КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва випускної кафедри)

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему:

Технологія біометричного контролю доступу на основі відбитків пальців

Піддубний Дмитро Анатолійович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій
(факультет)

Кібербезпеки та комп'ютерної інженерії
(назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ
„ ____ " _____ 20 25 року

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Технологія біометричного контролю доступу на основі відбитків пальців
(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав (-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Піддубний Дмитро Анатолійович
(прізвище, ім'я та по батькові повністю)
125 «Кібербезпека та захист інформації»
(спеціальність)
Безпека інформаційних і комунікаційних систем
(освітня програма)
Група БІКСм-24
Керівник Ізмайлова О. В.
(прізвище та ініціали)
Кандидат технічних наук, доцент
(вчене звання, науковий ступінь)
Рецензент _____
(прізвище та ініціали)

Ідентичність підтверджую

Київ 2025 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: Автоматизації і інформаційних технологій
Кафедра: Кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти: Магістр
Спеціальність: 125 «Кібербезпека та захист інформації»
ОПП: Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри
к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ
„ ____ ” _____ 20 25 року

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА

СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Піддубного Дмитра Анатолійовича

(прізвище, ім'я та по батькові здобувача)

1. Тема роботи «Технологія біометричного контролю доступу на основі відбитків пальців» затверджено наказом ректора КНУБА №1635/23.2/25 від «30» вересня 2025 року
2. Керівник роботи к.т.н. Ізмайлова Ольга Василівна, доцент кафедри кібербезпеки та комп'ютерної інженерії

(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3. Термін подання здобувачем роботи до захисту 15 грудня 2025 року.
4. Зміст пояснювальної записки за розділами:

Р. 1. Теоретичні основи біометричного контролю доступу.
Р. 2. Методи дослідження у сфері біометричного контролю доступу.
Р. 3. Проєктування та реалізація системи біометричного контролю доступу.

5. Графічний матеріал за розділами:

С. 2. Мета роботи

С. 3. Актуальність роботи

С. 4. Аналіз предметної області

С. 6. Відбитки пальців

С. 8. Методи зняття відбитків та їх порівняння

С. 10 Порівняння компонентів МАІ

С. 12 Опис компонентів системи

С. 15 Принципова електрична схема

С. 16 Алгоритм роботи

С. 17 Збірка прототипу

С. 19 Програмне забезпечення системи

С. 20 Тестування прототипу

С. 21 Висновки

6. Консультанти розділів атестаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта	Перевірив	
		дата	підпис
Розділ 1.	Шабала Є.Є., к.т.н, доцент		
Розділ 2.	Шабала Є.Є., к.т.н, доцент		
Розділ 3.	Вишняков В. М., к.т.н, доцент		

7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Теоретичні основи біометричного контролю доступу	15.10.2025 р.
Методи дослідження у сфері біометричного контролю доступу	27.10.2025 р.
Проєктування та реалізація системи біометричного контролю доступу	30.11.2025 р.
Остаточне оформлення роботи	10.12.2025 р.
Направлення роботи на рецензування, перевірка на плагіат	12.12.2025 р.
Попередній захист роботи на кафедрі	15.12.2025 р.

8. Дата видачі завдання: 30 вересня 2025 року.

Керівник _____ _____
(підпис) (прізвище та ініціали)

Студент _____ _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Піддубний Д. А. «Технологія біометричного контролю доступу на основі відбитків пальців».

Атестаційна випускна робота магістра за спеціальністю 125 «Кібербезпека та захист інформації», освітня програма: «Безпека інформаційних і комунікаційних систем». – Київський національний університет будівництва та архітектури. – Київ, 2025 рік.

Робота присвячена дослідженню технології біометричного контролю доступу на основі відбитків пальців та створенню доступної системи для захисту інформації від несанкціонованого доступу. Метою роботи є аналіз сучасних методів біометричної ідентифікації та подальша фізична реалізація системи контролю доступу, що забезпечує надійність, простоту використання та низьку собівартість.

У процесі дослідження проаналізовано системи контролю і управління доступом, розглянуто сучасні методи біометричної ідентифікації та виконано їх порівняння. Визначено основні вимоги до систем контролю доступу. Проведено класифікацію папілярних узорів, досліджено особливості відбитків пальців, принципи їх порівняння та здійснено аналіз власного відбитка. Виконано порівняльний аналіз методів надання доступу та технологій зняття відбитків пальців.

У практичній частині роботи здійснено вибір компонентів для побудови системи, розроблено алгоритм її функціонування, структурну та електричну схеми, а також створено програмну реалізацію прототипу.

Результатом роботи є функціонуюча система біометричного контролю доступу на основі відбитків пальців, що може бути використана для захисту персональної інформації та забезпечення фізичної безпеки об’єктів.

Ключові слова: біометрія, відбиток пальця, СКУД, ідентифікація, автентифікація, верифікація, інформаційна безпека, біометричні система.

ABSTRACT

Piddubnyi D. A. "Biometric access control technology based on fingerprints".

Master's degree final thesis in specialty 125 " Cybersecurity and information protection", educational program: "Security of information and communication systems". - Kyiv National University of Civil Engineering and Architecture. - Kyiv, 2025.

The work is devoted to the study of biometric access control technology based on fingerprints and the creation of an accessible system for protecting information from unauthorized access. The method of work is the analysis of modern methods of biometric identification and the subsequent physical implementation of the access control system, which ensures reliability, ease of use and low cost.

In the process of research, access control and management systems were analyzed, modern methods of biometric identification were understood and their comparison was performed. The main requirements for the access control system were determined. A classification of papillary patterns was carried out, the features of fingerprints were studied, the principles of their comparison were studied, and an analysis of one's own fingerprint was performed. A comparative analysis of access control methods and fingerprint technologies was performed.

In the practical part of the work, components were selected for building the system, an algorithm for its functioning, a structural and electrical diagram were developed, and a software implementation of the prototype was created.

The result of the work is a functional biometric control system based on fingerprints, which can be used to protect personal information and ensure the physical security of objects.

Keywords: biometrics, fingerprint, ACS, identification, authentication, verification, information security, biometric systems.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	ПІБ Піддубний Дмитро Анатолійович Piddubnyi Dmytro		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	Технологія біометричного контролю доступу на основі відбитків пальців		
	Biometric access control technology based on fingerprints		
Освітній ступінь	Магістр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека та захист інформації»		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	Ізмайлова Ольга Василівна		
Обсяг роботи:	*Пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	110 (131 з додатками)	3	23
Розділ 1	Теоретичні основи біометричного контролю доступу.		
Розділ 2	Методи дослідження у сфері біометричного контролю доступу.		
Розділ 3	Проєктування та реалізація системи біометричного контролю доступу.		
Висновки по роботі	У ході виконання дипломної роботи проаналізовано сучасні системи контролю доступу та біометричні методи аутентифікації. Розроблено та досліджено біометричну систему контролю доступу на основі відбитка пальця з використанням платформи Arduino.		
Ключові слова: Keywords:	біометрія, відбиток пальця, СКУД, ідентифікація, автентифікація, верифікація, інформаційна безпека, біометричні система. biometrics, fingerprint, ACS, identification, authentication, verification, information security, biometric systems.		

Здобувач _____/ _____

Керівник _____/ _____

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

СКД – система контролю доступу

СКУД – система контролю і управління доступом

ПІН – персональний ідентифікаційний номер

ПК – персональний комп’ютер

MAI – метод аналізу ієрархії

FAR – False Acceptance Rate

TAR – True Acceptance Rate

EER – Equal Error Rate

FRR – False Rejection Rate

RFID – Radio frequency identification

ISO – International Organization for Standardization

IEC – International Electrotechnical Commission

USB – Universal Serial Bus

UART – Universal Asynchronous Receiver-Transmitter

TTL – Time to live

SPI – Serial Peripheral Interface

ВСТУП

У сучасному світі, де інформаційна безпека набуває все більшого значення, технології біометричної ідентифікації користувачів стають незамінною складовою систем контролю та управління доступом.

Системи, які базуються на використанні паролів або ключ карток мають свої недоліки, такі як: можливість втрати, крадіжки або підробки ідентифікатора, що зменшує рівень захисту інформації або об’єкта, тому використання паролів та карток відходить на другий план. Біометричні системи навпаки, використовують фізіологічні характеристики людини, які практично не можна підробити. Це робить їх ефективними у підвищенні рівня безпеки та пояснює їхню популярність на сьогодні.

Найбільш поширеним на ринку України біометричним параметром, який використовується в комерційних системах контролю доступу є відбиток пальця. Використання відбитка пальця як біометричного ідентифікатора є актуальним та надійним методом для захисту інформації або певного об’єкта, який забезпечує високий рівень захищеності, точності та зручності використання системи.

Існуючі комерційні системи біометричного доступу є дуже дорогими, мають складну будову та потребують централізованого сервера для зберігання та обробки інформації, ці фактори обмежують застосування таких систем в малих установах, а тим більше у приватній власності.

Запропонована в даному проєкті система базується на недорогих компонентах, що дозволяє створити доступну, автономну систему контролю доступу без втрати її функціональності. Таким чином дана розробка заповнює технічну прогалину у бюджетному сегменті ринку біометричних систем.

Метою даної дипломної роботи є дослідження технологій біометричного контролю доступу на основі відбитків пальців з подальшою фізичною реалізацією. Проєкт передбачає створення системи контролю доступу на основі відбитків пальців, яку зможе дозволити собі кожен бажаючий користувач для захисту особистої інформації від несанкціонованого доступу.

Для досягнення мети проєкту були вирішені наступні завдання:

– проаналізована системи контролю і управління доступом;

– розглянуто існуючі методи біометричної ідентифікації та проведено порівняння між ними;

– визначено вимоги до систем контролю доступу;

– досліджено та класифіковано папілярні узори, розглянуто ознаки відбитків та принципи їх порівняння, проведено аналіз власного відбитку пальця;

– проведено аналіз методів надання доступу та методів зняття відбитків, проведено їх порівняння та обрано найбільш підходящий;

– обрано компоненти для реалізації системи, створено алгоритм роботи, схему з'єднань компонентів та програмну реалізацію.

Об'єктом дослідження є процес забезпечення доступу в системі контролю доступу з використанням біометричних технологій.

Предметом дослідження є оптимізація технології біометричного контролю доступу на основі відбитків пальців, її програмно-апаратна реалізація, та експериментальне дослідження результатів на її основі.

В рамках даного проєкту проведено теоретичний аналіз систем контролю доступу, розглянуто їх класифікацію та області застосування. Виконано аналіз сучасних біометричних методів ідентифікації людини, розглянуто їх класифікацію та проведено їх порівняння.

Далі в проєкті зосереджено увагу на методах, які використовуються під час його виконання. Розглянуто методи надання доступу. Проведено опис та порівняння методів зняття відбитків пальців. Досліджено глобальні та локальні ознаки відбитків, описані принципи порівняння з цими ознаками. Виконано зняття власного відбитка пальця та проведено його аналіз з виявленням характерних глобальних та локальних ознак. Здійснено вибір компонентів системи, ключові з яких було обрано за допомогою МАІ.

Наступним кроком проєкту є проєктування та реалізація біометричної СКД на основі відбитків пальців. Була сформована концепція проєкту. Розроблено

структурну, принципову та електричну монтажну схему прототипу. Наведено та описано алгоритм роботи системи. Виконано розробку програмного забезпечення. Проведено збірку та програмування прототипу системи. Здійснено тестування прототипу та проведено розрахунки затрат на створення власної біометричної системи контролю доступу на основі відбитків пальців.

Наукова новизна отриманих результатів полягає в отриманні комплексної технології бюджетної біометричної системи контролю доступу, орієнтовану на автономну роботу без підключення до неї серверних баз даних. Удосконалено метод побудови апаратно-програмної частини проєкту з використанням бюджетних та відкритих платформ, що дозволяє адаптувати систему під різні умови використання.

Результати роботи мають практичне значення для приватних будинків, навчальних закладів, офісів та малих підприємств, яким необхідно забезпечити персоналізований доступ до приміщень або інформації. Запропоновану систему можна реалізувати у вигляді окремого пристрою або як модуль у складі більш складних комплексів. Вона відзначається простотою монтажу, низькою собівартістю та високим рівнем надійності. Отримані результати можуть бути впроваджені на рівні приватного будинку для доступу до робочого кабінету, або наприклад для університетських лабораторій як контроль доступу до обладнання.

1. ТЕОРЕТИЧНІ ОСНОВИ БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ

1.1 Аналіз проблем, постанова задачі та цілі дослідження

На сьогодні питання безпеки та контролю доступу до інформації або приміщень набуває особливої актуальності. Системи контролю доступу є ключовим елементом у забезпеченні захисту від несанкціонованого доступу чи використання інформації. Традиційні методи автентифікації (паролі, картки або брелки) мають низку своїх недоліків, які вагомо впливають на захист. Вони можуть бути загублені, підроблені, скопійовані або передані навмисно іншій особі, що знижує загальний рівень безпеки.

