Проектування системи</i>	<i>Терлецький Т.В., доцент</i>		
<i>Нормоконтроль</i>	<i>Багнюк Н.В., доцент</i>		
<i>Гарант ОП</i>	<i>Лавренчук С.В., доцент</i>		
<i>Показник запозичень тексту</i>	_____ %		
<i>Академічна доброчесність</i>	<i>Міскевич О.І., асистент</i>		

7. Дата видачі завдання 23.12.2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	<i>Огляд літератури із досліджуваної проблеми, аналіз предметної області та наявних рішень</i>	до 10.02.2026 р.	
2.	<i>Розробка структурної схеми системи</i>	до 10.03.2026 р.	
3.	<i>Апаратно-програмна реалізація системи</i>	до 25.04.2026 р.	
4.	<i>Висновки</i>	до 28.04.2026 р.	
5.	<i>Формування списку використаних джерел</i>	до 30.04.2026 р.	
6.	<i>Оформлення пояснювальної записки</i>	до 05.05.2026 р.	
7.	<i>Представлення остаточного варіанту кваліфікаційної роботи керівникові</i>	до 05.05.2026 р.	
8.	<i>Нормоконтроль</i>	до 23.05.2026 р.	
9.	<i>Інструментальна перевірка на академічний плагіат</i>	до 26.05.2026 р.	
10.	<i>Здача кваліфікаційної роботи та всіх супровідних документів на кафедру</i>	до 28.05.2026 р.	

Здобувач вищої освіти

(підпис)

Владислав КЕНЗЕРСЬКИЙ

(прізвище, ініціали)

Керівник кваліфікаційної роботи

(підпис)

Тарас ТЕРЛЕЦЬКИЙ

(прізвище, ініціали)

АНОТАЦІЯ

Кензерський В. С. Апаратно-програмна реалізація контролю доступу за відбитком пальця. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел.

У першому розділі даної роботи висвітлено параметри рівнів безпеки біометричних модулів, основні технічні характеристики та службове призначення проектованої системи. Також проведено аналіз показників ефективності для професійної оцінки біометричних рішень, визначено сильні та слабкі сторони існуючих аналогів. Визначено основні вимоги до проектованої системи та завдання для її розроблення.

У другому розділі розроблено схему системи контролю доступу за відбитком пальця і пояснено принцип її роботи. Обґрунтовано вибір складових біометричної системи. Обґрунтовано вибір програмного забезпечення для розробки системи на базі платформи Arduino.

Третій розділ присвячений питанням практичної реалізації системи на програмному рівні. Описано процес ініціалізації та переведення мікроконтролера в режим байпас, підключення та програмування сканера відбитка пальця R305, дисплея LCD1602.

Ключові слова: система, мікроконтролер, відбиток пальця, схема підключення, програмування, сканер, ефективність, безпека.

ANNOTATION

Kenzersky V. Hardware and software implementation of fingerprint access control. Manuscript.

Qualifying work of a bachelor of EP Computer Engineering specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2026.

Qualification work consists of an introduction, three sections, conclusions, a references.

The first section of this work highlights the parameters of the security levels of biometric modules, the main technical characteristics, and the purpose of the designed system. An analysis of performance indicators for the professional assessment of biometric solutions is also carried out, the strengths and weaknesses of existing analogues are identified. The main requirements for the designed system and the tasks for its development are determined.

In the second section, a scheme of a fingerprint access control system is developed and the principle of its operation is explained. The choice of biometric system components is justified. The choice of software for developing a system based on the Arduino platform is justified.

The third section is devoted to the issues of practical implementation of the system at the software level. The process of initialization and switching the microcontroller to bypass mode, connection and programming of the R305 fingerprint scanner, LCD1602 display is described.

Keywords: system, microcontroller, fingerprint, connection diagram, programming, scanner, efficiency, security.

ВСТУП

У сучасних умовах цифровізації та підвищених вимог до безпеки об'єктів критичної, комерційної та приватної інфраструктури, надійний контроль доступу є першочерговим завданням. Традиційні засоби автентифікації такі як механічні ключі, магнітні картки або цифрові паролі мають суттєві недоліки. Картки та ключі можна загубити, передати третім особам або скопіювати, а паролі підглянути чи підібрати.

Найбільш ефективним вирішенням цієї проблеми є впровадження біометричних систем ідентифікації, серед яких розпізнавання за відбитком пальця залишається одним із найдоступніших, точних та швидкодійних методів. Унікальність папілярного візерунка кожної людини виключає можливість фальсифікації чи передачі «ідентифікатора» іншій особі, що зводить ймовірність несанкціонованого доступу до мінімуму.

Таким чином, розробка апаратно-програмного забезпечення СКД за відбитком пальця на основі Arduino є актуальною. Вона спрямована на створення бюджетного, але водночас високонадійного, гнучкого та енергоефективного рішення для автоматизації біометричного контролю доступу, яке легко адаптується під специфіку конкретного об'єкта та може стати базою для побудови складніших систем безпеки.

Метою даної роботи є розробка системи контролю доступу за відбитком пальця на основі модулів Ардуїно.

Об'єкт дослідження: процес автоматизації контролю та керування доступом до об'єктів (приміщень) на основі біометричних даних.

Предмет розроблення: апаратно-програмне забезпечення системи контролю доступу за відбитком пальця, реалізоване за допомогою мікроконтролерів сімейства Arduino та сканеру відбитків пальця.

ЗМІСТ

РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ.....	7
1.1 Технічні характеристики та службове призначення об'єкту проектування.....	7
1.2 Аналіз існуючих аналогів	9
1.3 Обґрунтування теми кваліфікаційної роботи бакалавра та постановка задачі на проектування.....	18
РОЗДІЛ 2 ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ТА МЕТОДІВ РЕАЛІЗАЦІЇ	20
2.1 Розробка схеми системи контролю доступу за відбитком пальця..	20
2.2 Обґрунтування вибору складових схеми.....	21
2.2.1 Обґрунтування вибору модуля мікроконтролера та його будова.....	21
2.2.2 Обґрунтування вибору модуля сканера відбитків пальців....	27
2.2.3 Обґрунтування вибору моделі електромагнітного замка.....	32
2.2.4 Обґрунтування вибору дисплея.....	33
2.3 Обґрунтування вибору програмного забезпечення для розробки системи на базі платформи Arduino.....	35
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ.....	37
3.1 Завантаження програми в плату Arduino UNO.....	38
3.2. Підключення та програмування сканера відбитка пальця R305...	39
3.3 Підключення та програмування дисплея LCD1602.....	43
ВИСНОВКИ.....	49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	51
ДОДАТКИ.....	54

РОЗДІЛ 1

АНАЛІТИЧНИЙ ОГЛЯД СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Технічні характеристики та службове призначення об'єкту проектування

Об'єктом проектування є система контролю доступу за відбитком пальця, яка повинна забезпечувати реєстрацію, порівняльний аналіз з наявною базою даних відбитків пальців та відкриття запірного пристрою типу електромагнітного замка.

В основі такої системи лежить здатність однозначно ідентифікувати особу за її унікальними біологічними характеристиками – папілярними лініями, що усуває вразливості, притаманні фізичним ключам чи паролем, такі як крадіжка або дублювання. Проектована система контролю доступу повинна забезпечувати цілісний цикл операцій – від високоточного сканування та цифрової обробки відбитку пальця до надійного керування виконавчими механізмами та інтеграції з мережевими протоколами моніторингу.

Таким чином, дана система має забезпечувати високу точність розпізнавання відбитків пальців, зберігати свою працездатність у разі зникнення напруги в загальній електромережі, бути інформативною (мати дисплей або інший пристрій для розуміння статусу системи).

Біометрична верифікація даної системи базується на оцінці диференціальних біологічних рис людини таких як відбитки пальців, що є найбільш доступними для реалізації на базі мікроконтролерної системи.

Сам папілярний візерунок складається з гребенів та западин, які формують складні структури – дуги, петлі та завитки. Ключовим елементом розпізнавання є так звані точки розгалуження або закінчення папілярних ліній.

Система на базі мікроконтролерної системи повинна оперувати двома основними статистичними показниками ефективності – коефіцієнтом помилкового доступу (False Acceptance Rate, FAR) та коефіцієнтом помилкової відмови (False Rejection Rate, FRR) [1]. Ці показники напряму залежать від

налаштованого рівня безпеки в прошивці сенсора (табл. 1.1). Чим нижче значення FAR, тим вища безпека системи і, відповідно, чим нижче FRR, тим зручніша система для користувача (менше помилкових відмов).

Таблиця 1.1 – Параметри рівнів безпеки біометричних модулів [1]

Рівень безпеки	Коефіцієнт FAR	Коефіцієнт FRR	Рекомендована сфера застосування
Рівень 1	< 0,01 %	< 0,1 %	Побутові пристрої з низьким ризиком
Рівень 2	< 0,005 %	< 0,5 %	Внутрішні двері офісних приміщень
Рівень 3	< 0,001 %	< 1,0 %	Основні входні двері
Рівень 4	< 0,0005 %	< 2,0 %	Сховища цінностей (сейфи), серверні
Рівень 5	< 0,0001 %	< 5,0 %	Високорежимні об'єкти з 2FA (двофакторна авторизація)

На практиці рівень 3 вважається оптимальним балансом [1], оскільки вищі рівні безпеки можуть призводити до необхідності повторного сканування пальця у разі його сухості або забруднення, що знижує комфорт експлуатації.

Таким чином, для замка на дверях, які є основним входом до приміщення, оптимальним варіантом є рівень безпеки біометричних модулів 3-й з коефіцієнтом FAR < 0,001 % і коефіцієнтом FRR < 1,0 %.

Із урахуванням вище сказаного, вихідні технічні характеристики згідно завдання на кваліфікаційну роботу, які планується закласти в систему, подано в таблиці 1.2.

Таблиця 1.2 – Технічні характеристики системи контролю доступу за відбитком пальця

Характеристика	Значення
Напруга живлення, В	12, ± 10 %
Максимальний струм споживання, А	1
Тип замка	електромеханічний
Коефіцієнт FAR	< 0,001 %
Коефіцієнт FRR	< 1,0 %
Тип дисплея	рідкокристалічний
Діапазон робочих температур, °	20...70

Дану систему пропонується до застосування в приватних домогосподарствах, або комерційних об'єктів для безключового доступу.

1.2 Аналіз існуючих аналогів

Еволюція засобів фізичної безпеки та систем контролю і управління доступом (СКУД) призвела до поступового витіснення традиційних методів ідентифікації, таких як механічні ключі, цифрові коди або безконтактні картки, на користь біометричних рішень. Використання відбитка пальця як основного ідентифікатора особистості є найбільш зрілою та широко впровадженою технологією в сучасному секторі безпеки. Це зумовлено унікальністю папілярних візерунків кожної людини, що забезпечує високий рівень безпеки та зручності, оскільки ідентифікатор неможливо забути, загубити або передати іншій особі. Сучасний ринок біометричних СКУД представлений широким спектром аналогів, які відрізняються за типом використовуваних сенсорів, архітектурою побудови системи, алгоритмами розпізнавання та можливостями інтеграції в комплексні екосистеми безпеки.