Одним з самих надійних способів ідентифікації особи є біометрична автентифікація, яка базується на фізіологічних особливостях людини, таких як: відбитки пальців, обличчя, голос, райдужна оболонка ока і так далі. Ці ознаки є унікальними для кожного індивіда та практично не піддаються підробкам, через це біометричні системи надзвичайно ефективні в роботі. Однак існуючі промислові рішення систем біометричної ідентифікації є дуже дорогими, вимагають складного програмного забезпечення, спеціального дорогого обладнання, регулярної технічної підтримки, що обмежує їх використання у побутових умовах.

Таким чином, актуальною науково-технічною задачею є дослідження існуючих та створення доступної та недорогої біометричної системи контролю доступу, яка буде забезпечувати належний рівень безпеки при мінімальних фінансових вкладеннях. Особливу увагу слід приділити простоті конструкції, використанню відкритих апаратних платформ і недорогих, але достатньо якісних біометричних модулів.

Об’єктом дослідження є процес забезпечення доступу в системі контролю доступу з використанням біометричних технологій.

Предметом дослідження є оптимізація технології біометричного контролю доступу на основі відбитків пальців, її програмно-апаратна реалізація, та експериментальне дослідження результатів на її основі.

Метою дослідження є розроблення доступної технології біометричного контролю доступу, яка може бути реалізована широким колом користувачів, зокрема у навчальних аудиторіях, офісах чи побутових умовах.

Аналіз сучасного розробок показує, що на ринку представлені чисельні рішення від таких виробників, як ZKTeco [1], HID Global [2], Suprema [3], які пропонують високоточні системи з функцією багатофакторної автентифікації. Проте їхня вартість залишається надто високою для освітніх установ або невеликих підприємств, а тим більше для приватних квартир або будинків. Водночас, зарубіжні дослідження демонструють ефективність використання бюджетних апаратних компонентів у поєднанні з мікроконтролерами відкритої архітектури для побудови локальних систем контролю доступу [4-6].

Вітчизняні публікації останніх років також показують зростання інтересу до створення спрощених біометричних систем для навчальних і лабораторних потреб. Зокрема, українські розробники успішно застосовують модулі зчитування відбитків пальців у поєднанні з платформами Arduino для реалізації прототипів систем доступу з можливістю керування електромагнітним замком [7, 8].

Отже, аналіз наукових і технічних джерел свідчить, що сьогодні існує реальна можливість створення бюджетної технології біометричного контролю доступу, яка за своєю функціональністю не поступатиметься дорогим промисловим аналогам. Основною перевагою такого підходу є доступність, простота реалізації та масштабованість. Це дозволяє рекомендувати подальший розвиток дослідження у напрямі розроблення економічної та ефективної системи біометричної автентифікації на основі відбитка пальця, призначеної для використання у повсякденному середовищі.

Для подальшого дослідження необхідно розглянути загальні принципи побудови та класифікації систем контролю і управління доступом, які становлять теоретичну основу будь-яких біометричних технологій. Аналіз їхніх функцій, структури та видів дозволить глибше зрозуміти місце біометричних рішень серед інших типів систем і визначити вимоги до розроблення доступної системи на основі відбитка пальця.

1.2 Поняття та класифікація систем контролю і управління доступом

Система контролю і управління доступом (СКУД або СКД) – це сукупність програмних та апаратних засобів безпеки, що регулюють вхід/вихід людей та забезпечує регулювання прав доступу до ресурсів, приміщень або інформаційних систем [9]. Головною метою СКД є обмеження доступу до захищених об’єктів для несанкціонованих осіб та надання доступу лише авторизованим користувачам. Дана система ідентифікує осіб, перевіряє їхні права доступу, а також реєструє всі події, що дозволяє контролювати робочий час та контролювати доступ до певних захищених зон.

На сьогодні існує широке різноманіття систем контролю доступу, зокрема:

– локальні і мережеві;

– дротові та радіоканальні;

– біометричні;

– спеціальні, з застосуванням ПІН-кодів, магнітних карт чи брелків.

Кожна вище вказана система контролю доступу має свої особливості та області застосування, наприклад:

– Локальні – працюють автономно, дані зберігаються на місці, контролер не має підключення до центральної мережі. Областями застосування таких систем є виключно невеликі офіси, приватні складські приміщення, де немає потреби в централізованому адмініструванні;

– Мережеві – підключені до кооперативної мережі або інтернету, дані централізовано обробляються та зберігаються. Застосовуються дані системи на великих підприємствах, в готелях, аеропортах, в місцях де важлива централізована обробка інформації та одночасний контроль доступу до багатьох точок;

– Дротові – передача даних відбувається по кабелю, дані системи характерні високою стабільністю та безпекою. Застосовуються в офісах, банківських установах, критично важливих об’єктах;

– Радіоканальні (бездротові) – використовують Wi-Fi, Bluetooth, RFID, зручні для встановлення, але мають підвищену вразливість до перешкод і злому.

Використовуються такі системи на тимчасових об’єктах та для модернізації старих приміщень без прокладання кабелю;

– Біометричні – використовують унікальні фізіологічні або поведінкові характеристики людини, такі як: відбитки пальців, райдужка ока, обличчя, голос і так далі. Таким системам властива висока надійність та стійкість до підробок. Застосовуються такі системи на об’єктах з високою потребою в безпеці: критична інфраструктура, військові бази, фінансові установи;

– Спеціальні (ПІН-коди, магнітні картки, брелок) – ці системи є зручними у використані, але захищеність таких систем є посередньою. ПІН-коди можуть бути підібрані, карткам та брелкам властиве клонування. Найбільше застосування даних систем припадає на готелі, житлові комплекси, офіси.

Принцип роботи СКУД такий: людина, яка має намір потрапити на той або інший об’єкт, сканує за допомогою спеціального пристрою певний ідентифікатор (ПІН-код, відбиток пальця або картку), далі зчитана інформація потрапляє на електронний пристрій, котрий звіряє отриману інформацію з базою даних. Далі система приймає рішення, надавати людині допуск до приміщення або ні.

Загалом для побудови СКУД потрібні такі технічні засоби:

1. Ідентифікатор, яким може виступати пластикова картка, спеціальний брелок, біометрика тощо;

2. Зчитувач – це спеціальний пристрій, який зчитуватиме ідентифікатор;

3. Контролер, який буде опрацьовувати отримані із зчитувача дані та приймати подальше рішення щодо надання доступу.

Розглянемо загальні переваги та недоліки для всіх системи контролю і управління доступом [10].

Основними перевагами даних системи є:

– Підвищення безпеки – приміщення з такою системою захищені від несанкціонованого доступу;

– Гнучке керування доступом – кожному користувачу можна задати право доступу до того або іншого приміщення;

– Ведення обліку – дана система реєструє всі події які відбуваються (час входу/виходу, спроби несанкціонованого доступу);

– Зручність у використанні – доступ до того або іншого об’єкта здійснюється швидко;

– Інтеграція з іншими системами – в дану систему можна інтегрувати допоміжні підсистеми, такі як сигналізація або відеоспостереження;

– Автоматизація обліку робочого часу – компанії можуть слідкувати за дотриманням робочих годин.

Недоліки даної системи:

– Вартість впровадження – обладнання та монтаж такого роду систем потребує значних інвестицій;

– Залежність від електроживлення – при збоях або відключенні електроенергії можливі проблеми з допуском;

– Необхідність регулярного технічного обслуговування – зчитувачі, замки, серверне обладнання потребують регулярної технічної та програмної підтримки.

1.3 Сутність та різновиди біометричних методів ідентифікації

«Біометрія» як поняття почало впроваджуватись в кінці XIX століття, розуміли під ним розділ науки, що займається експериментами в яких залучаються математичні статистики. Значно цікавість до біометрії зросла у кінці XX століття завдяки тому, що ця галузь почала використовуватись в розробках новітніх технологій безпеки, ідея яких зводилась до розпізнавання особи за унікальними параметрами генетичного коду.

Біометрія – це метод ідентифікація особи на основі унікальних біологічних або поведінкових характеристик, які притаманні лише конкретній людині.

Фізіологічні та поведінкові особливості людини, такі як: папілярний візерунок пальця, геометрія обличчя, райдужна оболонки ока, форма долоні, сітківка ока, ДНК, структура кровоносних судин, форма вуха, особливості клавіатурного набору

та підпису, є постійними та практично незмінними з часом характеристики кожної окремої особи.

Біометрія зараз це сукупність методів та засобів ідентифікації або верифікації людини, що базується на поведінкових та фізіологічних характеристиках людини.

Ідентифікація – це встановлення особи шляхом порівняння наданих параметрів, в тому числі і біометричних, з наявною інформацією в базах даних.

Верифікація – це порівняння параметрів, в тому чисті біометричних, для встановлення відповідності між особою та інформацією в базах даних для підтвердження їх ідентичності.

Біометрія являє собою одну з найбільш перспективних інформаційних технологій ідентифікації, яка активно розвивається та удосконалюється. Пристрої біометричної ідентифікації і верифікації використовуються вже майже п’ятдесят років. У XXI столітті біометрія набула швидкої популярності і стала застосовуватися у різноманітних сферах життя: від паспортів нового покоління до попереджень та розкриття злочинних дій та намірів окремих верст населення.

Зараз системи доступу та захисту до інформації, що використовують біометрію та її технології є найбільш надійними, а також і найбільш зручними для користувача, немає необхідності запам’ятовувати паролі, носити з собою картки або ключі. Для доступу потрібно лише просканувати палець або руку, обличчя або сітківку ока, та отримати доступ до території чи об’єкта під охороною, або доступ до комп’ютерної мережі та інформації з обмеженим доступом.

Головними причинами популярності біометричних технологій є: їх надійність, безпечність, комфортність та ефективність. В порівнянні з іншими технологіями біометрія працює безпосередньо з людиною та ідентифікує її індивідуальні ознаки, інакше біометричні пристрої не змогли б працювати.

Біометричне розпізнавання людини полягає в порівнянні фізіологічних та психологічних особливостей суб’єкта, який перевіряється, з його раніше наданими характеристиками, які розміщені у електронному вигляді в спеціалізованих базах даних біометричних систем. Головною метою біометричної ідентифікації є створення такої системи, яка б працювала безвідмовно та надавала доступ

ідентифікованим користувачам та водночас повністю виключала можливість несанкціонованого доступу до приміщень, комп'ютерних мереж або архівів інформації. Вважається, що порівняно з картками або паролями біометричні системи забезпечують вищий рівень захисту, оскільки фізіологічні та поведінкові характеристики людини не можна втратити, забути або підробити.

Існує багато методів біометричної автентифікації та ідентифікації, які можна розділити на дві групи, такі як: статичні та динамічні.

Статичні методи базуються на фізіологічній характеристиці людини, а саме унікальній характеристиці, яка надана людині від народження та не змінюється з часом.

Ці методи засновані на розпізнаванні, а саме:

– Відбитка пальця – в основі цього методу є унікальність малюнка папілярних узорів на пальцях кожної людини. Відбиток знятий за допомогою сканера, перетворюється на цифровий код, а далі порівнюється з раніше збереженим шаблоном, який був отриманий та зберігається в базі даних. Ця технологія була і залишається найбільш популярною на ринку в порівнянні з іншими методами;

– Долоні – даний метод застосовується рідко, базується він на індивідуальній геометрії долоні. За допомогою спеціального сканера, відтворюється тривимірне зображення долоні, далі за ним формується згортка, а вже по ній відбувається розпізнавання особи;

– Малюнку вен на долоні – спеціальна інфрачервона камера виконує зчитування малюнку вен на внутрішній частині долоні, далі зображення обробляється і за отриманим шаблоном розташування вен формується цифрова згортка, яка далі зберігається в базі даних, та вже по ній відбувається процес розпізнавання людини;

– Райдужної оболонки ока – візерунок райдужки є унікальною ознакою кожної людини. Для її розпізнавання достатньо портативної камери та спеціального програмного забезпечення, яка буде здійснювати сканування вказаної

ділянки обличчя, виокремлювати зображення ока людини, а потім виділяти малюнок райдужки, на основі якого формується цифровий ідентифікатор людини;

– Сітківки ока – це метод, який базується на малюнку кровоносних судин очного дна. Для того, щоб отримати зображення цього малюнка людина повинна поглянути на спеціальне джерело світла, яке підсвітить очне дно, а спеціальна камера зафіксує отриманий малюнок. Зараз цей метод майже не використовується;

– За формою обличчя – цей метод працює з двовимірним або тривимірним зображенням обличчя людини. На обличчі виділяються основні риси, такі як: контури очей, губ, носа і так далі, також вираховується відстань між ними. У результаті формується не тільки базове зображення обличчя, а також декілька варіантів які враховують зміни положення голови;

– ДНК – цей метод беззаперечний лідер в надійності, оскільки генетичний код неможливо підробити. Однак він є і найбільш складним, трудомістким та потребує значний затрат часу, що унеможливлює його використання в реальному часі.

Динамічні методи біометричної автентифікації базуються на аналізі поведінкових особливостей людини, які проявляються під час виконання рухів або інших дій. Такі методи побудовані на використанні характеристик, які супроводжують виконання певних дій та пов’язані з характерною людині манерою рухів. Якщо порівнювати з статичними, динамічні методи мають нижчу точність та ефективність, тому їх зазвичай застосовують як допоміжні засоби автентифікації.