Функціонування будь-якої системи контролю доступу за відбитком пальця ґрунтується на порівнянні щойно сканованого біометричного зразка з попередньо зареєстрованим шаблоном, що зберігається в базі даних. Цей процес не є абсолютним збігом, а базується на ймовірнісному аналізі, що вимагає використання специфічних метрик для оцінки ефективності та надійності системи.

Ключовими показниками ефективності для професійної оцінки біометричних рішень використовуються три основні параметри – FAR, FRR та EER, які визначають баланс між рівнем безпеки та комфортом експлуатації [2].

Перший параметр FAR, як було зазначено вище, – це коефіцієнт помилкового доступу. Ця метрика визначає ймовірність того, що система некоректно ідентифікує несанкціоновану особу як зареєстрованого користувача. У високозахищених середовищах, таких як банківські сховища чи серверні кімнати, низький показник FAR є пріоритетним. Наприклад, сучасні термінали Hikvision декларують FAR на рівні 0,001 %, що означає лише один випадок помилкового допуску на 100 000 спроб.

Інший параметр – коефіцієнт помилкової відмови FRR – визначає ймовірність того, що система відмовить у доступі легітимному користувачеві, чий шаблон присутній у системі. Високий FRR призводить до затримок на точках проходу та негативно впливає на користувацький досвід і тому для мало відповідальних точок доступу ця метрика має низькі значення (див. табл. 1.1)

Останній параметр EER – рівень рівної ймовірності помилок (Equal Error Rate). Це точка, де значення FAR та FRR збігаються (рис. 1.1). Чим нижчий показник EER, тим вища загальна точність та якість біометричного алгоритму [3].

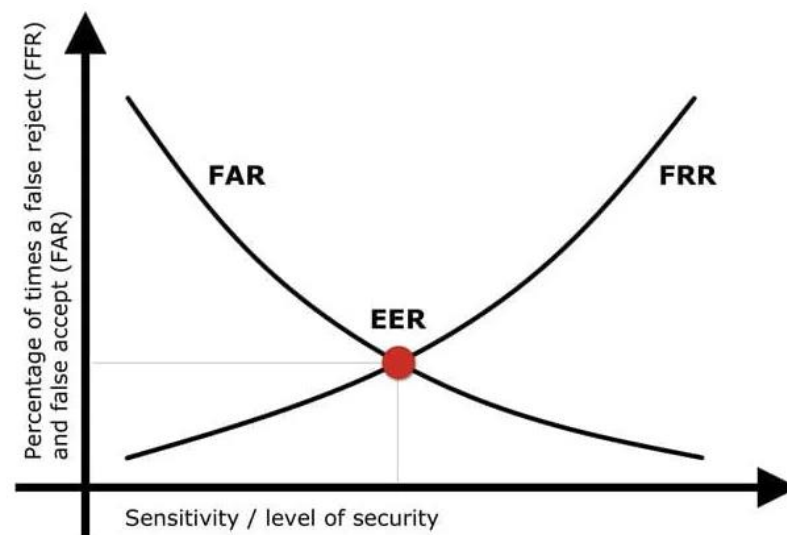


Рисунок 1.1 – Залежність взаємного впливу FAR та FRR [3]

Співвідношення між FAR та FRR регулюється порогом чутливості системи. Підвищення порогу для забезпечення максимальної безпеки (мінімізація FAR) неминуче веде до зростання кількості помилкових відмов (збільшення FRR).

Загалом, апаратна складова біометричної системи визначає її здатність працювати в різних умовах навколишнього середовища та стійкість до спроб злому за допомогою муляжів.

Апаратна реалізація зчитування відбитку пальця зчитувачами (сенсорами) здійснюється з використанням різних технологій: оптичної, емнісної та SilkID.

Оптичні зчитувачі є найбільш поширеним типом завдяки своїй надійності та відносно низькій вартості. Принцип їхньої роботи базується на фотографуванні папілярного візерунка за допомогою джерела світла та призми, де гребені пальця контактують з поверхнею, а западини залишаються на відстані, що створює контрастне зображення. Основним недоліком класичної оптики є вразливість до 2D-муляжів та фотографій, а також погіршення якості зчитування при сухості, вологості або забрудненні пальців.

Проте провідні виробники, такі як Suprema та ZKTeco, суттєво вдосконалили цю технологію [4]. Наприклад, сенсор OP5 від Suprema використовує алгоритми обробки зображень високої чіткості та вбудовану технологію виявлення «живого» пальця (Live Finger Detection, LFD), що аналізує динамічні зміни в тканинах під впливом світла.

Ємнісні сканери використовують мікроскопічні конденсатори, розташовані на кремнієвому чіпі [5]. Коли палець торкається сенсора, ємність кожного конденсатора змінюється залежно від відстані до шкіри (гребінь чи западина), що дозволяє побудувати детальну 8-бітну карту відбитка. Такі пристрої значно складніше обдурити муляжами, оскільки вони реагують на електричні властивості людського тіла [6]. Вони відзначаються компактністю, що дозволяє інтегрувати їх у мобільні термінали та розумні замки.

У свою чергу, компанія ZKTeco представила власну розробку – SilkID, яка є гібридом оптичного сенсора з розширеними можливостями аналізу глибоких шарів шкіри [7]. Ця технологія демонструє стабільність при зчитуванні сухих, мокрих та грубих пальців, що завжди було «слабким місцем» біометрії.

Залежно від способу обробки даних та керування виконавчими пристроями, біометричні СКУД поділяються на три основні категорії: автономні термінали та замки, мережеві термінали та універсальні IP-термінали.

Автономні системи поєднують зчитувач, контролер та базу даних в одному пристрої. Програмування здійснюється безпосередньо на терміналі за

допомогою вбудованої клавіатури або майстер-карт. Такі рішення, як автономні замки, є оптимальними для офісних кабінетів чи готельних номерів, де монтаж мережевої інфраструктури є економічно недоцільним. Вони живляться від батарейок, що спрощує інсталяцію, проте мають обмеження щодо дистанційного керування та аудиту подій у реальному часі.

У великих корпоративних системах використовуються мережеві біометричні контролери. В такій архітектурі зчитувач відбитків лише передає скановані дані на центральний контролер по інтерфейсу RS485 [8]. Контролер приймає рішення про доступ, що підвищує безпеку, оскільки лінія керування замком знаходиться всередині приміщення, а не в зовнішньому зчитувачі. Мережеві системи підтримують протоколи TCP/IP для передачі даних на сервер та можуть обслуговувати тисячі точок проходу.

Універсальні IP-термінали – це найбільш сучасний клас пристроїв, який поєднує можливості автономної роботи та повної інтеграції в мережу через Ethernet або Wi-Fi.

Стосовно нашого завдання – застосування в приватних домогосподарствах, або комерційних об'єктів для безключового доступу – доцільне впровадження автономної системи.

Загалом, сучасний ринок СКУД за відбитком пальця представлений величезною кількістю апаратних реалізацій від різних виробників – від бюджетних рішень до систем преміум-класу.

Замок Edinger Smart Fingerprint з функцією зчитування відбитку пальця (рис. 1.2) призначений для встановлення на ворота, хвіртку або входні двері [9] та має два основні блоки: біометричний зчитувач та електромеханічний блок. Його можна відкривати за відбитком пальця, механічним ключем або магнітною картою. Біометричний сенсор розташовується на зовнішній стороні дверей. Замок керується веб-застосунком.

Електромеханічний замок Edinger, що входить до комплекту, є бездротовим і живиться від 4-х батарейок. З однієї сторони це добре – забезпечує незалежне від зовнішньої електричної мережі енергоживлення, але з

іншої – обмежений ресурс роботи батарейок, а отже, є потреба постійно носити з собою ключі. Це пояснюється тим, що заміну батарейок можна зробити тільки з внутрішньої сторони, а роз’єм на підзарядку акумуляторів розташовано також там, і в один «прекрасний» момент можна залишитися на вулиці та не потрапити у середину.

Середня ринкова ціна замка, станом на весну 2026 року, становить 4800 гривень.



Рисунок 1.2 – Замок Edinger Smart Fingerprint зі зчитувачем відбитку пальця [9]

Загальні технічні характеристики замка Edinger Smart Fingerprint подано в таблиці 1.3.

Таблиця 1.3 – Технічні характеристики замка Edinger Smart Fingerprint

Характеристика	Значення
Тип замка	Електромеханічний
Призначення	Хвіртки, зовнішні двері
Відбиток пальця, шт.	До 100
Магнітна карта, шт.	До 100
Зовнішнє керування	Веб-додаток
Живлення, В	4 батарейки або акумулятори типу AA 1,5 В
Температура експлуатації	-15..+55° С

У відкритих технічних характеристиках та описі замка Edinger Smart Fingerprint не зазначено точного числового значення рівня помилок FAR, але

можна припустити, що це значення є нижче 0,001 %, оскільки, сучасні біометричні замки такого класу зазвичай мають такі показники FAR.

Інший аналог – це бездротовий електромоторний замок SEVEN LOCK SL-7770BF (рис. 1.3), який також призначений для встановлення на хвіртки та вхідні двері. Він виконаний за класом IP-54, що означає замок захищений від пилу і допускається незначне проникнення його проникнення у середину, що не порушує роботу, та від бризок води з будь-якого напрямку – тобто від дощу [10].

До складу комплекту входять два основні бездротових блоки: біометричної клавіатури та електромоторного замка [11]. Даний замок також має електромоторний привід, який виводить та вводить язичок з його корпусу

Всі блоки живляться від 4-х батарейок або акумуляторів 1,5 В типу АА. За даними виробника їх вистачає на 10000 циклів відкриття/закриття замка. Це означає, що батарейок вистачить приблизно на 1 рік уразі спрацювання замка 30 разів на день (але потрібно пам'ятати про саморозряд таких джерел живлення).

Середня ринкова ціна замка, станом на весну 2026 року, становить 4950 гривень.



Рисунок 1.3 – Замок SEVEN LOCK SL-7770BF [11]

Суттєвою відмінністю від попереднього замка Edinger Smart Fingerprint є те, що кожен блок оснащений роз'ємом на подання живлення від зовнішнього джерела.

Загальні технічні характеристики замка SEVEN LOCK SL-7770BF подано в таблиці 1.4.

Таблиця 1.4 – Технічні характеристики замка SEVEN LOCK SL-7770BF

Характеристика	Значення
Тип замка	Електромеханічний
Призначення	Хвіртки, зовнішні двері
Відбиток пальця, шт.	До 100
Магнітна карта, шт.	До 100
Зовнішнє керування	Веб-додаток
Живлення, В	4 батарейки або акумулятори типу AA 1,5 В
Температура експлуатації	-20...+60° С

У відкритих джерелах та описі замка SEVEN LOCK SL-7770BF не зазначено точного числового значення рівня помилок FAR, але за аналогією з попереднім замком можна припустити, що це значення є нижче 0,001 %.

Ще один аналог – накладний smart замок ATIS Lock A20T (рис. 1.4). Він підтримує наступні типи доступу: за відбитком пальця, за RFID-картою, за пін-кодом, через веб-застосунок або за допомогою механічного ключа [12].



Рисунок 1.4 – Замок ATIS Lock A20T [12]

Він належить до накладних електромеханічних замків, оскільки має електродвигун (рис. 1.5), і призначений для встановлення на входні двері квартир та приватних будинків.

Середня ринкова ціна замка, станом на весну 2026 року, становить 4840 гривень.



Рисунок 1.5 – Внутрішня будова замка ATIS Lock A20T

Як видно з рисунка 1.5, електромеханічна та електронна частини замка розташовані у зовнішньому блоці, а його елементи живлення – 4-ри акумуляторні батареї типу AA – у внутрішньому. Якщо виникає потреба «аварійного живлення» – його можна подати через бічний роз'єм USB Type-C.

За даними виробника [12] живлення від акумуляторних батарей типу AA має вистачити на 1,5 року.

Замок ATIS Lock A20T має значення рівня помилок FAR нижче 0,001 %.

Загальні технічні характеристики замка ATIS Lock A20T подано в таблиці 1.5.

Таблиця 1.5 – Технічні характеристики замка ATIS Lock A20T

Характеристика	Значення
Тип замка	Електромеханічний
Призначення	Хвіртки, зовнішні двері
Відбиток пальця, шт.	До 100
Магнітна карта, шт.	До 100
Зовнішнє керування	Веб-додаток
Елемент живлення	4 акумулятори типу AA
Напруга живлення, В	4,5-9
Струм споживання в режимі очікування, мкА	60
Робочий струм, мА	300
Аварійне джерело живлення	порт USB Type-C
Температура експлуатації	-20...+60° C

З проведеного аналізу існуючих аналогів замків з біометричним доступом за відбитком пальця стає зрозуміло, що такий замок має три основні складові: силову (електромеханічний привід), електронну (відповідає за зчитування відбитку пальця з сенсора та подачі сигналу керування на силовий блок) та програмну (зберігає базу відбитків пальців, порівнює наданий відбиток з наявною базою та видає відповідний сигнал на електронний блок керування силовим модулем).

Електромеханічний привод у переважній більшості має редуктор, який побудовано на основі конічної прямозубої передачі (рис. 1.5). Останньому характерне високий рівень шуму під час роботи, значні навантаження на вали (осі) та потребує періодичного обслуговування (змащення). Всі ці передачі виготовлено з силумінового сплаву, який належить до крихкого матеріалу, що має низьку довговічність та не підлягає ремонту. Таким чином, потрібно розглянути інший підхід до реалізації силової частини проектного замка.

У свою чергу, всі існуючі замки з біометричним доступом за відбитком пальця в якості джерела живлення мають 4-ри батарейки або акумулятори типу розміру AA та можливість подачі резервного живлення через роз'єми USB

Type-C чи мікро- USB. З однієї сторони це добре, але у певний момент призведе також до відповідних незручностей.

Подібні замки, які встановлюють на відкриття хвірток та входних дверей, повинні відповідати третьому рівню безпеки та мати коефіцієнт FAR < 0,001 % і FRR < 1,0 %, що відповідає типу точкам доступу «Основні входні двері».

1.3 Обґрунтування теми кваліфікаційної роботи бакалавра та постановка задачі на проектування

Традиційні системи контролю доступу (механічні замки, кодові клавіатури, RFID-картки) мають основний недолік: вони ідентифікують наявність відповідного «ключа» або знання пароля, а не саму особу. RFID-картку можна загубити, передати третій особі чи скопіювати, а пароль – записати, вкрати або зламати.

Біометрична автентифікація вирішує цю проблему, оскільки використовує унікальні фізіологічні характеристики людини, які неможливо забути, передати іншим або легко підробити. Це суттєво оптимізує процеси перевірки, підвищує внутрішню безпеку об'єктів та прискорює пропускну здатність [13].

Перехід на біометрію усуває постійні витрати на заміну чи відновлення втрачених карток або ключів, що робить систему економічно вигідною у довгостроковій перспективі.

Пропонована система будується за модульним принципом на базі доступних та надійних електронних компонентів низької вартості, що спрощує її масштабування та ремонт.

Проектована система повинна відповідати наступним вимогам:

- розпізнавати, порівнювати з наявними в базі системи та підтверджувати у разі збігу достовірність наданого відбиток пальця;
- бути енергоефективною та стійкою до зникнення напруги в загальній електромережі;

- відповідати Рівню 3 безпеки.

Для апаратно-програмної реалізації контролю доступу за відбитком пальця необхідно:

- розробити схему системи;
- обрати функціональні модулі системи та необхідне програмне забезпечення;
- здійснити практичну реалізацію системи.

РОЗДІЛ 2

ОБГРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ТА МЕТОДІВ РЕАЛІЗАЦІЇ

2.1 Розробка схеми системи контролю доступу за відбитком пальця

Систему контролю доступу за відбитком пальця планується розробити на базі модулів Arduino. Проектована система повинна надавати доступ до внутрішнього приміщення чи території через входні двері або хвіртку та виконувати наступні функції: відкриття/закриття замка; реєстрацію, порівняння та видалення шаблону відбитка з бази даних; світлозвукове відображення стану системи зі сторони входу та внутрішньої сторони; елементи керування (кнопки).

В якості запірного пристрою пропонується використати замок електромагнітного типу (обґрунтування типу подано у п. 1.2 першого розділу даної роботи).

Функції реєстрації, порівняння та видалення шаблону відбитка з бази даних буде виконувати сканер відбитків пальців оптичного принципу дії

Стан системи має відображати LCD дисплей, на який буде виводитися інформація про доступ/заборону до приміщення, події системи, доступ до меню програми та переходи по ньому, а також два світлових індикатора (червоний і зелений), які мають сповіщати про доступ/заборону до приміщення.

Для переходу по опціях меню програми потрібно застосувати два модулі кнопок Arduino.

Пропоновану структурну схему такої системи подано на рисунку 2.1.

Для виконання вище згаданих функцій, із врахуванням даних зазначених у таблиці 1.2, планується застосувати наступні модулі:

- Arduino Uno;
- зумер;
- 2 кнопки;
- LCD дисплей;
- 2 світлових діоди;

- силовий ключ;
- електроригельний замок;
- оптичний сканер відбитків пальців;
- джерело безперебійного живлення 220 В/12 В.

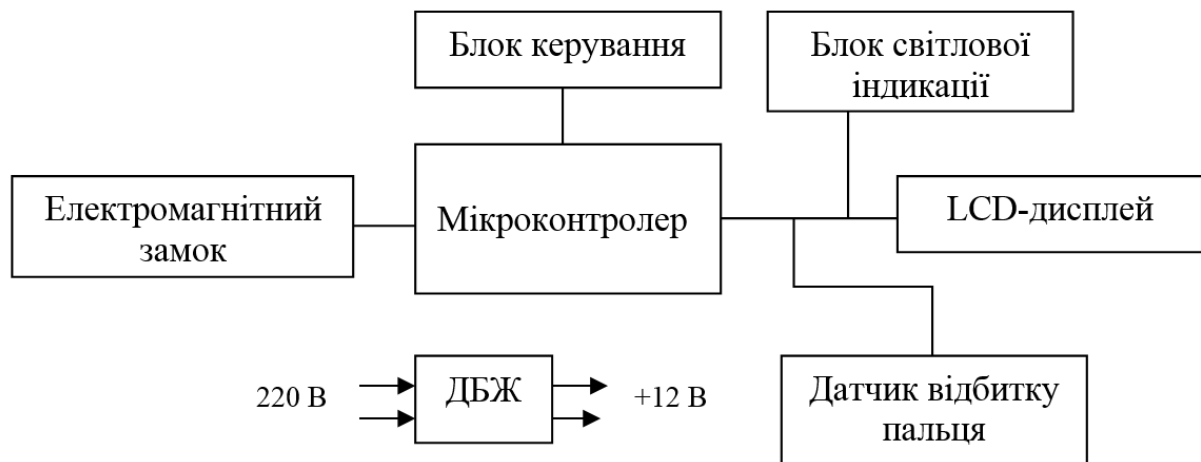


Рисунок 2.1 – Структурна схема системи контролю доступу за відбитком пальця

Ці модулі потрібно підключити до плати мікроконтролера в якості якого планується використати Arduino Uno.

2.2 Обґрунтування вибору складових схеми

Вибір складових, перерахованих у п. 2.1 даного розділу, здійснено на основі дослідження наявних на ринку компонентів та аналізу їх параметрів.

2.2.1 Обґрунтування вибору модуля мікроконтролера та його будова

Вибір мікроконтролера здійснено на основі порівняння характеристик двох контролерів Arduino Pro Mini та Arduino UNO.

При виборі між Arduino UNO та Arduino Pro Mini ми стикнулися з дилемою між компактністю та функціональністю. Хоча обидві плати можуть базуватися на ідентичному мікроконтролері ATmega328P, архітектурна

реалізація Arduino UNO надає суттєві переваги в аспектах надійності, інтеграції периферії, зручності налагодження та ремонтпридатності.

Найбільш очевидною та фундаментальною перевагою Arduino UNO є наявність повністю інтегрованого інтерфейсу USB-to-Serial. У моделях Arduino UNO R3 це реалізовано за допомогою додаткового мікроконтролера ATmega16U2, який діє як програмний міст між комп'ютером та основним чіпом. Це забезпечує безперебійне підключення через стандартний кабель USB Type-B, що робить процес завантаження коду максимально наближеним до концепції «plug-and-play» [14, 15].

На відміну від цього, Arduino Pro Mini позбавлена будь-яких бортових засобів зв'язку з USB для досягнення мінімальних габаритів та зниження собівартості. Для програмування Pro Mini розробник змушений використовувати зовнішній FTDI-адаптер або інший перетворювач USB-to-TTL. Це створює додаткові складнощі, оскільки вимагає точного з'єднання шести пінів (DTR, TX, RX, VCC, GND, CTS) та контролю за напругою логічних рівнів. Помилка в підключенні або відсутність лінії DTR може призвести до невдачі при завантаженні коду, оскільки мікроконтролер потребує вчасного апаратного скидання для входу в режим завантажувача [15].

Використання ATmega16U2 на платі UNO також надає можливість перепрошити сам інтерфейсний чіп за допомогою протоколу DFU, що дозволяє перетворити Arduino UNO на HID-пристрій (клавіатуру, мишу або MIDI-контролер). Така гнучкість недоступна для Pro Mini, де зв'язок обмежений лише стандартним UART-інтерфейсом через зовнішні модулі.

Arduino UNO володіє значно складнішою та потужнішою системою регулювання напруги порівняно з Pro Mini. Наявність виділеного роз'єму DC Barrel Jack (рис. 2.2) та лінійного регулятора дозволяє платі приймати зовнішню напругу в широкому діапазоні від 7 до 12 В. Це важливо для проектів, де пристрій повинен працювати автономно від блоків живлення або акумуляторів без необхідності попереднього регулювання напруги до точних 5 В.