До цих методів належать:

– За рукописним почерком – зазвичай для цього виду автентифікації або ідентифікації особи використовується її підпис (іноді написання кодового слова). Цифровий ідентифікаційний код формується залежно від необхідного рівня захисту та наявності відповідного апаратного забезпечення. Ідентифікація за цим методом може бути двох типів:

- за самим підписом, коли для ідентифікації використовується ступінь збігу двох графічних зображень;

- за динамічними характеристиками підпису, тобто для ідентифікації формується цифрова згортка, яка містить часові параметри підпису та статичні характеристики сили натискання на поверхню графічного планшету під час виконання підпису;

– За клавіатурним почерком або динаміка клавіатурного набору тексту – цей метод схожий на попередній метод, проте замість підпису використовується набір певного кодового слова. Якщо застосовується особистий пароль користувача, тоді така автентифікація вважається двофакторною. Метод не потребує спеціального обладнання, окрім стандартної клавіатури. Основною характеристикою для формування згортки є динаміка набору кодового слова;

– За голосом – цей метод є одним з найстаріших методів біометричної автентифікації, зараз розвиток цього методу вийшов на новий рівень через збільшення потреби у його використанні. Для формування ідентифікаційного коду використовують поєднання частотних та статичних характеристик голосу;

– За допомогою інших методів – крім перелічених вище поширених динамічних методів, ще існують ще такі способи ідентифікації, як: ідентифікація за рухом губ під час вимовляння кодового слова, за ходою, за динамікою повороту ключа в дверному замку тощо [11].

Потрібно сказати, що статичні методи ідентифікації є набагато надійніші та якісніші за динамічні, але вони є значно дорожчими. Дослідження біометричного ринку України на 2024 рік показали, що використання біометричних методів ідентифікації за остання два роки продовжує зростати і на 39% підприємств України вже запроваджено дану технологію [12].

Світові ж дослідження вказують відсоткові співвідношення застосування різних біометричних методів, де домінує переважно метод відбитків пальців, що показано на рисунку 1.1 [13].

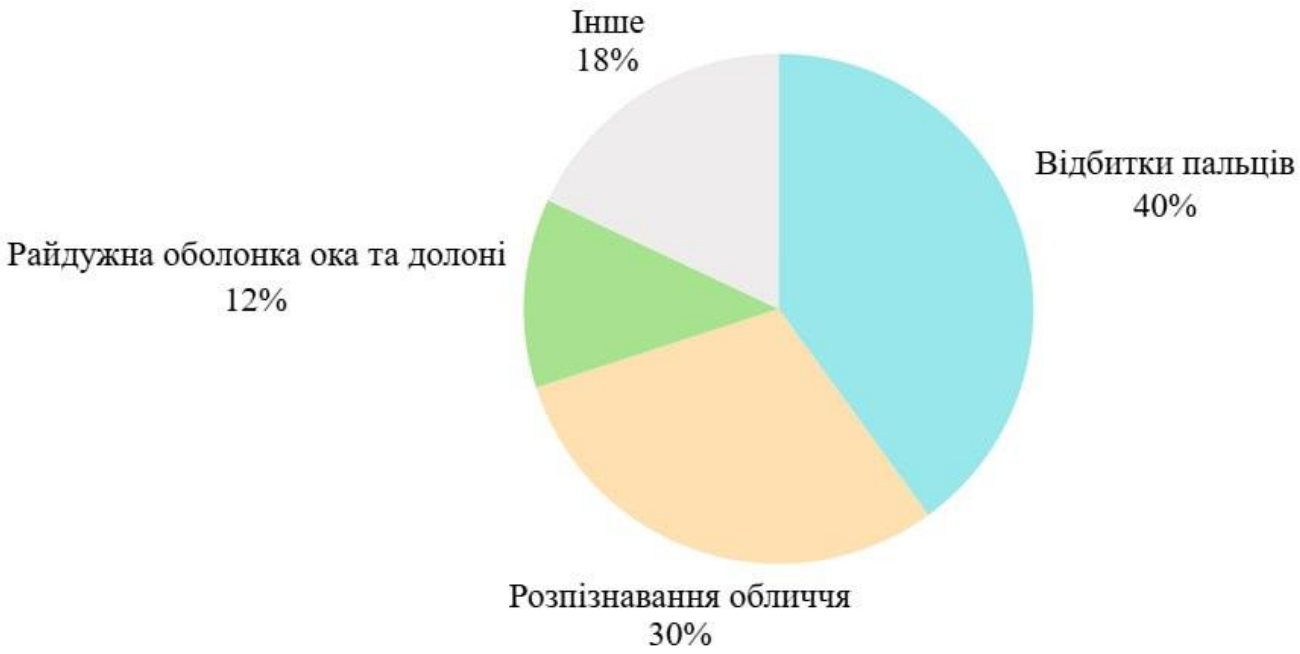


Рисунок 1.1 – Сегментація біометричного ринку на 2024 рік за поширенням використання біометричних ідентифікаторів

1.4 Структура та принцип роботи біометричної системи

Будь-яка біометрична система повинна забезпечувати розпізнавання людини за наявним шаблоном та визначати достовірність її фізіологічних та поведінкових характеристик. Біометричні системи поділяються на дві частини: модуль реєстрації та модуль верифікації (ідентифікації), показано на рисунку 1.2.

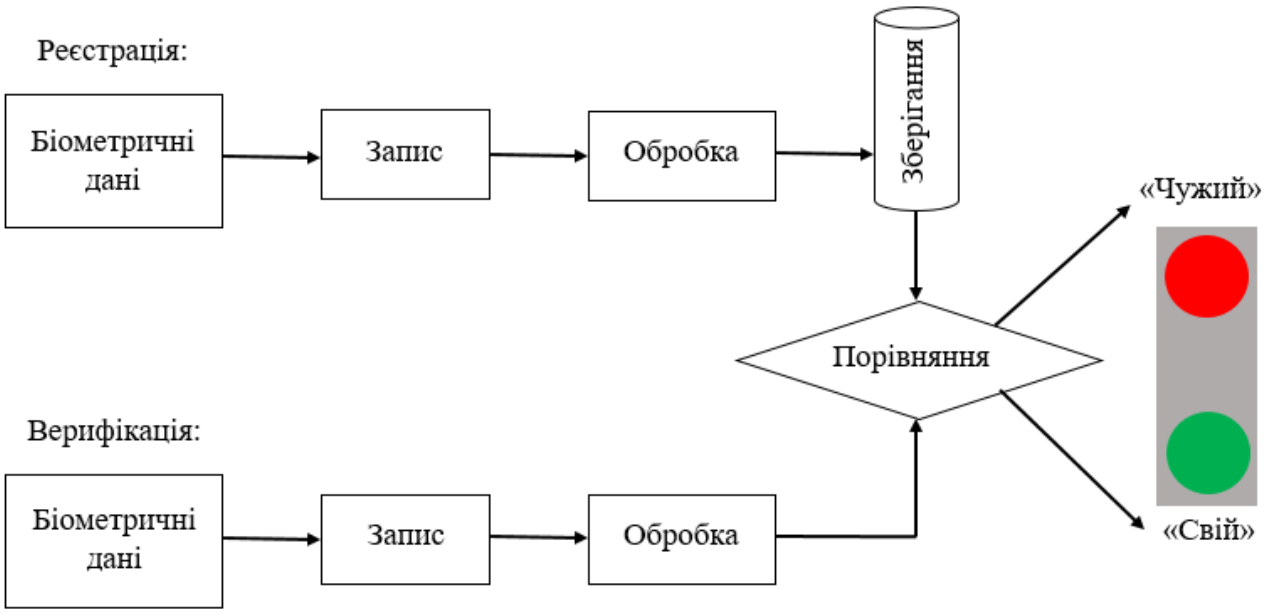


Рисунок 1.2 – Блок-схема біометричної системи

Модуль реєстрації відповідає за те щоб система навчилась ідентифікувати конкретну людину. На цьому етапі біометричні датчики сканують необхідні фізіологічні або поведінкові характеристики користувача та перетворюють їх у цифровий формат. Спеціальний алгоритм обробляє отриману інформацію, виокремлює характерні ознаки та формує цифрове представлення, так званий шаблон. Електронний шаблон кожного користувача зберігається в базі даних біометричної системи.

Модуль верифікації відповідає за розпізнавання користувача. Біометричний датчик на цьому етані знімає та реєструє характеристики людини, далі перетворює їх у той формат, в якому зберігається цифровий шаблон. Отриманий шаблон порівнюється з шаблоном який зберігається в базі даних для підтвердження користувача.

Реалізація всіх біометричних технологій ідентифікації проходить в основні чотири етапи:

– реєстрація ідентифікатора (запис) – збір фізіологічних або поведінкових характеристик, які далі перетворюється в шаблон, котрий доступний комп’ютерним технологіям та який зберігається в пам’яті біометричної системи.

Потрібно зазначити реєстрація в деяких методах може відрізнятися. До прикладу метод відбитка пальця є контактним, а метод сітківки ока – безконтактним;

– виокремлення – з ідентифікатора, який пред'являється людиною для контролю, формуються та виокремлюються унікальні ознаки, які далі аналізуються системою. Потім ознаки для кожного методи відрізняються, наприклад для методу відбитків пальців виокремлюється унікальний малюнок завитків, а для методу райдужки ока виокремлюється малюнок кровоносних судин ока;

– порівняння – порівнюються відомості представленого ідентифікатора з тим який був зареєстрований раніше;

– ухвалення рішення – ухвалення рішення про збіг або незбіг ідентифікатора, який був пред'являється, та того який був раніше зареєстрований [14].

1.5 Вимоги до систем контролю доступу та аналіз загроз

Система контролю доступу повинна забезпечувати надійний захист інформації та об'єктів від несанкціонованого доступу. Основними вимогами до СКУД є:

– Ідентифікація та верифікація. Система повинна чітко ідентифікувати користувача, який намагається отримати доступ (за допомогою паролів, карток, біометричних даних і так далі);

– Управління доступом. Система повинна дозволяти створювати та керувати різними рівнями доступу для різних категорій користувачів, враховуючи їхній статус, обов'язки та ролі. Права доступу повинні легко налаштовуватись для забезпечення доступу уповноваженим особам до конкретних зон;

– Контроль та моніторинг. Система повинна регулювати вхід та вихід користувачів, реєструвати всі події, як успішні так і несанкціоновані;

– Безпека та захист. Основне завдання системи запобігати несанкціонованому доступу та захищати певний об'єкт від проникнення. Важливою вимогою також є забезпечення захисту інформації, яка обробляється самою системою;

– Масштабованість. Система має легко збільшувати свої ресурси та продуктивність у відповідності до навантажень на неї. Також система має взаємодіяти з іншими системами безпеки, такими як сигналізація або відеоспостереження;

– Зручність використання. Користувачі повинні швидко та інтуїтивно отримувати доступ до об’єкта;

– Відповідність стандартам безпеки. Система повинна відповідати міжнародним на національним нормам, наприклад ISO/IEC 27001 [15].

Якщо ми говоримо про безпеку та захист системи то слід звернути увагу на метрики ефективності системи, такі як FAR, FRR та EER.

FAR (False Acceptance Rate – коефіцієнт помилкового прийняття) – визначає, наскільки добре ваша система може ідентифікувати самозванців. Це відсоток випадків, коли самозванець помилково приймається системою.

FRR (False Rejection Rate – коефіцієнт помилкових відмов) – це відношення кількості помилкових відмов, поділених на загальну кількість спроб. FRR розраховується шляхом ділення кількості помилкових відхилень на загальну кількість спроб. Якщо низький FRR, це означає, що система відхиляє більше людей, ніж має бути.

FAR і FRR безпосередньо пов’язані. Як один підніметься, то другий опуститься. Точка, в якій ці дві лінії перетинаються, відома як рівна частота помилок (EER). Тут відсоток хибних прийомів і хибних відмов однаковий.

FAR і FRR є двома важливими показниками, які можна використовувати для оцінки ефективності системи. Ці показники зазвичай налаштовуються в програмному забезпеченні шляхом налаштування порогового значення системи. Варто зазначити, FAR і FRR впливатимуть на рівень безпеки системи. Це означає, що коли ви збільшуєте або зменшуєте ці показники, кількість придатних спроб автентифікації відповідно зменшуватиметься або збільшуватиметься.

Високий FAR означає, що система, швидше за все, неправильно прийме неавторизованого користувача, що може поставити під загрозу безпеку системи. Низький FAR із низьким FRR вказує на високий рівень безпеки. Встановлюючи

порогові значення для певної системи, важливо знайти баланс між рівнем помилкового прийняття (FAR) і коефіцієнтом помилкового відхилення (FRR). Компроміс між безпекою та зручністю використання має відображатися у виборі порогового значення [13].