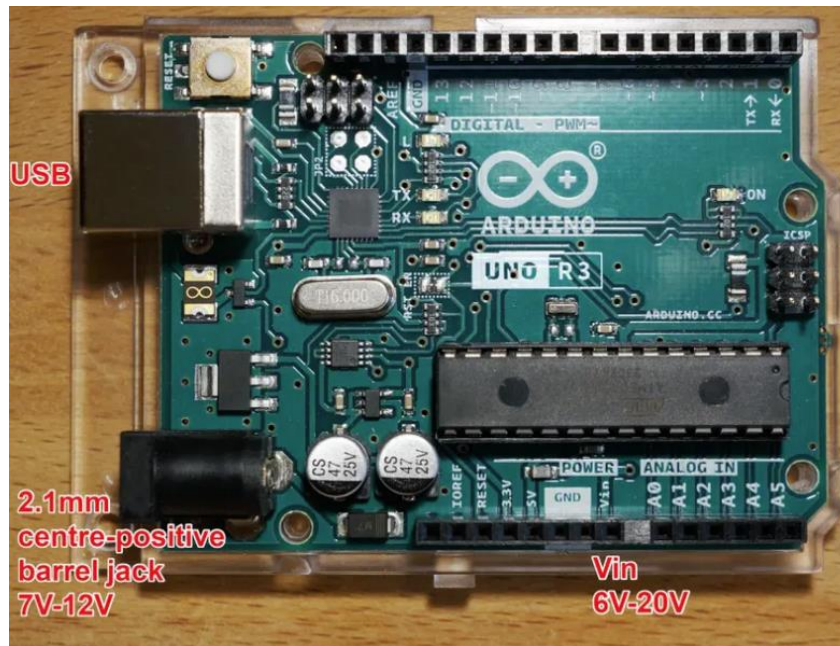


Рисунок 2.2 – Роз’єми живлення мікроконтролера Arduino UNO [15]

Arduino Pro Mini має вбудований мініатюрний регулятор напруги, який має дуже обмежені можливості щодо розсіювання тепла. Якщо UNO може стабільно видавати значний струм для живлення периферії, що важливо для електромагнітного замка, то регулятор Pro Mini при входній напрузі 12 В швидко перегрівається навіть при невеликих навантаженнях, що обмежує можливість підключення сенсорів, дисплеїв або реле безпосередньо до піна VCC [15].

Ще однією важливою перевагою є наявність окремої лінії живлення 3,3 В на борту UNO, яка забезпечується спеціалізованим регулятором. Це дозволяє безпосередньо жити сучасні низьковольтні модулі, що працюють при напрузі 3,3 В, навіть якщо основний мікроконтролер працює при 5 В. У випадку з Pro Mini користувач змушений обирати або 5-вольтову версію (де немає виходу 3,3 В), або 3,3-вольтову версію, яка працює на зниженій тактовій частоті 8 МГц.

Порівняльна характеристика двох мікроконтролерів керуванням живлення та електричної стійкості подана в таблиці 2.1.

Для інженерного проектування UNO надає вищий рівень безпеки завдяки наявності самовідновлювального запобіжника, який розриває ланцюг

при перевищенні струму 500 мА через USB. Це захищає як саму плату, так і USB-порт комп'ютера від коротких замикань, які часто трапляються під час макетування. Pro Mini позбавлена такої вбудованої системи захисту [15].

Таблиця 2.1 – Характеристики UNO та Pro Mini по керуванню живлення та електричній стійкості

Характеристика живлення	UNO	Pro Mini
Вхідна напруга (DC Jack/RAW)	7-12 В	5-12 В
Вихідний струм 5V/VCC	до 800 мА	~150-200 мА
Вихідний струм 3.3V	50-150 мА	відсутній
Захист від переполюсовки	присутній	відсутній

Форм-фактор Arduino UNO став де-факто промисловим стандартом, що породило величезну екосистему сумісних плат розширення – шилдів (shields). Шилди дозволяють миттєво додавати функції, такі як GPS, Ethernet, керування двигунами, WiFi або CNC-керування, просто встановлюючи одну плату поверх іншої. Механічна сумісність забезпечується стандартизованим розташуванням гніздових роз'ємів.

Arduino Pro Mini через свої мініатюрні розміри та відсутність стандартизованих роз'ємів не сумісна з жодним із цих шилдів. Використання Pro Mini вимагає або монтажу на макетну плату, що часто призводить до «павутини» дротів, або розробки спеціалізованої друкованої плати. Це значно уповільнює процес створення повнофункціонального прототипу.

Ключовою перевагою класичної Arduino UNO R3 є те, що мікроконтролер ATmega328P встановлено у спеціальну панельку, а не припаяно. В умовах розробки, де висока ймовірність помилкового підключення високої напруги до цифрових пінів, можливість простої заміни чіпа є безцінною. Якщо розробник випадково спалить мікроконтролер, він може витягнути пошкоджений чіп та вставити новий, не купуючи нову плату.

На противагу цьому, Arduino Pro Mini використовує виключно поверхневий SMD монтаж. Вихід з ладу мікроконтролера на такій платі фактично означає її повну утилізацію, оскільки демонтаж та повторна пайка

SMD-компонентів вимагає спеціального обладнання та навичок, якими володіють далеко не всі початківці та навіть досвідчені інженери.

Більше того, знімна природа DIP-чіпа на UNO дозволяє розробникам використовувати плату лише як програматор. Після налагодження коду чіп можна вийняти та встановити безпосередньо у власну схему на друкованій платі або breadboard, залишивши плату UNO для наступних проектів.

Таким чином, можна стверджувати, що Arduino UNO є суттєво кращим модулем для розробки, ніж Arduino Pro Mini, завдяки своїй архітектурній повноті та експлуатаційній гнучкості. Основні переваги UNO – вбудований USB-інтерфейс, потужна система живлення, захист від електричних помилок та ремонтпридатність через DIP-панельку – роблять її ідеальним фундаментом для будь-якого проекту.

Arduino Pro Mini залишається спеціалізованим інструментом для фінальної стадії розробки, де пріоритетом є мінімізація фізичного об'єму або енергоспоживання (наприклад, у переносному медичному обладнанні або компактних IoT-датчиках на батарейках).

Розпінування виводів Arduino UNO подано на рисунку 2.3.

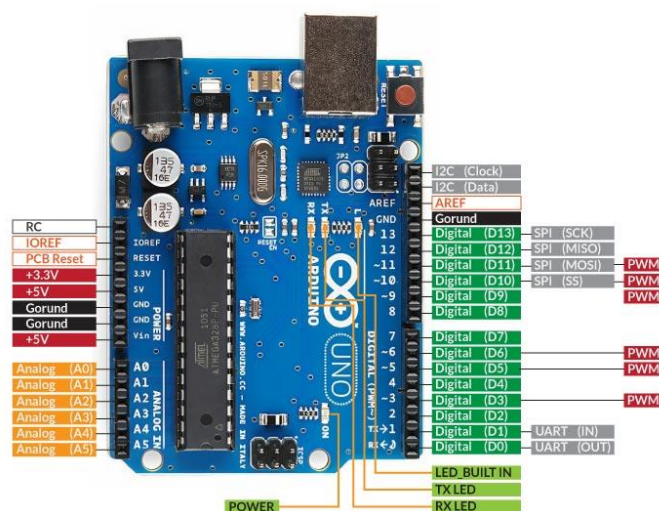


Рисунок 2.3 – Призначення виводів Arduino UNO [16]

Як видно з рисунка 2.3 розташування контактів Arduino UNO організовано за окремими категоріями, включаючи контакти живлення, цифрові контакти, аналогові контакти та контакти спеціальних функцій. Кожна категорія відіграє певну роль у забезпеченні функціональності плати.

Контакти живлення необхідні для роботи плати та підключених пристроїв. Основні контакти включають:

- VIN (підключення зовнішнього джерела живлення 7-12 В);
- 5 В та 3,3 В забезпечують регульовані виходи напруги для периферійних пристроїв;
- GND (заземлення) замикає коло живлення;
- IOREF забезпечує опорну напругу для контактів вводу/виводу.

Arduino UNO має 14 цифрових контактів (D0-D13), які можуть функціонувати як входи або виходи.

Контакти 0 (RX) та 1 (TX) зарезервовані для послідовного зв'язку.

Контакти 2-13 – контакти вводу/виводу загального призначення.

Виводи ШІМ (3, 5, 6, 9, 10, 11) підтримують широтно-імпульсну модуляцію, ідеально підходить для таких застосувань, як керування двигунами та регулювання яскравості світлодіодів.

Для взаємодії з цими контактами потрібно використовувати такі функції, як `pinMode()`, `digitalWrite()` та `digitalRead()` [16].

Аналогові контакти (A0-A5) дозволяють зчитувати сигнали безперервної напруги, часто від датчиків. За потреби також можуть функціонувати як цифровий ввід/вивід.

Спеціальні функціональні контакти:

- Reset Pin (скидає плату при спрацьовуванні);
- AREF (використовується для забезпечення зовнішньої опорної напруги для аналогових входів);
- Serial Pins (RX/TX) полегшують зв'язок UART для послідовного обміну даними.

Роз'єм ICSP (внутрішньосхемне послідовне програмування) дозволяє безпосередньо програмувати мікроконтролер або підключати додаткові периферійні пристрої.

Пін MISO (Головний-Вхід-Підлеглий-Вихід) призначений для отримання даних від периферійних пристроїв.

Пін MOSI (Головний-Вихід-Вхід-Підлеглий) призначений для надсилання даних на периферійні пристрої.

Пін SCK (Послідовний годинник) синхронізує передачу даних.

Комунікаційні піни:

– виводи I2C: SCL (лінія тактової частоти) та SDA (лінія даних) розташовані на A5 та A4 відповідно;

– виводи SPI: спільні функції з роз'ємом ICSP (MISO, MOSI та SCK);

– виводи UART: TX (вивод 1) та RX (вивод 0) відповідають за послідовний зв'язок.

Для програмування плати Arduino Uno потрібне середовище розробки Arduino IDE.

2.2.2 Обґрунтування вибору модуля сканера відбитків пальців

Моделі FPM10A, ZFM-20 та R305 стали фактичним стандартом для розробників завдяки їхній інтегрованій архітектурі «все в одному», яка поєднує оптичну систему захоплення зображення, спеціалізований цифровий сигнальний процесор (DSP) та енергонезалежну пам'ять для зберігання шаблонів. Ці модулі забезпечують високу швидкість обробки даних та автономність, виконуючи складні алгоритми виділення мінуцій (особливих точок) та їх зіставлення безпосередньо на апаратному рівні.

В основі функціонування моделей FPM10A, ZFM-20 та R305 лежить принцип порушеного повного внутрішнього відбиття. Оптичний блок кожного модуля складається зі скляної призми, системи освітлення (зазвичай на базі червоних або зелених світлодіодів) та CMOS-матриці. Коли палець користувача притискається до поверхні призми, гребені папілярного візерунка вступають у контакт зі склом, що призводить до поглинання або розсіювання світла в точках

контакту, тоді як впадини залишаються відокремленими від скла повітряним прошарком, забезпечуючи повне відбиття світла назад до сенсора.

Цей механізм дозволяє формувати висококонтрастне двовимірне зображення папілярного візерунка, де гребені виглядають темними ділянками, а впадини – світлими. Отримане зображення має роздільну здатність близько 500-508 точок на дюйм, що є оптимальним показником для ідентифікації основних мінуцій, таких як закінчення ліній та їх розгалуження.