Перейдемо до аналізу загроз СКУД:

– Несанкціонований доступ. Отримання доступу до даних або системи без відповідних прав, що може призвести до їх зміни, викрадення, видалення або розповсюдження;

– Кібератаки та програмні загрози:

- Спрямовані атаки на перехоплення даних між зчитувачем, контролером і сервером, що дозволяє отримати ідентифікатори чи паролі;
- Атаки спрямовані на перевантаження серверів чи мережевої складової системи, що робить систему недоступною користувачам;
- Використання шкідливого програмного забезпечення (віруси, трояни), що дозволяє віддалено змінювати права доступу;

– Технічні загрози:

- Підключення до контролера чи сканера з метою обходу авторизації.
- Вивід з ладу сканера, контролера або замка, що приводить до відмови в доступі або неконтрольованого доступу.
- Перехоплення сигналу під час зчитування сканером даних з картки, брелка або біометричної ознаки і контролером;
- Виготовлення підробки ідентифікатора: копій ключ-карт, клонування брелків, використання підробок біометричних даних (муляжі відбитків, запис голосу, фото обличчя, 3D-муляжі);

– Організаційні загрози:

- Вплив соціальної інженерії на користувачів системи з метою отримання паролів, карток доступу або біометричних даних;
- Людська необережність, халатність у відношенні до ідентифікаторів;

1.6 Дактилоскопія як метод ідентифікації особи

1.6.1 Властивості та класифікація папілярних узорів

Дактилоскопія є одним із найстаріших та водночас найнадійніших методів ідентифікації людини. Узори на внутрішній стороні рук та пальців були відомі ще представникам стародавньої медицини.

Наприкінці XX століття поняття «дактилоскопія» (від грецького «daktylos – палець» і «skopeo – дивлюся») – це розділ криміналістики та біометрії, що визначає будову узорів внутрішніх поверхонь нігтьових фаланг пальців рук, для ідентифікації особистості, кримінальної реєстрації та розшуку злочинця. На долонній поверхні кінцевих фаланг пальців рук є рельєфні лінії – так звані папілярні, побудова яких обумовлена рядами виступів шкіри, розділених своєрідними заглибленнями.

Папілярні лінії утворюють складні шкірні візерунки, які в свою чергу мають такі властивості:

– індивідуальність – сукупність папілярних ліній, які створюють неповторний малюнок за їх конфігурацією та розташуванням, який практично ніколи не повторюється в інших узорах;

– порівняну стійкість – зовнішня будова папілярного узору, яка формується ще в період внутрішньоутробного розвитку та зберігається впродовж усього життя людини;

– відновлюваність – при поверхневих пошкодженнях шкіри папілярні лінії через деякий час відновлюються у своєму попередньому вигляді.

Незважаючи на широке різноманіття папілярних узорів, їх можна чітко класифікувати, що полегшить процес ідентифікації. Всі узори, поділяються на три основні типи: дугові, петльові та завиткові, ці типи є фундаментом їх класифікації.

Дугові узори формуються потоком папілярних ліній і в центральній частині узору мають вигин, так звану внутрішню дугу. Будова і форма цієї дуги розділює їх на підтипи. Згідно з українською системою класифікації (у різних країнах різні

системи класифікації) дугові узор можуть бути: простими, шатровими, із невизначеною побудовою центру, помилково-петльовими, помилково-завитковими і аномальними.

Петльові узори формуються з папілярних ліній, які починаються з одного краю пальця, далі огинають центр, утворюють петлю та повертаються до краю пальця з якого починались. Петльовий узор формується багатьох петель, які розташовані одна в одній. Для віднесення узору до петльового необхідною є наявність в центрі узору щонайменше однієї повної петлі. Залежно від форми петель, взаємного розташування їх ніжок та орієнтації в площині петльові узори розділяють на дев'ять підтипів: простий, зігнутий, половинчастий, замкнутий, з системою петель паралельні петлі, з системою петель «зустрічні петлі», помилково-завиткові та петльові узори, що нечасто спостерігалося.

Завиткові узори формуються потоком папілярних ліній, які в центральній частині згинаються у вигляді кіл, овалів або спіралей, що огинають один одного чи утворюють різні комбінації. Різноманіття завиткових узорів зумовлено особливостями їх внутрішньої структури. Визначають 12 підвидів завиткових узорів: простий узор – коло, простий узор – овал, простий узор – спіраль, петля-спіраль, петлі-спіралі, петля-равлик, зігнута петля, неповний завитковий узор, петлі-клубки з різностороннім і одностороннім розташуванням ніжок петель і завиткові узори, які часто простежуються. Варто зазначити, що в різних країнах застосовується різні системи класифікації, тому підвиди папілярних узорів можуть відрізнятися [11].

Всі вище вказані типи папілярних узорів показано на рисунку 1.3.

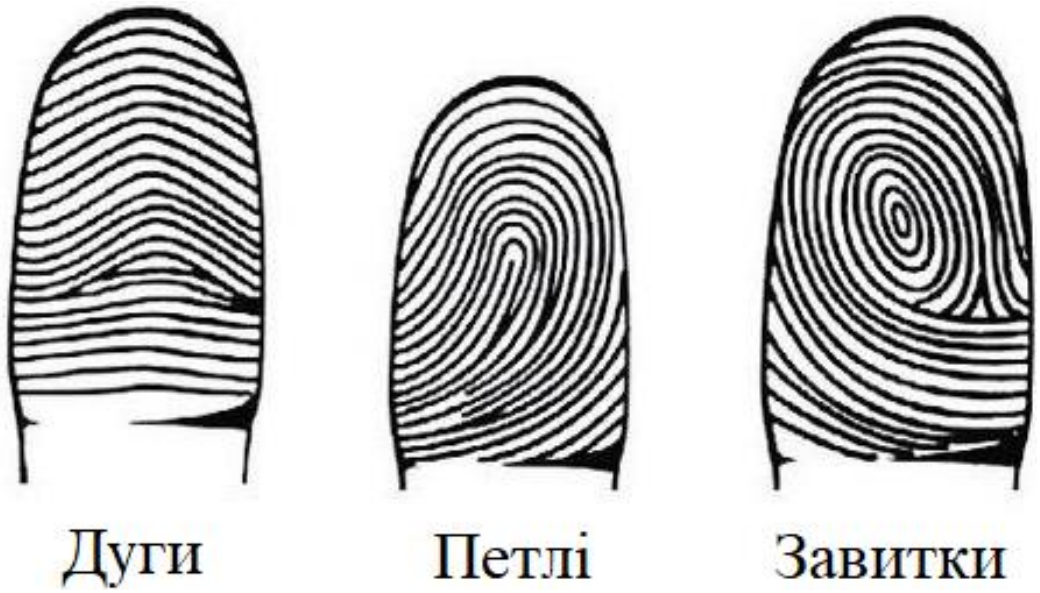


Рисунок 1.3 – Типи папілярних узорів

На сьогодні дактилоскопія виконує дві ключові функції: криміналістичну – ідентифікація осіб в слідчій справі; прикладну – використання принципів дактилоскопії у біометричних системах контролю доступу та автентифікації користувачів.

1.6.2 Різниця між дактилоскопією та біометричним методом відбитків пальців

Обидва методи базуються на аналізі унікальних малюнків папілярних ліній, проте між ними суттєві розбіжності, такі як:

1) Походження та сфери застосування

– Дактилоскопія виникла в межах криміналістики та орієнтована на ідентифікацію особи у правоохоронній сфері;

– Біометричне сканування є результатом розвитку інформаційних технологій та використовується у сферах безпеки.

2) Технологія отримання відбитка

– У дактилоскопії традиційним є використання чорнильний або порошкових методів зняття відбитків, відбитки знімаються та порівнюються експертами криміналістами;

– У біометричних системах використовуються спеціальні сенсори: оптичні, ємнісні та ультразвукові.

3) Методи аналізу відбитків

– Порівняння структурний аналіз ліній та мінуцій в дактилоскопії проводять експерти;

– На той час як в біометричних системах аналіз повністю автоматичний, відбиток перетворюється на цифровий шаблон, після чого порівнюється з раніше збереженим шаблоном в базі даних.

Проаналізувавши, можна зробити висновки, що дактилоскопія є науково-криміналістичним методом ідентифікації, а біометричне сканування – її технологічним продовженням у сфері безпеки.

1.7 Порівняння біометричних методів контролю доступу

Проведемо порівняльний аналіз біометричних методів за низкою критеріїв.

До основних критеріїв, за якими буде здійснене порівняння відносяться:

1. Рівень унікальності – ступінь індивідуальності біометричної ознаки, що визначає ймовірність збігу характеристик у різних осіб;
2. Точність та надійність – здатність системи забезпечувати правильну ідентифікацію користувача з мінімальними помилками (FAR – хибне прийняття, FRR – хибне відхилення);
3. Зручність використання – швидкість та комфортність процедури автентифікації;
4. Вартість впровадження – фінансові витрати на обладнання, програмне забезпечення та технічне обслуговування;
5. Стійкість до підробки – здатність системи протистояти атакам шляхом імітації чи підробки біометричних ознак.

На основі зазначених критеріїв проведено узагальнене порівняння найбільш поширених біометричних методів, наведене у таблиці 1.1.

Таблиця 1.1 – Порівняння біометричних методів

Біометричний метод	**Рівень унікальності**	**Точність та надійність**	**Зручність використання**	**Вартість впровадження**	**Стійкість до підробки**
За відбитком пальців	Високий	Висока	Висока	Низька	Середня
За формою долоні	Середній	Середня	Висока	Середня	Середня
За венозною сіткою	Дуже високий	Дуже висока	Висока	Висока	Дуже висока
За сітківкою ока	Дуже високий	Дуже висока	Низька	Висока	Дуже висока
За райдужною оболонкою ока	Дуже високий	Дуже висока	Середня	Висока	Дуже висока
За формою обличчя	Середній	Середня–висока	Дуже висока	Середня	Середня
За голосом	Середній	Середня	Висока	Низька	Низька
За рукописним почерком	Середній	Середня	Середня	Низька	Низька-середня
За клавіатурним почерком	Середній	Середня	Висока	Дуже низька	Низька

Проведене порівняння показує, що найбільш точними та захищеними від підробки є методи, засновані на аналізі райдужної оболонки ока, сітківки ока та венозної сітки. Вони забезпечують майже стовідсоткову ідентифікацію, проте їхня висока вартість і складність у використанні обмежують масове впровадження.

Методи відбитків пальців та геометрії долоні, мають найкраще співвідношення між вартістю, швидкістю роботи та точністю, завдяки чому широко застосовуються у системах контролю.

Технології розпізнавання обличчя та голосу характеризуються високою зручністю та безконтактністю, але меншою стійкістю до атак, тому найбільш ефективні при використанні у багатофакторних схемах автентифікації.

Враховуючи проведене порівняння об’єктом дослідження у даному проєкті обрано біометричний метод ідентифікації за відбитками пальців, оскільки він є найкращим варіантом, який поєднує в собі такі критерії, як: вартість, швидкість роботи, точність та зручність для користувачів.

1.8 Висновок по розділу 1

У першому розділі магістерської роботи проведено теоретичний аналіз систем контролю та управління доступом. Розглянуто класифікацію СКУД, визначено типи таких систем та області їх застосування. Описано принцип роботи систем керування доступом та технічні засоби, які необхідні для їх побудови. Особливу увагу приділено питанню переваг та недоліків таких систем надання доступу.

Особливий акцент зроблено на біометричних технологіях, які зараз є одним із ключових напрямів розвитку систем контролю доступу. Наведена коротка історія становлення біометрії, подано визначення ключових понять. Розглянуто статичні та динамічні методи біометричної ідентифікації людини, проведено аналіз ринку України на застосування різних біометричних методів. За результатами дослідження встановлено, що найбільш поширеним методом є ідентифікація за відбитком пальця.

Проведено порівняльний аналіз біометричних методів за основними критеріями. Враховуючи результати порівняння, як об’єкт дослідження в даній роботі обрано біометричний метод ідентифікації за відбитками пальців, оскільки він є найкращим з точки зору вартості, швидкодії, точності та зручності використання.

Додатково розглянуто структуру та принцип роботи біометричних систем, описано функції основних модулів, а також загальні етапи реалізації біометричних технологій ідентифікації особи. Проведено аналіз вимог до систем контролю

доступу та виявлено основні загрози, що можуть впливати на їх безпечне функціонування.

Окрему увагу зосереджено на технології ідентифікації за відбитками пальців: проаналізовано її історичний розвиток, здійснено порівняння дактилоскопії та сучасних біометричних методів, охарактеризовано основні типи папілярних узорів і їх властивості.

Підсумком проведеної роботи в даному розділі магістерської роботи є сформована база для подальшої розробки біометричної системи контролю доступу. Проведений аналіз дав змогу:

– визначити ключові вимоги для побудови ефективних і безпечних СКУД;

– аргументувати вибір біометричної технології на основі відбитків пальців як основного методу автентифікації для подальшої розробки;

– створити основу для розробки практичної частини системи, опис якої буде проводитись в наступних розділах магістерської роботи.

2. МЕТОДИ ДОСЛІДЖЕННЯ У СФЕРІ БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ

2.1 Методи надання доступу в біометричних СКД за відбитком пальця

В біометричних СКД широкого застосування набули різні методи автентифікації. Найбільш поширеними у використанні є однофакторна автентифікація, двофакторна автентифікація та режим привілейованого доступу. Розглянемо всі ці методи.