Кожен з модулів оснащений вбудованим DSP, який виконує роль головного обчислювального ядра. Процесор виконує наступні операції [17-19]:

- покращення якості зображення та фільтрація шумів, що виникають через забруднення призми або сухість шкіри користувача;
- бінаризацію та скелетизацію зображення для підготовки до пошуку мінуцій;
- генерацію цифрового шаблону, який зазвичай має розмір 512 байт, та супутнього файлу ознак розміром 256 байт;
- виконання алгоритмів зіставлення в режимах 1:1 (верифікація за конкретним ID) та 1:N (ідентифікація шляхом пошуку по всій базі даних) .

Математично процес порівняння базується на обчисленні відстані між векторами ознак або оцінці конфігурації точок у просторі. Модулі дозволяють налаштовувати рівень безпеки (Security Level) від 1 до 5, що фактично змінює поріг чутливості алгоритму порівняння.

Загальні технічні характеристики модулів FPM10A, ZFM-20 та R305 подано в таблиці 2.2.

FPM10A позиціонується як найбільш доступне та гнучке рішення для прототипування та аматорських проектів. Його компактні розміри та сумісність з широким діапазоном напруги живлення роблять його ідеальним для інтеграції з мікроконтролерами Arduino, ESP32 та Raspberry Pi.

Аналіз ринкових пропозицій показує, що під маркуванням FPM10A можуть постачатися модулі з дещо різними характеристиками пам'яті, що

вказує на існування декількох апаратних ревізій (100/162/200/300/1000 шаблонів).

Таблиця 2.2 – Порівняльна характеристика модулів FPM10A, ZFM-20 та R305

Характеристика	FPM10A	ZFM-20	R305
Напруга живлення	3,3 V-6,0 V	3,3 V-6,0 V	4,2 V-6,0 V
Інтерфейс	UART (TTL), USB	UART (TTL), USB	UART (TTL), USB
Місткість пам'яті	100 – 1000 шаблонів	162 – 256 шаблонів	162 – 980 шаблонів
Час зчитування	< 1,0 сек	< 1,0 сек	< 0,5 сек
FAR (помилка допуску)	< 0,001 %	< 0,00 1%	< 0,001 %
FRR (помилка відхилення)	< 1,0 %	< 1,0 %	< 1,0 %
Робочий струм	< 120 мА	~100 мА	~100 мА

Однією з ключових переваг FPM10A (рис. 2.4) є його компактне вікно зчитування (14x18 мм), що дозволяє використовувати його в малогабаритних пристроях, таких як дверні ручки зі сканером або портативні сейфи. Однак менша площа вікна вимагає від користувача більш точного прикладання пальця, що може призводити до підвищення коефіцієнта помилкового відхилення (FRR) у недосвідчених користувачів.



Рисунок 2.4 – Модуль FPM10A [18]

FPM10A має одну з найкращих програмних підтримок серед бюджетних сенсорів. Бібліотека Adafruit Fingerprint Sensor Library забезпечує повний

спектр функцій: від реєстрації до видалення та пошуку шаблонів. Вбудоване червоне підсвічування лінзи слугує індикатором активності пристрою, що полегшує взаємодію з кінцевим користувачем.

У свою чергу, серія ZFM-20 (рис. 2.5) від виробника ZhianTec розроблялася з акцентом на більшу витривалість та здатність працювати в умовах інтенсивної експлуатації. Ця модель часто виступає базовою архітектурою для професійних систем контролю доступу.

ZFM-20 вирізняється більшим вікном зчитування (18x22 мм), що значно покращує зручність використання. Більша площа контакту дозволяє сенсору зафіксувати більше унікальних точок, що безпосередньо впливає на точність ідентифікації та швидкість пошуку в великих базах даних.



Рисунок 2.5 – Модуль ZFM-20 [19]

Особливістю ZFM-20 є вбудований апаратний 32-бітний генератор випадкових чисел (RNG), який може бути використаний у протоколах безпеки для генерації сесійних ключів або «солі» при передачі даних, що підвищує захищеність системи від атак типу «перехоплення-відтворення».

На відміну від багатьох спрощених модулів, ZFM-20 надає розширені можливості для вивантаження необроблених зображень відбитків. При використанні інтерфейсу USB 2.0 Full Speed пристрій передає 8-бітне зображення (256 рівнів сірого), що дозволяє використовувати його в ролі периферійного сканера для ПК. Це робить його придатним для банківських

терміналів або систем видачі документів, де правила вимагають збереження не лише шаблонів, а й візуальних доказів ідентифікації.

Інший модуль R305 є збалансованою моделлю, яка поєднує високу точність, велику ємність пам'яті та відносно низьку вартість. Він часто зустрічається в системах обліку робочого часу та електронних сейфах.

Однією з унікальних характеристик R305 є наявність двох типів конструктивного виконання: розділеного, де оптичний сенсор та керуюча плата з'єднані шлейфом, та інтегрованого, де всі компоненти розміщені в одному корпусі. Це надає дизайнерам кінцевих пристроїв більшу свободу у компонованні.

Модуль R305 базується на чіпі AS601, який забезпечує відмінну продуктивність алгоритмів обробки. Висока роздільна здатність (до 508 DPI) та велике вікно (18x22 мм) дозволяють йому стабільно працювати з «проблемними» відбитками, які мають механічні пошкодження або вікові зміни шкіри.

Незважаючи на спільну технологічну базу, пряме порівняння FPM10A, ZFM-20 та R305 виявляє значні розбіжності в експлуатаційних можливостях.

Збільшення площі сканування на 57 % у моделей ZFM-20 та R305 порівняно з FPM10A робить їх більш придатними для публічних систем, де користувачі не завжди прикладають палець ідеально рівно.

Усі три моделі є досить енергоємними під час активного сканування через роботу підсвітки та DSP, але найбільш широкий діапазон робочих температур має модуль ZFM-20. Цей модуль має явну перевагу для використання в неопалюваних приміщеннях або промислових цехах завдяки ширшому діапазону робочих температур.

Проведений аналіз модулів FPM10A, ZFM-20 та R305 демонструє, що вибір конкретної моделі повинен базуватися на пріоритетах проекту щодо масштабованості, надійності та бюджету. Стосовно нашого завдання найоптимальнішим є використання модуля ZFM-20 або R305.

2.2.3 Обґрунтування вибору моделі електромагнітного замка

З викладеного в п.1.2 даної роботи стає зрозуміло, що краще застосовувати електромагнітні ригельні замки соленоїдного типу замість електромеханічних.

З погляду логіки безпеки та поведінки системи в умовах надзвичайних ситуацій (зокрема, при втраті енергопостачання), електроригельні пристрої класифікуються на три категорії: нормальні відкриті, нормально закриті і універсальні.

У нормально відкритих замках запірний механізм блокується виключно за наявності живлення. У разі знеструмлення об'єкта ригель автоматично ховається всередину корпусу під дією поворотної пружини. Такі замки є обов'язковими для встановлення на шляхах евакуації, пожежних та запасних виходах, оскільки вони гарантують вільний вихід людей у разі аварії.

У нормально закритих замках блокування дверей забезпечується за відсутності електричного струму. Для відмикання необхідно подати імпульс напруги. Даний тип застосовується в приміщеннях з високими вимогами до збереження майна (серверні, депозитарії, склади), оскільки навіть при повному вимкненні енергії периметр залишається захищеним. Для запобігання блокуванню персоналу в таких зонах нормально закриті ригелі часто комплектуються механічними профільними циліндрами для відкривання звичайним ключем.

Універсальні замки. Обладнані внутрішнім перемикачем логіки роботи, що дозволяє адаптувати одну й ту саму модель під сценарії NO або NC безпосередньо на стадії інсталяції.

З вище сказаного стає зрозуміло, що з метою економії живлення доцільно застосовувати нормально закриті або універсальні замки, які підтримують сценарій NC.

Ринок України в сегменті електроригельних замикаючих пристроїв представлений різними брендами YLI Electronic, ATIS, SEVEN Lock та іншими вартістю 446-968 грн.

Проведений аналіз присутніх на ринку України ригельних електромагнітних замків дозволив обрати в якості виконавчого пристрою електромагнітний замок ригельного типу Yli Electronic YE-302A (рис. 2.6) – «...універсальний замок накладного типу, призначений для встановлення на дверцята шафок, камери зберігання, хвіртки, торгові вітрини магазинів та інші конструкції невеликого розміру. Головним позитивним моментом цього товару є те, що при відключенні живлення електромагнітний замок залишається закритим, так у будь-якій ситуації ваші речі залишаються в безпеці...» [20].



Рисунок 2.6 – Електромагнітний замок ригельного типу Yli Electronic YE-302A

Інші замки потрібного типу є врізними і суттєво переважають обраний за ціновою політикою, що робить їх недоцільне використання у нашому проєкті.

2.2.4 Обґрунтування вибору дисплея

На ринку представлено чотири ключові технологічні групи дисплеїв, кожна з яких базується на відмінних фізичних принципах: пасивні рідкокристалічні дисплеї (LCD), активні рідкокристалічні тонкоплівкові транзисторні панелі (TFT LCD), органічні світлодіодні індикатори (OLED) та дисплеї на основі електронного чорнила (ePaper) [21].

При інтеграції засобів візуалізації з апаратною платформою Arduino ключовим інженерним обмеженням є обсяг пам'яті мікроконтролера. Накопичувачі та оперативна пам'ять суттєво відрізняються залежно від

покоління та архітектури обчислювального ядра, що безпосередньо диктує сумісність із графічними бібліотеками.

Обсяг оперативної пам'яті (SRAM) є критичним ресурсом для графічних дисплеїв, оскільки більшість графічних бібліотек функціонують за принципом повного кадрового буфера в RAM з його подальшим скиданням на контролер через послідовний інтерфейс. Для монохромного OLED-дисплея з роздільною здатністю 128x64 пікселів мінімальний розмір кадрового буфера становить 1024 байтів. Виділення 1024 байтів під буфер бібліотеки Adafruit_SSD1306 на платформі Arduino Uno R3 поглинає рівно 50 % усієї доступної оперативної пам'яті мікроконтролера ATmega328P. З урахуванням динамічних потреб стеку та інших системних змінних, завантаження статичної пам'яті понад 60 % часто призводить до краху програми [21].

Для дисплеїв більшої роздільної здатності, наприклад OLED SSD1322 (256x64 пікселів), кадровий буфер вимагає 2048 байтів SRAM, що дорівнює повній ємності пам'яті Arduino Uno.

На противагу графічним панелям, символічні LCD-дисплеї під керуванням HD44780 мають вбудовану пам'ять знакогенератора та пам'ять відображення обсягом 80 байтів, яка інтегрована безпосередньо у кристал контролера дисплея. Програма на Arduino лише надсилає кодові ASCII-значення символів [21].

При компіляції базового проєкту для роботи з символічним LCD за допомогою утиліти LiquidCrystal у середовищі PlatformIO статичне споживання RAM становить лише 208 байтів, а обсяг коду у флеш-пам'яті не перевищує 3940 байтів. Це робить символічні дисплеї найбільш стабільними та невимогливими до апаратних ресурсів рішеннями.

З огляду на сказане стає зрозуміло, що для нашого проєкту доречно застосувати символічний LCD-дисплей, наприклад LCD1602.

2.3 Обґрунтування вибору програмного забезпечення для розробки системи на базі платформи Arduino

Вибір програмного забезпечення безпосередньо впливає на надійність, швидкість розпізнавання, безпеку збереження персональних даних та загальну масштабованість системи.

Для написання керуючого коду в екосистемі Arduino основним інструментом є бібліотека Adafruit Fingerprint Sensor Library. Вона абстрагує низькорівневий пакетний обмін командами через послідовний порт і надає розробнику високорівневий API для виконання таких операцій, як зняття кадру (`getImage`), генерація математичної моделі (`image2Tz` та `createModel`) та її збереження у внутрішній базі даних (`storeModel`) [22, 23].

У системах, побудованих на базі платформ з підтримкою мови Python, використовується бібліотека `adafruit-circuitpython-fingerprint`. Дане програмне забезпечення встановлюється за допомогою пакетного менеджера `pip` і надає аналогічні за функціоналом методи для управління процесом сканування та автентифікації користувачів через об'єкти типу `Adafruit_Fingerprint` [23].

Вибір інтегрованого середовища розробки (IDE) визначає ефективність структурування коду, швидкість його компіляції та зручність управління сторонніми залежностями при створенні програмного забезпечення для СКУД.

Для простих локальних СКУД на базі офіційних плат Arduino Uno, де обсяг коду не перевищує 500 рядків, використання Arduino IDE є виправданим завдяки низькому порогу входження та простоті інтерфейсу. Проте, при розробці складних мережевих систем на базі мікроконтролерів ESP32, вибір PlatformIO є більш доцільним. Це середовище дозволяє гнучко налаштовувати конфігурації плат, компілювати код під різні типи мікросхем в один клік та автоматично завантажувати необхідні версії бібліотек.

У свою чергу, вибір інструментарію розробки між хмарним чи локальним середовищем визначає продуктивність праці розробника, оскільки хмарні та локальні рішення мають принципово різні архітектурні ліміти та експлуатаційні

моделі. Хмарне середовище Arduino Cloud Editor функціонує в межах суворих обмежень безкоштовного тарифного плану, що ускладнює розробку складних безпекових систем. Зокрема, користувач хмари обмежений можливістю підключення лише 2 пристроїв та синхронізацією не більше 5 хмарних змінних на один пристрій. Крім того, хмарне сховище лімітоване об'ємом 100 МБ або лімітом у 100 ескізів, історія накопичення даних датчиків зберігається лише протягом 1 дня, а об'єм вхідного трафіку обмежений 10 МБ на місяць. Найбільш критичним обмеженням для розробника біометричної СКУД є ліміт на кількість компіляцій та завантажень коду, який у безкоштовній хмарі становить лише 25 операцій на добу.

У процесі налагодження взаємодії мікроконтролера з біометричним сканером виникає необхідність частих дрібних правок коду (зміна швидкості обміну, коригування тайм-аутів очікування пальця, зміна пінів програмного серійного порту), що призводить до вичерпання ліміту у 25 компіляцій за перші пів години роботи. Після цього розробник повністю втрачає можливість тестувати пристрій до початку наступної доби або змушений переходити на платну підписку. Локальне середовище розробки Arduino IDE (як класична версія 1.x, так і сучасна 2.x) використовує ресурси локального комп'ютера, не має жодних лімітів на кількість компіляцій та обмежується лише фізичним обсягом жорсткого диска або SSD-накопичувача ПК.

Головна проблема хмарного середовища полягає в тому, що користувач не має жодного інструменту для фізичного видалення вбудованих системних бібліотек, які конфліктують із його кодом. У локальному середовищі Arduino IDE ця проблема вирішується за лічені секунди. Користувач може увімкнути режим детального виводу компіляції (Verbose Output) в меню Preferences, точно локалізувати шляхи розташування файлів, що викликають конфлікт, та фізично видалити або перейменувати конфліктну теку на жорсткому диску свого комп'ютера.

Таким чином, застосування локального середовища розробки Arduino IDE є оптимальним варіантом.

РОЗДІЛ 3

ПРАКТИЧНА РЕАЛІЗАЦІЯ

Інтерфейс Arduino IDE містить наступні основні елементи: текстовий редактор для написання коду; область для виведення повідомлень; текстову консоль, панель інструментів із традиційними кнопками та головне меню. Даний софт дозволяє взаємодіяти з Arduino як передачі даних, так прошивки коду в контролер.

Програми для Arduino пишуться на стандартній мові C++. Насправді це просто набір стандартних функцій C/C++ та бібліотек, які утворюють так званий шар апаратної абстракції (Hardware Abstraction Layer/API). Він створений для того, щоб новачкам не доводилося вивчати складні системні реєстри мікроконтролера.

Програма, написана для Arduino, називається скетчем та зберігається у файлі з розширенням `.ino`.

Кожен базовий скетч має обов'язкову структуру, що складається з двох основних функцій: `void setup` і `void loop`.

Така структура спрощує програмування, оскільки IDE сама додає необхідну системну функцію `main()`, яка в класичному C++ запускає програму та організовує цей нескінченний цикл роботи процесора.

Коли активізувати кнопку Verify або Upload в Arduino IDE, відбувається наступний ланцюг дій:

- препроцесинг: IDE знаходить у папці проекту всі файли `.ino`, об'єднує їх в один файл із розширенням `.cpp`, автоматично додає системний заголовок `#include <Arduino.h>` та генерує прототипи функцій, якщо їх забули оголосити заздалегідь;

- пошук залежностей: компілятор сканує код на наявність інструкцій `#include` (наприклад, `#include <Adafruit_Fingerprint.h>`), визначає, які бібліотеки використовуються в проекті, та підключає шляхи до них;

- компіляція: спеціальний компілятор перетворює текстовий код C++ та всі залучені файли бібліотек у двійковий машинний код – об'єктні файли .o;
- лінкування: об'єктні файли програми об'єднуються зі стандартними функціями ядра Arduino. Результатом цього процесу є створення одного бінарного файлу, який містить готові байти інструкцій для процесора;
- завантаження: IDE запускає утиліту завантаження. Комп'ютер передає файл прошивки через USB-кабель до плати. Вбудована в мікроконтролер маленька програма – завантажувач – приймає ці байти та записує їх безпосередньо у флеш-пам'ять пристрою.

Щойно завантаження завершується, плата автоматично перезавантажується і відразу починає виконувати код самостійно – для її подальшої роботи комп'ютер більше не потрібен.

3.1 Завантаження програми в плату Arduino UNO

Завантаження скетчу в плату Arduino UNO – це процес, який вимагає дотримання кількох послідовних кроків: підготовки обладнання та софту, підключення плати, налаштування середовища Arduino IDE, написання або вибір коду, компіляція та завантаження.

Для початку потрібно мати саму плату Arduino UNO і USB-кабель з потрібним типом роз'єму Type-B (рис. 3.1) та встановити на ПК програму Arduino IDE.



Рисунок 3.1 – Необхідне обладнання для завантаження скетчу

Плату слід з'єднати з ПК, після чого на платі має засвітитися світловий діод живлення.

Перед тим як натискати кнопку «Завантажити», потрібно пояснити комп'ютеру, куди саме і на яку плату ми відправляємо код. Для цього в Arduino IDE потрібно вибрати у верхньому меню тип плати: Інструменти (Tools) → Плата (Board) → Arduino AVR Boards → Arduino Uno.

У подальшому потрібно обрати порт: Інструменти (Tools) → Порт (Port). Порт потрібно обрати той, біля якого в дужках написано (Arduino Uno).

Компіляція та завантаження відбуваються наступним чином.

У лівому верхньому кутку Arduino IDE є дві головні кнопки:

– «Перевірити» (кнопка з галочкою): вона компілює код – перевіряє його на наявність помилок. Натисніть її. Якщо знизу з'явився напис "Компіляцію завершено" (Done compiling), все добре.

– «Завантажити» (кнопка зі стрілкою вправо): вона прошиває плату.

Під час завантаження на самій платі Arduino UNO почнуть швидко блимати світлодіоди TX та RX (передача та прийом даних). Це знак того, що код «заливається» в чип.

Коли процес завершиться, внизу в IDE з'явиться напис «Завантаження завершено» (Done uploading).

Після цього вбудований світлодіод на платі (позначений буквою L) почне блимати з інтервалом в одну секунду.

3.2. Підключення та програмування сканера відбитка пальця R305

Оптичний сканер відбитків пальців R305 поєднує в собі високошвидкісний цифровий сигнальний процесор AS601, світлодіодне підсвічування та оптичну матрицю зчитування. Цей пристрій самостійно виконує весь спектр складних математичних обчислень, пов'язаних із сегментацією зображення, виділенням ключових точок (мінуцій), генерацією

шаблонів, а також пошуком збігів у вбудованій енергонезалежній флеш-пам'яті за алгоритмами 1:1 або 1:N [23].

Перед початком програмування перевірено працездатність сканера безпосередньо за допомогою ПК та спеціалізованого програмного забезпечення SYNO Demo (рис. 3.2). Для цього мікроконтролер ATmega328P переведено у режим високого імпедансу (байпас), завантажуючи в плату порожній скетч (ліст. 3.1).

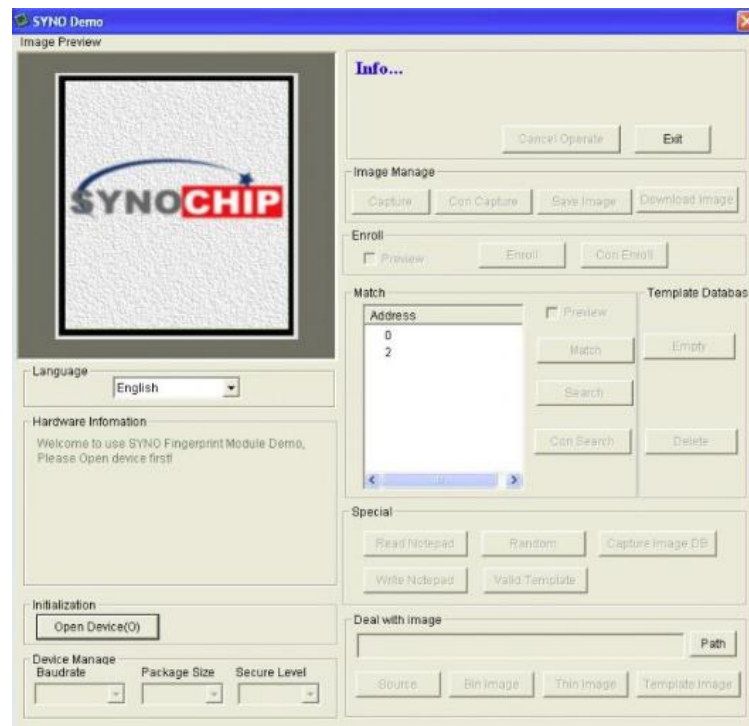


Рисунок 3.2 – Робоче вікно спеціалізованого ПЗ SYNO Demo

Лістинг 3.1 – Скетч переведення мікроконтролера в режим байпас

```
void setup() {
    pinMode(0, INPUT);
    pinMode(1, INPUT);
}

void loop() {
}
```

кінець лістингу 3.1

Фізичне підключення модуля R305 до плати Arduino Uno здійснюється за схемою, поданою на рисунку 3.3 [24].