Однофакторна автентифікація передбачає надання доступу виключно на основі біометричного параметра користувача – відбитка пальця. У цьому випадку користувачеві достатньо прикласти палець до сканера, після чого система проводить зіставлення отриманого зображення з шаблонами, що зберігаються у базі даних. Основними перевагами цього методу є простота використання, швидкість та зручність. Недоліками є відсутність додаткового рівня захисту у разі компрометації біометричних даних, а також можливі проблеми із розпізнаванням при механічних ушкодженнях шкіри чи забрудненні сенсора.

Двофакторна автентифікація поєднує біометричний параметр із додатковим фактором – брелком, ПІН-кодом або карткою доступу. Такий метод значно підвищує рівень захищеності системи, адже для несанкціонованого доступу зловмиснику необхідно одночасно підробити як відбиток пальця, так і другий фактор для автентифікації. Двофакторна автентифікація застосовується на об’єктах із підвищеними вимогами безпеки, однак потребує більшого часу для здійснення процедури доступу та ускладнює взаємодію користувача з системою.

Режим привілейованого доступу дозволяє встановлювати різні рівні прав для окремих категорій користувачів. У даному випадку відбиток пальця використовується не лише для підтвердження особи, але й для визначення її ролі у системі. Це забезпечує можливість надання доступу до певних зон або ресурсів залежно від посадових обов’язків чи статусу особи (наприклад, студенти мають доступ лише до навчальних аудиторій, викладачі – до кабінетів та лабораторій, а

адміністративний персонал – до серверних приміщень чи архівів). Основною перевагою цього режиму є гнучке управління правами доступу, проте його реалізація вимагає ретельного адміністрування та контролю за правильністю налаштування рівнів доступу.

Таким чином, застосування різних методів автентифікації у біометричних системах контролю доступу дозволяє досягти балансу між зручністю, швидкістю і надійністю захисту. Вибір конкретного методу залежить від рівня безпеки об’єкта та вимог до організації процесу ідентифікації.

В зв’язку з фінансовими можливостями та браком часу було вирішено розглядати лише однофакторну автентифікацію за біометрією пальця. Це дозволить використовувати цю роботу як літературу і для однофакторної автентифікації і як один з компонентів системи інших методик доступу.

2.2 Методи зняття відбитків пальців та їх аналіз

На сьогоднішній день сканери відбитків пальців є найбільш популярним методом біометричної автентифікації в різних сферах застосування. Загальна технологія розпізнавання відбитків базується на принципі порівняння унікальних характеристик відбитка пальця людини з раніше створеним та збереженим шаблоном. Незважаючи на те що принцип роботи даних систем є одним для всіх, методи зняття відбитка можуть відрізнятись. Існує три основних методи сканування відбитків на принципі яких створені сканери, це такі методи як: ємнісний, оптичний та ультразвуковий. Кожен з цих методів має свої особливості, переваги та недоліки, що впливають на їхню ефективність роботи та зручність у використанні.

Проведемо більш детальний аналіз вищевказаних методів:

1. Ємнісний метод

Ємнісний метод використовує властивість людської шкіри проводити електричний струм. Коли палець торкається до сканера, кожен піксель визначає зміни в електричному полі, які викликані структурою відбитка пальця. Параметри

цих змін записуються і використовуються для створення цифрового представлення відбитка. Принцип роботи ємнісного сканера показано на рисунку 2.1 [16].

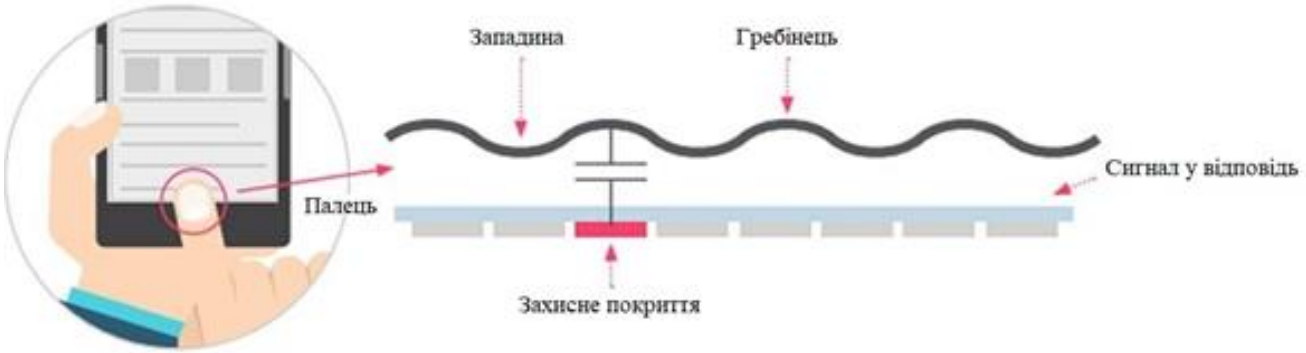


Рисунок 2.1 – Принцип роботи ємнісного типу сканерів

Якість зображення відбитка, що отримують за допомогою ємнісних сканерів досить посередня. Даний метод дуже чутливий до різних електростатичних розрядів та інших електричних полів, що значно знижує ефективність цього методу, однак незважаючи на це він є одним з самих поширених методів для отримання відбитків пальців. Такий тип сканерів порівняно легко можна «обдурити» імітованим муляжем відбитка пальця або прихованим відбитком який залишився на поверхні сканера.

Ємнісні сканери мають середню ціну серед інших, але під час експлуатації вони не довговічні, ці сканери надзвичайно чутливі до залишкової статичної електрики. На практиці дуже часто вони виходять з ладу після того, як до них торкнулася людина, руки якої були наелектризовані внаслідок тертя об одяг із вовняної або шовкової тканини.

2. Оптичний метод

Оптичний метод використовує світлочутливу матрицю а також джерело світла для зняття відбитка пальця. Під час того, як палець притискається до датчика під ним активується джерело світла, яке підсвічує палець та формує зображення відбитку. Світло яке відбилося фіксується світлочутливою матрицею, що забезпечує отримання цифрового зображення відбитка пальця. Принцип роботи оптичного сканера показано на рисунку 2.2 [15].

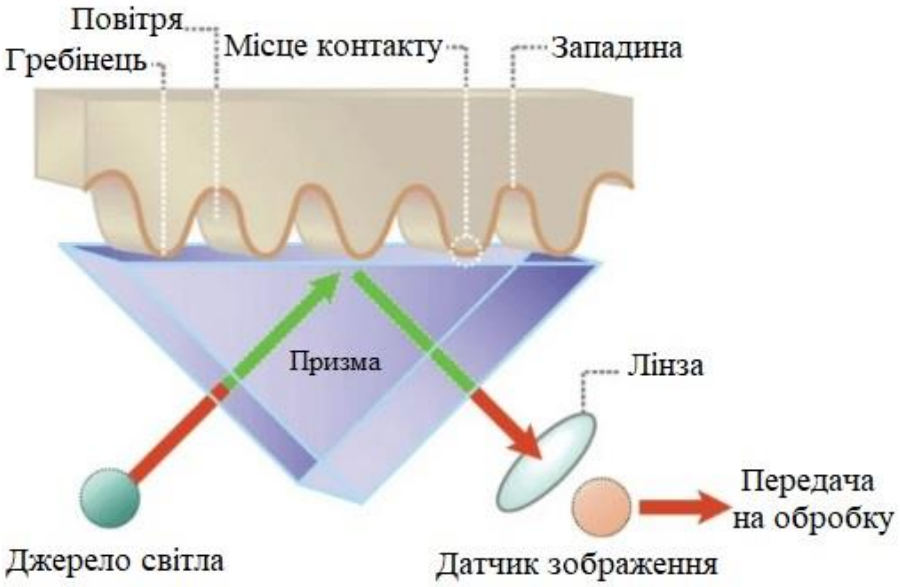


Рисунок 2.2 – Принцип роботи оптичного типу сканерів

Одним із недоліків даної технології є непомітний відбиток пальця, який залишається на сканері та може бути використаний злочинцем для «обману» системи. Ще одним суттєвим недоліком цього методу є те що він не завжди може відрізнити справжність пальця від гарного муляжу.

Але використання останніх технічних досягнень разом з цією технологією призвели до того, що нині одну з найдосконаліших технологій ідентифікації за відбитками пальців забезпечують саме оптичні сканери. Вони дещо дорожчі за ємнісні сканери, але позбавлені багатьох їх вад, є довговічними, а тому й економічними, відрізняються зручністю та доволі прості у використанні. Зображення відбитків, які отримуються на основі цього методу, є досить високої якості.

3. Ультразвуковий метод

Ультразвуковий метод працює за принципом, схожим на апарат ультразвукової діагностики. За допомогою електричного струму він генерує непомітні звукові хвилі, які проходять через сканер. Коли ці хвилі зустрічають відбиток пальця, вони відбиваються від його заглиблень і виступів по різному, повертаються до сканера і перетворюються на цифровий сигнал. Принцип роботи ультразвукового сканера показано на рисунку 2.3 [15].

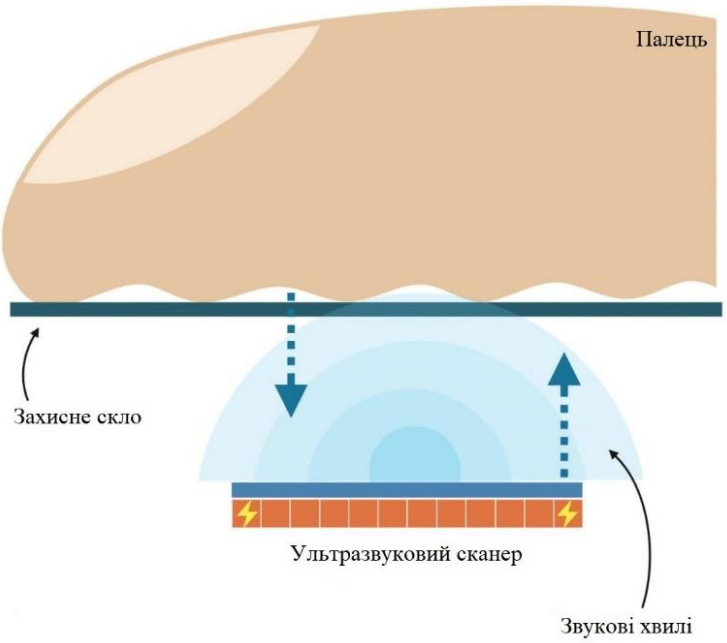


Рисунок 2.3 – Принцип роботи ультразвукового типу сканерів

Даний тип сканерів забезпечують високу точність, оскільки аналізують не лише поверхню а й глибину шкірного покриву. Вони працюють з вологими та брудними руками, що є значною перевагою в порівнянні з оптичним сканером. Цей тип сканерів складніше обійти, оскільки вони використовують складніші методи зчитування відбитка. Недоліками таких сканерів є їхня ціна та низька швидкість сканування.

Порівняння ключових критеріїв наведених вище методів показано в таблиці 2.1

Таблиця 2.1 – Порівняння методів сканування відбитків

Критерії	**Ємнісний**	**Оптичний**	**Ультразвуковий**
Якість зображення	Середня	Висока	Дуже висока
Вартість	Низька-середня	Середня-висока	Висока
Швидкість сканування	Висока	Висока	Середня-низька
Стійкість сканування до забруднень та вологи	Низька	Середня	Висока
Вразливість до підробок	Висока	Середня	Низька

Продовження таблиці 2.1

Чутливість до надлишкової енергії	Висока	Низька	Низька
Довговічність	Низька	Висока	Висока
Переваги	Дешеві; прості у використанні	Є балансом між якістю, надійністю та ціною	Підвищена стійкість, гарний варіант для об’єктів з високими вимогами захисту
Недоліки	Чутливі до надлишкової енергії; легко обманюються; не довговічні	Піддаються спуфінгу; часто відбитки залишаються на поверхні сканера	Дорогі; повільні сканування; важкі в інтегруванні в прототипи
Сфери застосування	Бюджетні СКД; смартфони бюджетного сегменту	Офісні та приватні СКД	Об’єкти з високими вимогами безпеки: банківські установи, преміальні СКД

Провівши аналіз методів зняття відбитків пальців для побудови системи контролю доступу було обрано сканер який буде працювати на основі оптичного методу. Сканери які базуються на основі оптичного методу мають такі переваги:

– висока якість отриманого зображення – світлочутлива матриця забезпечує детальне відтворення особливостей відбитка пальця, що підвищує точність ідентифікації;

– довговічність та надійність роботи – у конструкції відсутні рухомі частини, а скляна або кварцова поверхня стійка до зношування;

– зручність використання – сканери не потребують спеціальних умов для роботи та є простими в експлуатації;

– широка поширеність та підтримка – велика кількість готових рішень і програмних бібліотек спрощує інтеграцію в систему контролю доступу;

– найкраще співвідношення ціни та якості – при порівнянні з ультразвуковими сенсорами вони мають нижчу вартість, зберігаючи при цьому достатньо високу точність і надійність.

2.3 Ознаки відбитків пальців та принципи порівняння за ознаками

Незважаючи на всю різноманітність папілярних узорів, вони піддаються чіткій класифікації, яка забезпечує процес їх індивідуалізації та ідентифікації. У кожному відбитку можна визначити два типи ознак: локальні та глобальні. Глобальні ознаки – це ті, які можна побачити неозброєним оком. Наведемо типи глобальних ознак: 1) ліва петля; 2) права петля; 3) центральна петля; 4) подвійна петля; 5) дельта; 6) дуга; 7) спіраль; 8) змішана ознака. Всі ці ознаки показано на рисунку 2.4 [17].

Рисунок 2.4 – Типи глобальних ознак

Інший тип ознак – локальні. Це локальні особливості папілярних ліній унікальні для кожного відбитка пальця. Їх виокремлення пов’язано з тим, що лінії відбитків пальців не є прямими. Вони часто зламані, розгалужені, змінюють напрям і мають розриви. Точки, в яких лінії закінчуються, розгалужуються або змінюють

напрямок, називаються точками мінуціями. Ці точки забезпечують унікальну інформацію про відбиток пальця при ідентифікації особистості. Кожен відбиток пальця містить до 70 мінуцій. Локальні ознаки такі як: розриви, розгалуження та закінчення можемо спостерігати на рисунку 2.5.

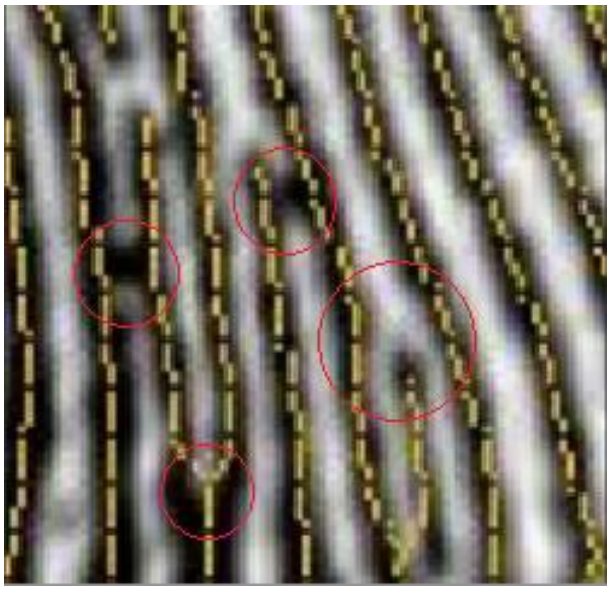


Рисунок 2.5 – Приклади локальних ознак

На практиці бувають випадки, що відбитки пальців різних людей можуть мати однакові глобальні ознаки, але неможлива наявність однакових мікро візерунків мінуцій. Саме тому глобальні ознаки використовують для розділення бази даних на класи та на етапі автентифікації. На етапі розпізнавання використовують вже локальні ознаки.

Розглянемо наступні принципи порівняння відбитків за локальними ознаками:

1) Користувач торкається сенсора, який зчитує зображення відбитка пальця;

2) Поліпшення якості початкового зображення відбитка пальця. На даному етапі збільшується різкість кордонів папілярних ліній, прибираються шуми, покращується контраст зображення;

3) Обчислення поля орієнтації папілярних ліній відбитка. Зображення розбивається на блоки, зі стороною більше 4 пікселів і по градієнтам яскравості визначається напрямок папілярних ліній. Показано на рисунку 2.6;

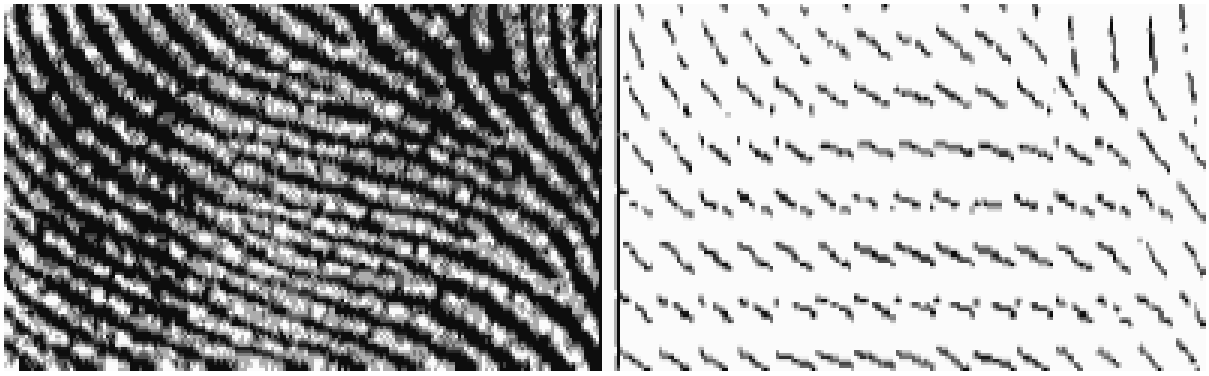


Рисунок 2.6 – Обчислення поля орієнтації папілярних ліній

4) Зображення приводиться до чорно-білого вигляду;

5) Стоншення ліній зображення відбитка. Проводиться до ширини лінії в 1 піксель. Показано на рисунку 2.7;

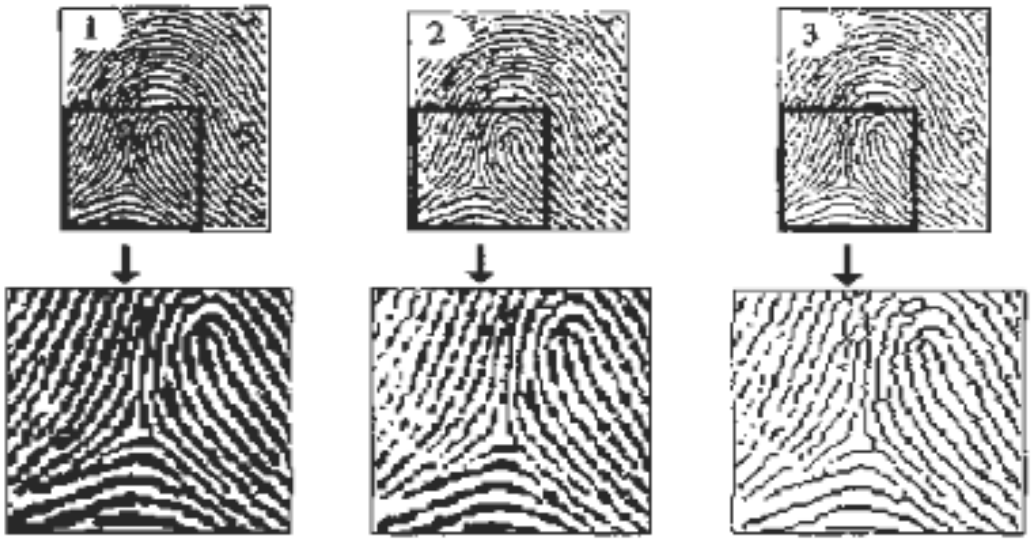


Рисунок 2.7 – Процес стоншення ліній відбитка

6) Виділення мінуцій. Зображення відбитка розбивається на блоки 9×9 пікселів. Після цього підраховується число чорних (ненульових) пікселів, що знаходяться навколо центру. Піксель в центрі вважається мінуцією, якщо він сам ненульовий, і сусідніх ненульових пікселів один (мінуція "закінчення") або два (мінуція "роздвоєння"). Показано на рисунку 2.8;

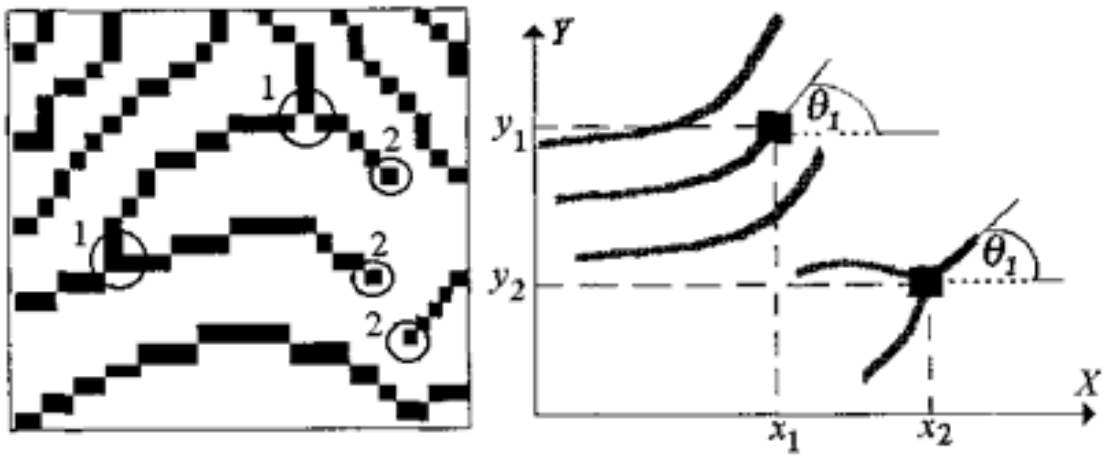


Рисунок 2.8 – Етап виділення мінуцій

Координати виявлених мінуцій та їх кути орієнтації записуються у вектор:

$$W(p) = [(x1, y1, t1), (x2, y2, t2)...(xp, yp, tp)], \quad (2.1)$$

де p – число мінуцій

При реєстрації користувачів цей вектор вважається еталоном і записується в базу даних. При розпізнаванні вектор визначає поточний відбиток.

7) Зіставлення мінуцій. Два відбитка одного пальця будуть відрізнятися один від одного поворотом, зсувом, зміною масштабу та площею дотику в залежності від того, як користувач прикладає палець до сканера. Тому не можна сказати, чи належить відбиток людині чи ні на підставі простого їхнього порівняння (вектори еталона і поточного відбитка можуть відрізнятися по довжині, містити невідповідні мінуції і так далі). Через це процес зіставлення повинен бути реалізований для кожної мінуції окремо.

Етапи порівняння мінуцій:

– реєстрація даних;

– пошук пар відповідних мінуцій;

– оцінка відповідності відбитків;

– при реєстрації визначаються параметри афінних перетворень (кут повороту, масштаб і зрушення), за яких деяка мінуція з одного вектора є певною мінуції з другого.

Оцінка відповідності відбитків виконується за такою формулою:

$$K = \frac{(D*D*100\%)}{(p*q)}, \qquad (2.2)$$

де D – кількість збіглися мінуцій;

p – кількість мінуцій еталона;

q – кількість мінуцій ідентифікованої відбитка.

У випадку, якщо результат перевищує 65%, відбитки вважаються ідентичними.

Якщо виконувалася автентифікація, то на цьому все і закінчується. Для ідентифікації необхідно повторити цей процес для всіх відбитків в базі даних.

Розглянемо метод на основі глобальних ознак. При цьому виконується виявлення глобальних ознак відбитка. Кількість цих ознак і їх взаємне розташування дозволяє класифікувати тип візерунка. Остаточне розпізнавання виконується на основі локальних ознак. Вважається, що тип візерунка може визначати характер, темперамент і здібності людини, тому цей метод можна використовувати і в цілях, відмінних від ідентифікації / автентифікації.

Розглянемо метод порівняння відбитків на основі графів. Показано на рисунку 2.9.

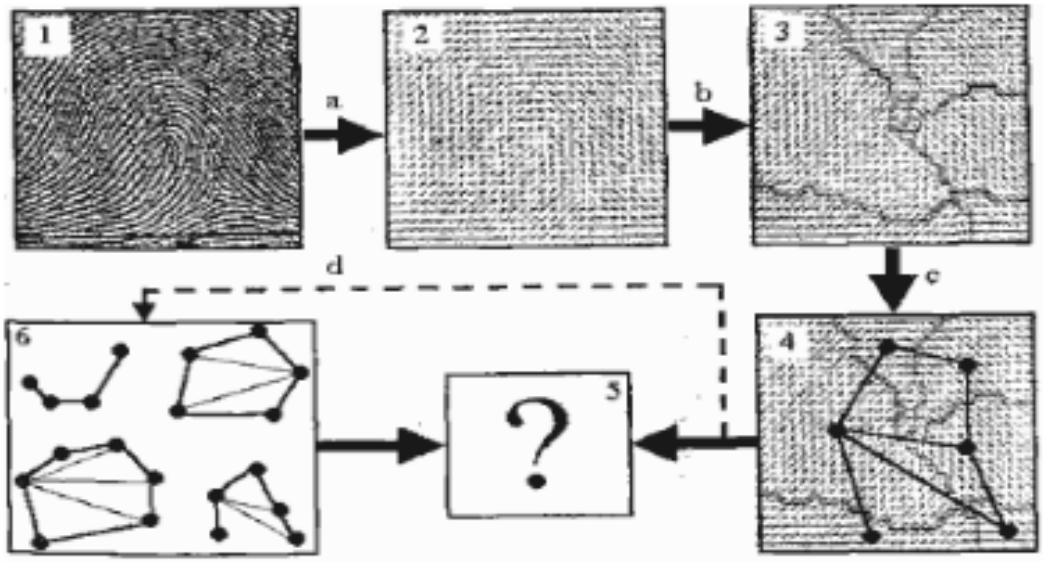


Рисунок 2.9 – Метод на основі графів

Початкове зображення відбитка (1) перетворюється на зображення поля орієнтації папілярних ліній (2). На ньому (2) помітні області з однаковою орієнтацією ліній, тому можна провести межі між цими областями (3). Потім визначаються центри цих областей і виходить граф (4). Стрілкою "d" відзначений запис в базу даних при реєстрації користувача. Визначення подібності відбитків реалізовано в квадраті 5. Подальші дії аналогічні попереднього методу - порівняння по локальних ознаками.