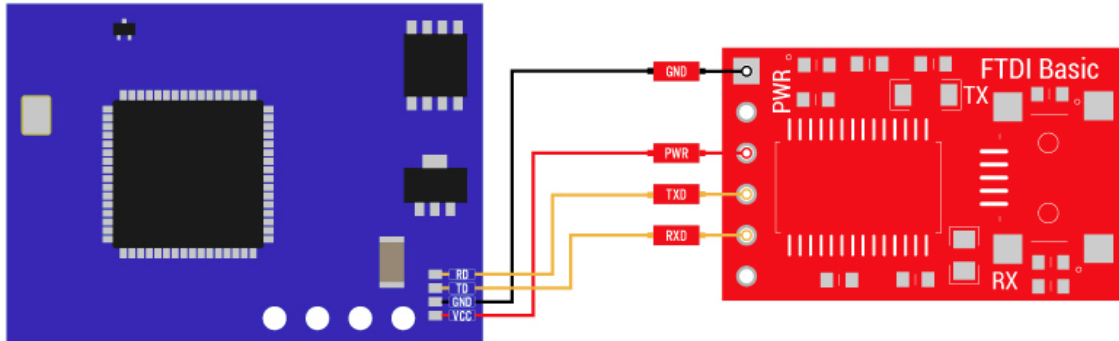


Рисунок 3.3 Схема підключення сканера відбитків пальця R305

При такому підключенні лінії комутуються безпосередньо до апаратного мосту USB-UART плати Arduino Uno:

- червоний дрiт сканера (VCC) підключається до виводу 5V Arduino;
- чорний дрiт сканера (GND) підключається до виводу GND Arduino;
- білий дрiт сканера (RX) підключається до виводу Digital 1 (TX апаратного порту Arduino);
- зелений дрiт сканера (TX) підключається до виводу Digital 0 (RX апаратного порту Arduino).

Після завантаження цього скетчу утиліта SYNO Demo отримує прямий доступ до R305, що дозволяє візуалізувати отриманий відбиток пальця, налаштовувати пароль пристрою та проводити первинне тестування датчика (рис. 3.4).

Для взаємодії з модулем R305 використовується бібліотека **Adafruit Fingerprint Sensor Library**. Процес встановлення складається з наступних кроків:

- у середовищі Arduino IDE необхідно відкрити вкладку меню Скетч → Підключити бібліотеку → Керувати бібліотеками...;
- у вікні пошуку «Менеджера бібліотек» слід ввести ключове слово **Fingerprint**;

– серед результатів пошуку необхідно вибрати та встановити бібліотеку Adafruit (ліст. 3.2).

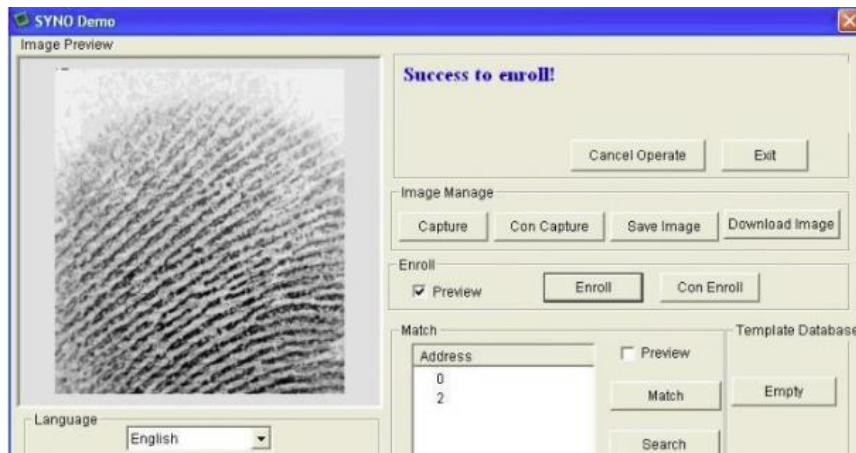


Рисунок 3.4 – Приклад візуалізації відбитка пальця в ПЗ SYNO Demo

Лістинг 3.2 – Скетч підключення сканера відбитків R305

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>

SoftwareSerial mySerial(2, 3);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

uint8_t id;

void setup() {
  Serial.begin(9600);
  while (!Serial);
  delay(100);

  Serial.println("\n\nРежим реєстрації відбитка пальця в системі R305");

  finger.begin(57600);

  if (finger.verifyPassword()) {
    Serial.println("Сканер відбитків пальців виявлено та успішно активовано!");
  } else {
    Serial.println("Помилка: Не вдалося знайти сканер відбитків. Перевірте дроти.");
    while (1) { delay(1); }
  }

  finger.getParameters();
```

```

Serial.print("Максимальна місткість внутрішньої пам'яті: ");
Serial.print(finger.capacity);
Serial.println(" шаблонів.");
}

```

кінець лістингу 3.2

Сама реєстрація відбитка є трифазним процесом. Спочатку датчик робить перший оптичний знімок папілярних ліній і створює тимчасову модель у буфері символів №1. Далі потрібно повторно прикласти той самий палець для створення другого знімка та формування моделі в буфері №2. На третьому етапі DSP порівнює обидва зображення на предмет ідентичності та, у разі успішного збігу, записує зашифрований хеш-шаблон у вказану комірку флеш-пам'яті під унікальним ID.

Повний скетч програми для роботи з модулем відбитків пальця подано у Додатку А даної роботи.

У режимі верифікації сканер очікує прикладання пальця, робить знімок, перетворює його на ознаки та виконує швидке апаратне порівняння з усіма записами у флеш-пам'яті за допомогою виклику методу `fingerFastSearch()`. У разі успіху сканер повертає ID розпізнаного шаблону та рівень достовірності відповідності (додаток Б).

3.3 Підключення та програмування дисплея LCD1602

Дисплей LCD1602 підтримує кілька конфігурацій обміну даними, що відрізняються кількістю задіяних провідників та швидкістю передачі даних. Вибір інтерфейсу є компромісом між апаратною складністю та завантаженістю портів введення-виведення мікроконтролера.

8-бітний паралельний режим передає дані швидше, але практично повністю займає цифрові порти плати Arduino Uno, що унеможливорює підключення сторонньої периферії. 4-бітний режим (рис. 3.5) усуває цю проблему, зменшуючи потребу в лініях даних до чотирьох (використовуються

виводи D4-D7 дисплея) [25]. Найбільш технологічним рішенням є послідовний інтерфейс I2C, який за допомогою спеціального I2C-бекпека (адаптера) транслює двопровідний послідовний потік даних у паралельні команди для РК-контролера.

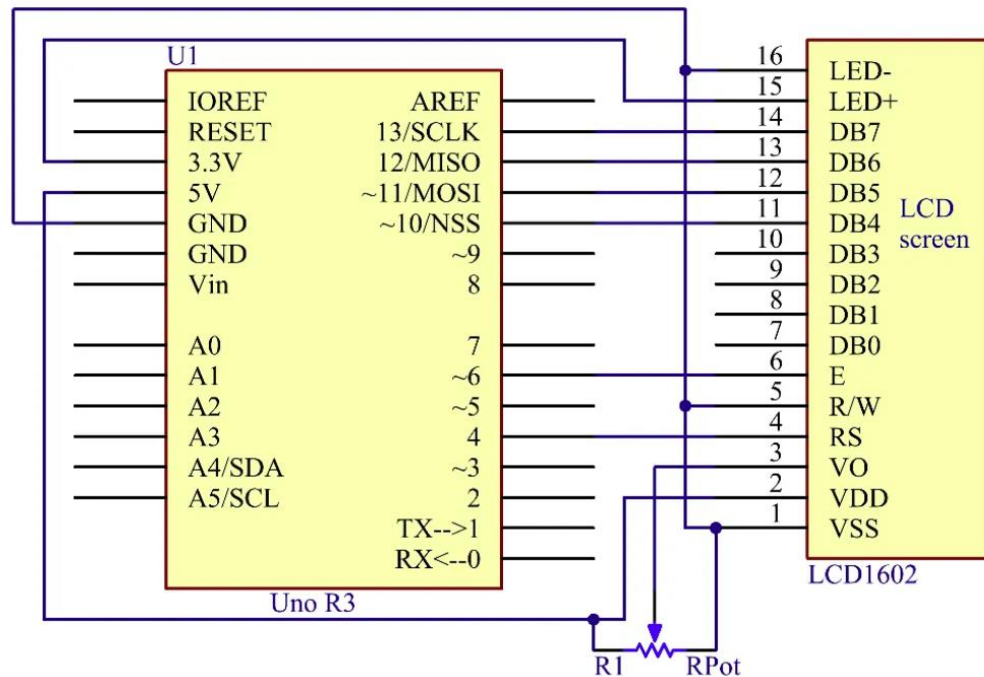


Рисунок 3.5 – Схема підключення LCD1602 до Arduino Uno [25]

Для прямого паралельного підключення LCD1602 до Arduino Uno використовується стандартний 16-контактний роз'єм дисплея. Оскільки мікроконтролер Arduino Uno здебільшого лише записує дані на дисплей, лінія читання/запису (R/W) з'єднується із землею (GND), що звільняє ще один порт мікроконтролера. Контрастність символів регулюється подачею аналогової напруги на вивід VO через потенціометр опором від 10 кОм до 50 кОм. Для підсвічування екрана анод підключається до лінії живлення через обмежувальний резистор номіналом 220 Ом (для запобігання виходу з ладу світлодіода), а катод з'єднується з GND. Альтернативно, у деяких спрощених схемах анод підключають безпосередньо до виходу 3,3 V без додаткового резистора.

Для програмної ініціалізації використовується вбудована бібліотека `LiquidCrystal.h` (ліст. 3.3). Програма повинна точно повторювати апаратне підключення через конструктор об'єкта.

Лістинг 3.3 – Скетч ініціалізації LCD1602

```
#include <LiquidCrystal.h>

const int pin_RS = 12;
const int pin_EN = 11;
const int pin_D4 = 5;
const int pin_D5 = 4;
const int pin_D6 = 3;
const int pin_D7 = 2;

LiquidCrystal lcd(pin_RS, pin_EN, pin_D4, pin_D5, pin_D6, pin_D7);

void setup() {
    lcd.begin(16, 2);

    lcd.clear();

    lcd.print("Arduino Uno");

    lcd.setCursor(0, 1);
    lcd.print("Parallel Mode");
}

void loop() {
}
```

кінець лістингу 3.3

Інтеграція LCD1602 за допомогою інтерфейсу I2C базується на застосуванні мікросхеми PCF8574 (або PCF8574A). Цей чіп є 8-бітним розширювачем введення-виведення, який приймає послідовні команди від Arduino Uno по двох дротах шини I2C (SDA та SCL) і розподіляє їх на паралельні лінії керування та даних дисплея.

Шина I2C на Arduino Uno реалізована на апаратних виводах аналогового порту. Лінія даних (SDA) підключається до контакту A4, а лінія тактування (SCL) – до контакту A5. На платах ревізії Uno R3 ці лінії також дублюються на

окремі виводи SDA та SCL, розташовані на цифровій колодці поруч із контактом AREF.

Адресація пристроїв на шині I2C визначається станом апаратних виводів A0, A1 та A2 на платі адаптера. Шляхом створення припойних перемичок на цих контактах розробник може змінювати базову адресу пристрою.

Для запобігання програмним помилкам через неправильну адресу рекомендується застосовувати діагностичний скетч-сканер (ліст. 3.4). Він сканує шину I2C шляхом надсилання стартового імпульсу та очікування сигналу підтвердження прийому від пристроїв. Якщо пристрій відповідає, його адреса негайно виводиться в послідовний порт.

Лістинг 3.4 – Діагностичний скетч-сканер шини I2C