2.4 Аналіз власного відбитка пальця

Щоб проаналізувати свій власний відбиток пальця перш за все потрібно його зняти. Найпростішим способом це зробити в домашніх умовах є використання порошкового методу, який використовують в криміналістиці. Перш за все товстим шаром нанесемо олівцем на папір смужку шириною 2 × 2 сантиметри, далі до нанесеної смужку міцно притискаємо палець і цей палець притискаємо до смужки скоча. На скотчі залишиться відбиток пальця, для кращого сприйняття даний шматок скотчу приклеїмо на білий папір. Результат виконаних дій спостерігаємо на рисунку 2.10.

Рисунок 2.10 – Отриманий відбиток пальця

Виконаємо покращення отриманого зображення за допомогою фото редактора. Результат показано на рисунку 2.11.

Рисунок 2.11 – Покращене зображення відбитку

Після отримання відбитку пальця перейдемо до аналізу глобальних та локальних ознак.

Глобальні ознаки: неозброєним оком спостерігаємо що відбиток пальця є досить симетричним, з наявною звичайною петлею в його центрі (рис. 2.12) та з змішаною ознакою в центрі звичайної петлі (рис. 2.13).

Рисунок 2.12 – Звичайна петля

Рисунок 2.13 – Змішана ознака

Локальні ознаки: їх виокремлення пов’язано з тим, що лінії відбитків пальців не є прямими. Вони часто зламані, розгалужені, змінюють напрям і мають розриви, локальні ознаки спостерігаємо на рисунку 2.14.

Рисунок 2.14 – Точки мінуції

2.5 Порівняння оптичних сканерів відбитків пальця

Сьогодні на ринку представлено широке різноманіття моделей оптичних сканерів відбитків пальців. Для практичної реалізації біометричної системи контролю доступу на основі відбитків пальців для порівняння було обрано три моделі сканерів: R307 [18], AS608 [19] та FPM10A [20], серед яких в подальшому буде зроблено вибір. Порівняння оптичних сканерів показано в таблиці 2.2.

Таблиця 2.2 – Порівняння опричних сканерів відбитків пальців

	Моделі оптичних сканерів		
Параметри	R307	AS608	FPM10A
Тип сенсора	Оптичний	Оптичний	Оптичний
Інтерфейс	UART (TTL), USB	UART (TTL), USB	UART (TTL)
Об’єм відбитків	∽1000 відбитків	∽300 відбитків	∽300 відбитків
Роздільна здатність	500dpi	500dpi	500dpi
Швидкість розпізнавання	<1 секунда	<1 секунда	∽1 секунда
Швидкість реєстрації	1-2 секунди	1-2 секунди	2-3 секунди
FAR (False Acceptance Rate)	∽0,001%	∽0,001%	∽0,001%
FRR (False Rejection Rate)	∽1%	∽1-2%	∽2%
Рівень надійність	Високий	Середній	Середній
Вартість	Середня	Низька	Низька-середня
Ресурс сенсора	>1 млн дотиків	∽500 тис. дотиків	∽500 тис. дотиків
Метод збереження даних	Внутрішня пам’ять	Внутрішня пам’ять	Внутрішня пам’ять

Для проведення якісного порівняння оптичних сканерів, та вибору найкращого з них було застосовано метод аналізу ієрархії.

Метод аналізу ієрархії (MAI) – математичний інструмент системного підходу до складних проблем прийняття рішень. MAI не наказує особі, що приймає рішення, якого-небудь «правильного» рішення, а дозволяє їй в інтерактивному режимі знайти такий варіант, який найкращим чином узгоджується з його розумінням суті проблеми і вимогами до її вирішення.

Метод аналізу ієрархій корисний, оскільки він дозволяє формалізувати складні рішення, структурувавши проблему як багаторівневу ієрархію. Це допомагає зрозуміти зв'язки між елементами, визначити пріоритети, синтезувати правила

прийняття рішень та порівнювати альтернативи на основі експертних оцінок, що робить його універсальним для багатьох сфер.

Метод аналізу ієрархій використовується у всьому світі для прийняття рішень в різноманітних ситуаціях: від управління на міждержавному рівні до вирішення галузевих і приватних проблем в бізнесі, промисловості, охороні здоров'я та освіті [21].

Основні переваги:

– Структурування проблеми: Метод дозволяє розбити складну проблему на менші, керовані частини, розташовуючи їх у багаторівневій ієрархії;

– Формалізація рішень: Він допомагає формалізувати зв'язки між елементами та визначити пріоритети, які часто є суб'єктивними, використовуючи парні порівняння;

– Покращення розуміння: Процес побудови ієрархії допомагає учасникам краще зрозуміти проблему, контекст та точки зору інших людей;

– Синтез правил: Метод дозволяє синтезувати правило для прийняття рішення, яке базується на перевагах різних альтернатив.

Недолік:

– Залежність від експертів: Одним з недоліків є те, що для роботи методу потрібно отримати великий обсяг точної інформації від експертів.

Етапи методу аналізу ієрархій:

1. Побудова якісної моделі проблеми у вигляді ієрархії, що включає мету, альтернативні варіанти досягнення цілі та критерії для оцінки якості альтернатив;
2. Визначення пріоритетів всіх елементів ієрархії з використанням методу експертного оцінювання на основі парних порівнянь;
3. Перевірка суджень експерта на узгодженість;
4. Синтез глобальних пріоритетів альтернатив шляхом лінійної згортки пріоритетів елементів на ієрархії;
5. Прийняття рішення на основі отриманих результатів.

Порівняння сканерів було вирішено провести по критеріях, які відповідають поставленій меті даного проєкту – створити бюджетну та функціональну систему, а саме:

– FAR – рівень помилкового прийняття;

– FRR – рівень помилкової відмови;

– Ціна – наскільки дорогий сканер;

– Надійність – наскільки сканер надійний та його ресурс;

– Масштабованість – можливість сканера ефективно обробляти зростаючий обсяг роботи.

Для порівняння на кожному рівні ієрархії об’єктів в результаті оцінювання експертів будується матриця парних порівнянь. Окрім порівняння необхідно визначити добуток, вектор та вагу, за такими формулами:

$$\beta_j = \sqrt[n]{\prod_{j=1}^{n} a_{ij}}, \tag{2.3}$$

де **β**i – проміжне значення для і-го рядка;

$\prod_{j=1}^{n}$ – символ добутку;

a_{ij} – елементи порівнянь парних порівнянь, розташованих на перетині і-го рядка та j-го стовпця.

$$P_i = \frac{\beta_i}{\sum_{k=1}^{n} \beta_k}, \tag{2.4}$$

де P_i – вага і-го елемента;

$\sum_{k=1}^{n} \beta_k$-сума всіх проміжних значень β для всіх n елементів

Матриці парних порівнянь для кожного з критеріїв показані на рисунку 2.15 – 2.19. Також необхідно побудувати матрицю парних порівнянь критеріїв між собою, показано на рисунку 2.20.

FAR						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	1	1	1	1	0,3333
AS608	1	1	1	1	1	0,3333
FPM10A	1	1	1	1	1	0,3333
					3	1

Рисунок 2.15 – Матриці парних порівнянь критерія «FAR»

FRR						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	5	7	35	3,2711	0,7396
AS608	0,2	1	2	0,4	0,7368	0,1666
FPM10A	0,14285714	0,5	1	0,07143	0,4149	0,0938
					4,4228	1

Рисунок 2.16 – Матриці парних порівнянь критерія «FRR»

Ціна						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	0,2	0,33333	0,06667	0,4055	0,104729434
AS608	5	1	3	15	2,4662	0,636985572
FPM10A	3	0,3333	1	1	1	0,258284994
					3,8717	1

Рисунок 2.17 – Матриці парних порівнянь критерія «Ціна»

Надійність						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	5	5	25	2,924	0,7143
AS608	0,2	1	1	0,2	0,5848	0,1429
FPM10A	0,2	1	1	0,2	0,5848	0,1429
					4,0936	1

Рисунок 2.18 – Матриці парних порівнянь критерія «Надійність»

Масштабованість						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	5	7	35	3,2711	0,730644671
AS608	0,2	1	3	0,6	0,8434	0,188394097
FPM10A	0,1428571	0,3333	1	0,04762	0,3625	0,080961232
					4,477	1

Рисунок 2.19 – Матриці парних порівнянь критерія «Масштабованість»

	FAR	FFR	ЦІНА	НАДІЙНІСТЬ	МАСШТАБОВАНІСТЬ	Добуток	Вектор	Вага
FAR	1	1	3	5	7	105	2,5365	0,3638
FFR	1	1	3	5	7	105	2,5365	0,3638
ЦІНА	0,333333333	0,3333	1	3	5	1,666667	1,1076	0,1588
НАДІЙНІСТЬ	0,2	0,2	0,3333	1	3	0,04	0,5253	0,0753
МАСШТАБОВАНІСТЬ	0,142857143	0,1429	0,2	0,333333333	1	0,001361	0,2671	0,0383
							6,973	1

Рисунок 2.20 – Матриця парних порівнянь критеріїв

Наступним етапом потрібно перевірити узгодженість матриць та побудувати графіки для кожної матриці. Для цього кожній матриці потрібно вичислити n* – максимальне особисте число матриці за формулою:

$$n^* = \frac{\sum_j^n n_j}{n}, \tag{2.5}$$

де n – розмірність матриці

Індекс погодженості H:

$$H=\frac{n^{*}-n}{n-1}, \tag{2.6}$$

де n – розмірність матриці

n* – максимальне особисте число матриці

Стохастичний коефіцієнт погодженості RH:

$$RH=\frac{1.98*(n-2)}{n}, \tag{2.7}$$

де n – розмірність матриці

Коефіцієнт погодженості матриці HR:

$$HR=\frac{H}{RH}, \tag{2.8}$$

де H – розмірність матриці;

RH – стохастичний коефіцієнт погодженості

Результати проведених розрахунків показано на рисунках 2.21 – 2.26.

FAR						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	1	1	1	1	0,3333
AS608	1	1	1	1	1	0,3333
FPM10A	1	1	1	1	1	0,3333
					3	1

n	3
N*R307	3
N*AS608	3
N*FPM10A	3
n*	3
H	0
RH	0,66
HR	0

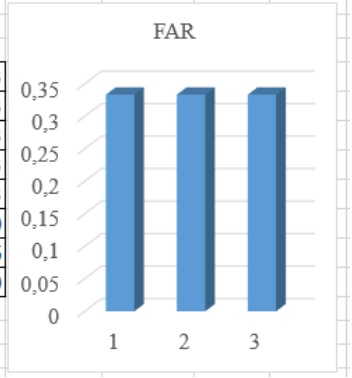


Рисунок 2.21 – Матриця порівняння альтернатив за критерієм «FAR»

FRR						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	5	7	35	3,2711	0,7396
AS608	0,2	1	2	0,4	0,7368	0,1666
FPM10A	0,14285714	0,5	1	0,07143	0,4149	0,0938
					4,4228	1

n	3
N*R307	3,0142
N*AS608	3,0142
N*FPM10A	3,0142
n*	3,0142
H	0,0071
RH	0,66
HR	0,0107

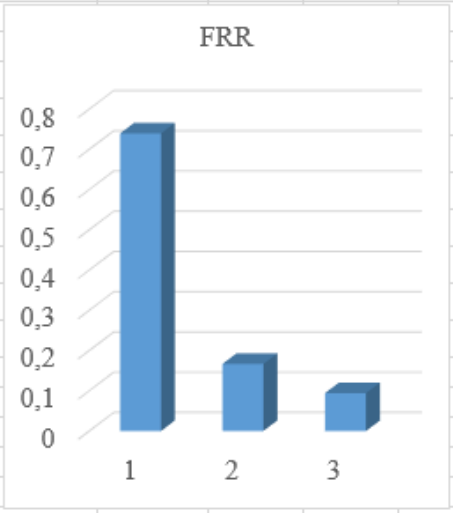


Рисунок 2.22 – Матриця порівняння альтернатив за критерієм «FRR»