```
#include <Wire.h>

void setup() {
    Wire.begin();
    Serial.begin(9600);
    while (!Serial) {}
    Serial.println("\nI2C Address Scanner Initiated...");
}

void loop() {
    byte error, address;
    int devicesFound = 0;

    Serial.println("Scanning active address space (1-127)...");

    for (address = 1; address < 127; address++) {
        Wire.beginTransmission(address);
        error = Wire.endTransmission();

        if (error == 0) {
            Serial.print("Device identified at address: 0x");
            if (address < 16) Serial.print("0");
            Serial.print(address, HEX);
            Serial.println("!");
            devicesFound++;
        }
    }

    if (devicesFound == 0) {
        Serial.println("No functional I2C devices detected.\n");
    } else {
```

```

    Serial.println("Scan sequence completed.\n");
}

delay(5000);
}

```

кінець лістингу 3.4

Шина I2C фізично передає інформацію по одному байту за транзакцію. Для відображення текстових рядків бібліотека `LiquidCrystal_I2C.h` внутрішньо розбиває масиви символів на окремі байти та передає їх послідовно за допомогою циклічних ітерацій (ліст. 3.5).

Лістинг 3.5 – Програмна реалізація шини I2C

```

#include <Wire.h>
#include <LiquidCrystal_I2C.h>

LiquidCrystal_I2C lcd(0x27, 16, 2);

void setup() {
    lcd.init();

    lcd.backlight();

    lcd.setCursor(0, 0);
    lcd.print("I2C Serial Mode");

    lcd.setCursor(0, 1);
    lcd.print("System Ready");
}

void loop() {
}

```

кінець лістингу 3.5

Найбільш поширеною проблемою при першому запуску дисплея є ситуація, коли підсвічування працює, але символи на екрані не відображаються або виглядають як суцільні темні прямокутники. Це явище безпосередньо пов'язане з різницею потенціалів між виводом живлення логіки (VCC) та виводом контрастності (VVO).

Для коректної орієнтації рідких кристалів та формування чітких символів напруга зміщення на виводі VO має бути приблизно на 4,5 В нижчою за рівень живлення логіки дисплея.

За номінальної напруги живлення мікроконтролера $VCC = 5,0$ В, напруга на виводі VO має бути на рівні +0,5 В відносно заземлення (GND). Це значення забезпечується стандартним підлаштовним потенціометром.

Таким чином, для розробки нашої системи правильним вибором є застосування послідовного інтерфейсу I2C на базі розширювача PCF8574. Таке рішення дозволяє вивільнити дефіцитні порти мікроконтролера для підключення датчиків та виконавчих пристроїв. При цьому для забезпечення максимальної стабільності роботи та запобігання проблемам із різним пін-мапінгом рекомендується використовувати бібліотеку `hd44780.h`. Особливу увагу слід приділяти якості та стабільності ліній живлення 5,0 В, оскільки навіть незначне просідання напруги повністю порушує фізичні умови роботи рідкокристалічної матриці та робить дисплей нечитабельним.

ВИСНОВКИ

Для реалізації поставленого завдання розроблено структурну схему системи, згідно якої потрібні наступні модулі: Arduino Uno, зумер, 2 кнопки, LCD дисплей, 2 світлових діоди, силовий ключ, електроригельний замок, оптичний сканер відбитків пальців, джерело безперебійного живлення 220 В/12 В.

В якості мікроконтролера доцільно використати Arduino UNO, що є суттєво кращим модулем для розробки, ніж Arduino Pro Mini, завдяки своїй архітектурній повноті та експлуатаційній гнучкості. Основні переваги UNO – вбудований USB-інтерфейс, потужна система живлення, захист від електричних помилок та ремонтпридатність через DIP-панельку, що роблять його ідеальним для реалізації нашої системи.

Проведений аналіз сканерів відбитків пальця FPM10A, ZFM-20 та R305 показав, що вибір конкретної моделі повинен базуватися на пріоритетах проекту щодо масштабованості, надійності та бюджету. Стосовно нашого завдання найоптимальнішим є використання модуля R305.

Аналіз присутніх на ринку України ригельних електромагнітних замків дозволив обрати в якості виконавчого пристрою електромагнітний замок ригельного типу Yli Electronic YE-302A, призначений для встановлення на дверцята шафок, камери зберігання та хвіртки. Головною перевагою цього замка є те, що при зникненні напруги електромагнітний замок залишається закритим.

Аналіз функціональних можливостей та технічних характеристик рідкокристалічні дисплеїв та індикаторів вказав на доречність застосування символьний LCD-дисплея LCD1602.

Для перевірки працездатності сканера відбитку пальця за допомогою спеціалізованого програмного забезпечення SYNO Demo мікроконтролер потрібно перевести у режим високого імпедансу (байпас) та завантажити в плату відповідний скетч. Після завантаження скетчу утиліта SYNO Demo

отримує прямий доступ до R305, що дозволяє візуалізувати отриманий відбиток пальця, налаштовувати пароль пристрою та проводити первинне тестування датчика.

Реєстрація відбитка пальця є трифазним процесом. Спочатку датчик робить перший оптичний знімок папілярних ліній і створює тимчасову модель у буфері символів №1. Далі потрібно повторно прикласти той самий палець для створення другого знімка та формування моделі в буфері №2. На третьому етапі DSP порівнює обидва зображення на предмет ідентичності та, у разі успішного збігу, записує зашифрований хеш-шаблон у вказану комірку флеш-пам'яті під унікальним ID.

У режимі верифікації сканер очікує прикладання пальця, робить знімок, перетворює його на ознаки та виконує швидке апаратне порівняння з усіма записами у флеш-пам'яті за допомогою виклику методу `fingerFastSearch()`.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Fingerprint Sensor R307 vs AS608: Complete Biometric Module Buyer Guide for Arduino. URL: <https://zbotic.in/fingerprint-sensor-r307-vs-as608-complete-biometric-module-buyer-guide-for-arduino/> (access date: 11.04.2026).
2. CDVI. Security to Access. FAR and FRR in biometric security. URL: <https://www.cdvi.co.uk/blog-far-and-frr-in-biometric-security/> (access date: 11.04.2026).
3. Recogtech. FAR and FRR: security level versus ease of use. URL: <https://recogtech.com/en/insights-en/far-and-frr-security-level-versus-ease-of-use/> (access date: 11.04.2026).
4. Suprema BioEntry W2. URL: <https://autoidindia.com/wp-content/uploads/2017/03/BioEntry-W2-Copy.pdf> (access date: 11.04.26).
5. Optical vs Capacitive Fingerprint Scanners: What You Need to Know. URL: <https://www.miaxis.net/company-news/optical-vs-capacitive-fingerprint-scanners-what-you-need-to-know.html> (access date: 11.04.2026).
6. Види біометричної аутентифікації. URL: <https://nixj.ua/vidi-biometrichno-autentifikas> (дата звернення: 11.04.2026).
7. ProCapture-T Fingerprint Access Control Terminal. URL: <https://zkteco.technology/en/product/procapture-t-2/> (access date: 11.04.2026).
8. Біометричні контролери для систем контролю доступу. URL: <https://securitylab.com.ua/sistemy-kontrolya-dostupa/biometricheskie/kontrollery/> (дата звернення: 11.04.2026).
9. Edinger Smart Fingerprint – замок з зчитувачем відбитку пальця. URL: <https://novi-vorota.com.ua/ua/zamok-edinger-smart-lock.html> (дата звернення: 13.04.2026).
10. Розшифровка ступеня захисту (IP) і класу антивандального захисту (IK). URL: <https://vatra.in.ua/info/statti/rozshyfovka-stupenia-zakhystu-ip-i-klasu-antyvandalnoho-zakhystu-ik/> (дата звернення: 13.04.2026).

11. Розумний біометричний замок SEVEN LOCK SL-7770BF. URL: <https://surl.lt/uyilbj> (дата звернення: 13.04.2026).

12. Інтернет-магазин систем безпеки IP-24. Smart замок ATIS Lock A20T зі сканером відбитку пальця і зчитувачем Mifare. URL: <https://surl.li/tddhmv> (дата звернення: 13.04.2026).

13. Електронний навчальний посібник з дисципліни «Економіка та організація інноваційної діяльності». Комплексне оцінювання ефективності інноваційної діяльності. URL: https://elib.tsatu.edu.ua/dep/feb/ptbd_1/page34.html (дата звернення: 13.04.2026).

14. Arduino Comparison Guide. URL: <https://learn.sparkfun.com/tutorials/arduino-comparison-guide/all?print> (access date: 27.04.2026).

15. What Are the Key Differences Between Arduino Uno and Mini? URL: <https://www.panoxdisplay.com/solution/arduino-uno-vs-mini/> (access date: 27.04.2026).

16. Arduino Uno. URL: <https://components101.com/microcontrollers/arduino-uno> (access date: 27.04.2026).

17. R305 Optical Fingerprint Reader Sensor Module. URL: <https://www.mathaelectronics.com/product/r305-optical-fingerprint-reader-sensor-module/> (access date: 27.04.2026).

18. FPM10A Optical Fingerprint Reader Module. URL: <https://www.robotechbd.com/product/sensors/fpm10a-fingerprint-reader-module-3-3v-5v/> (access date: 27.04.2026).

19. R30X Series Fingerprint Identification Module. User Manual. URL: <https://www.rhydolabz.com/documents/finger-print-module.pdf> (access date: 27.04.2026).

20. Електромеханічний замок Yli Electronic YE-302A. URL: <https://surl.li/fbfjkz> (дата звернення: 02.05.2026).

21. What is the Difference Between a LCD, TFT, IPS, LED and OLED? URL: <https://orientdisplay.com/knowledge-base/lcd-basics/lcd-vs-tft-ips-led-oled-display/>. (access date: 02.05.2026).

22. Adafruit-Fingerprint-Sensor-Library. URL: <https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library>. (access date: 03.05.2026).

23. Fingerprint Sensor R307 vs AS608: Complete Biometric Module Buyer Guide for Arduino. URL: <https://zbotic.in/fingerprint-sensor-r307-vs-as608-complete-biometric-module-buyer-guide-for-arduino/>. (дата звернення: 03.05.2026).

24. Getting Started with Optical Fingerprint Reader – R305. URL: <https://wiki.rhydolabz.com/?p=15770>. (access date: 03.05.2026).

25. LCD 1602 With Arduino Uno R3. URL: <https://www.instructables.com/LCD-1602-With-Arduino-Uno-R3/>. (access date: 04.05.2026).

26. Кваліфікаційна робота: методичні вказівки до виконання кваліфікаційної роботи бакалавра для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія денної та заочної форм навчання / уклад. С.В. Лавренчук, Н.В. Багнюк. Луцьк: ЛНТУ, 2024. 56 с.