Ціна						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	0,2	0,33333	0,06667	0,4055	0,104729434
AS608	5	1	3	15	2,4662	0,636985572
FPM10A	3	0,3333	1	1	1	0,258284994
					3,8717	1

n	3
N*R307	3,0385
N*AS608	3,0385
N*FPM10A	3,0385
n*	3,0385
H	0,0193
RH	0,66
HR	0,0292

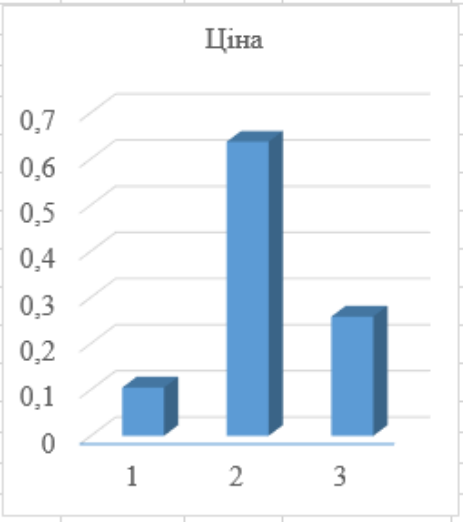


Рисунок 2.23 – Матриця порівняння альтернатив за критерієм «Ціна»

Надійність						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	5	5	25	2,924	0,7143
AS608	0,2	1	1	0,2	0,5848	0,1429
FPM10A	0,2	1	1	0,2	0,5848	0,1429
					4,0936	1

n	3
N*R307	3
N*AS608	3
N*FPM10A	3
n*	3
H	0
RH	0,66
HR	0

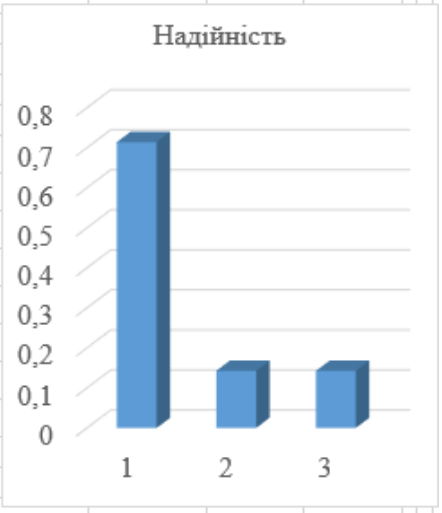


Рисунок 2.24 – Матриця порівняння альтернатив за критерієм «Надійність»

Масштабованість						
	R307	AS608	FPM10A	Добуток	Вектор	Вага
R307	1	5	7	35	3,2711	0,730644671
AS608	0,2	1	3	0,6	0,8434	0,188394097
FPM10A	0,1428571	0,3333	1	0,04762	0,3625	0,080961232
					4,477	1

n	3
N*R307	3,0649
N*AS608	3,0649
N*FPM10A	3,0649
n*	3,0649
H	0,0324
RH	0,66
HR	0,0492

Рисунок 2. 25 – Матриця порівняння альтернатив за критерієм «Масштабованість»

	FAR	FFR	ЦІНА	НАДІЙНІСТЬ	МАСШТАБОВАНІСТЬ	Добуток	Вектор	Вага
FAR	1	1	3	5	7	105	2,5365	0,3638
FFR	1	1	3	5	7	105	2,5365	0,3638
ЦІНА	0,333333333	0,3333	1	3	5	1,666667	1,1076	0,1588
НАДІЙНІСТЬ	0,2	0,2	0,3333	1	3	0,04	0,5253	0,0753
МАСШТАБОВАНІСТЬ	0,142857143	0,1429	0,2	0,333333333	1	0,001361	0,2671	0,0383
							6,973	1

n	5
N*FAR	5,0827
N*FFR	5,0827
N*ЦІНА	5,1556
N*НАДІЙНІСТЬ	5,1599
N*МАСШТАБОВАНІСТЬ	5,1975
n*	5,1357
H	0,0339
RH	1,188
HR	0,0286

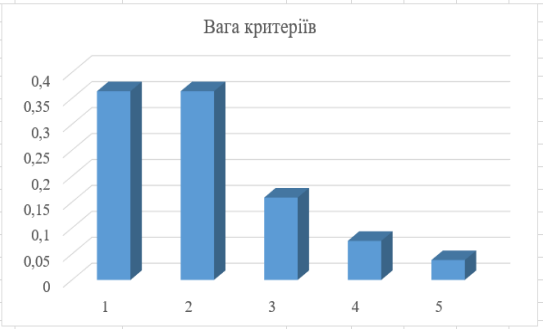


Рисунок 2.26 – Матриця парних порівнянь критеріїв

Далі перейдемо до оцінки та вибору найкращого кандидата з порівняних. Створюємо узагальнюючу матрицю з кожною моделлю сканера, кожним критерієм та вагою критеріїв. В таблицю вносимо дані ваг відносно кожної моделі сканера до кожного критерію, які були отримані раніше, показано на рисунку 2.27.

Узагальнююча оцінка кандидатів						
	FAR	FFR	ЦІНА	НАДІЙНІСТЬ	МАШТАБОВАНІСТЬ	Vi
R307	0,33333	0,7396	0,1047	0,714285714	0,730644671	0,48872
AS608	0,33333	0,1666	0,637	0,142857143	0,188394097	0,30101
FPM10A	0,33333	0,0938	0,2583	0,142857143	0,080961232	0,21027
Вага крит.	0,36376	0,3638	0,1588	0,075333696	0,038310676	1

Рисунок 2.27 – Узагальнюча оцінка кандидатів

Хоча ціна, один з найважливіших критеріїв, у сканера R307 більша за інші порівнювані моделі, його переваги щодо надійності, FAR та FRR роблять його найкращим варіантом для подальшої розробки.

2.6 Порівняння плат керування для СКД

Для реалізації прототипа макета біометричної СКД по відбитку пальця слід обрати плату керування, яка буде обробляти дані з сенсора відбитків пальців та керувати замком. Зараз на ринку велике різноманіття апаратних платформ, серед яких найбільшою популярністю користуються такі плати, як: Arduino UNO [22], ESP32 [23] та STM32 [24]. Проведемо порівняння даних плат керування по ключовим параметрам, та оберемо найбільш підходящу для проєкту. Порівняння плат керування показано в таблиці 2.3.

Таблиця 2.3 – Порівняння плат керування

	Моделі плат керування		
Параметри	Arduino UNO	ESP32	STM32
Мікроконтролер	ATmega328P	Xtensa LX6	ARM Cortex-M3
Тактова частота	16 МГц	240 МГц	72 МГц
RAM-пам’ять	2 КБ	520 КБ	20 КБ
Flash-пам’ять	32 КБ	4 МБ	від 64 КБ
Робоча напруга	5 В	5 В	3,3 В
Кількість портів	14 цифрових, 6 аналогових	∽ 34, залежить від моделі	∽ 37, залежить від моделі
Інтерфейси	UART, I2C, SPI	UART, I2C, SPI, CAN, Wi-Fi, Bluetooth	UART, I2C, SPI, CAN, USB
Вартість	Середня	Висока-середня	Середня

Порівняння плат керування було вирішено провести також за допомогою MAI по таких критеріях, як:

– Ціна – вартість плати;

– Підтримка та налаштування – наскільки легко налаштувати плату у випадку поломки;

– Пам'ять – об’єм пам’яті.

Для порівняння на кожному рівні ієрархії об’єктів в результаті оцінювання експертів будується матриця парних порівнянь. Матриці парних порівнянь для кожного з критеріїв показані на рисунку 2.28 – 2.30. Також необхідно побудувати матрицю парних порівнянь критеріїв між собою, показано на рисунку 2.31.

Ціна						
	UNO	ESP32	STM32	Добуток	Вектор	Вага
UNO	1	3	1	3	1,4422	0,4286
ESP32	0,3333	1	0,3333	0,11111	0,4807	0,1429
STM32	1	3	1	3	1,4422	0,4286
					3,3652	1

Рисунок 2.28 – Матриці парних порівнянь критерія «Ціна»

Підтримка та налаштування						
	UNO	ESP32	STM32	Добуток	Вектор	Вага
UNO	1	5	3	15	2,4662	0,637
ESP32	0,2	1	0,3333	0,06667	0,4055	0,1047
STM32	0,3333	3	1	1	1	0,2583
					3,8717	1

Рисунок 2.29 – Матриці парних порівнянь критерія «Підтримка»

Пам'ять						
	UNO	ESP32	STM32	Добуток	Вектор	Вага
UNO	1	0,2	0,3333	0,06667	0,4055	0,1047
ESP32	5	1	3	15	2,4662	0,637
STM32	3	0,3333	1	1	1	0,2583
					3,8717	1

Рисунок 2.30 – Матриці парних порівнянь критерія «Пам’ять»

ЦІНА - ПІДТРИМКА ТА НАЛАШТУВАННЯ - ПАМ'ЯТЬ						
	ЦІНА	ПІДТРИМКА	ПАМ'ЯТЬ	Добуток	Вектор	Вага
ЦІНА	1	5	7	35	3,2711	0,7306447
ПІДТРИМКА	0,2	1	3	0,6	0,8434	0,1883941
ПАМ'ЯТЬ	0,1429	0,333333333	1	0,04762	0,3625	0,0809612
					4,477	1

Рисунок 2.31 – Матриця парних порівнянь критеріїв

Наступним етапом потрібно перевірити узгодженість матриць та побудувати графіки для кожної матриці, показано на рисунках 2.32 – 2.35. Для цього кожній матриці потрібно вичислити n*, H, RH, HR формули яких наведені в пункті порівняння сканерів.

Ціна						
	UNO	ESP32	STM32	Добуток	Вектор	Вага
UNO	1	3	1	3	1,4422	0,4286
ESP32	0,3333	1	0,3333	0,11111	0,4807	0,1429
STM32	1	3	1	3	1,4422	0,4286
					3,3652	1

n	3
N*UNO	3
N*ESP32	3
N*STM32	3
n*	3
H	0
RH	0,66
HR	0

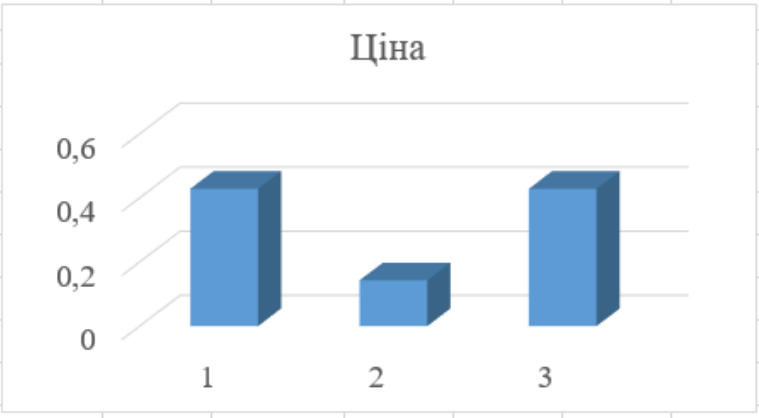


Рисунок 2.32 – Матриця порівняння альтернатив за критерієм «Ціна»

Підтримка та налаштування						
	UNO	ESP32	STM32	Добуток	Вектор	Вага
UNO	1	5	3	15	2,4662	0,637
ESP32	0,2	1	0,3333	0,06667	0,4055	0,1047
STM32	0,3333	3	1	1	1	0,2583
					3,8717	1

n	3
N*UNO	3,0385
N*ESP32	3,0385
N*STM32	3,0385
n*	3,0385
H	0,0193
RH	0,66
HR	0,0292

Рисунок 2.33 – Матриця порівняння альтернатив за критерієм «Підтримка»

Пам'ять						
	UNO	ESP32	STM32	Добуток	Вектор	Вага
UNO	1	0,2	0,3333	0,06667	0,4055	0,1047
ESP32	5	1	3	15	2,4662	0,637
STM32	3	0,3333	1	1	1	0,2583
					3,8717	1

n	3
N*UNO	3,0385
N*ESP32	3,0385
N*STM32	3,0385
n*	3,0385
H	0,0193
RH	0,66
HR	0,0292

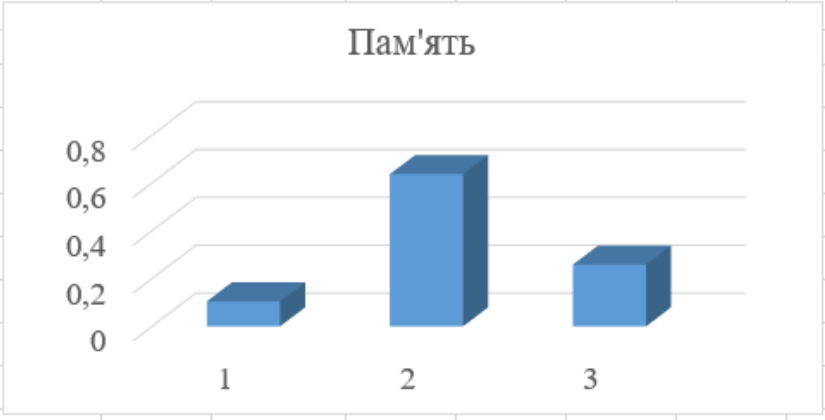


Рисунок 2.34 – Матриця порівняння альтернатив за критерієм «Пам’ять»

ЦІНА - ПІДТРИМКА ТА НАЛАШТУВАННЯ - ПАМ'ЯТЬ						
	ЦІНА	ПІДТРИМКА	ПАМ'ЯТЬ	Добуток	Вектор	Вага
ЦІНА	1	5	7	35	3,2711	0,7306447
ПІДТРИМКА	0,2	1	3	0,6	0,8434	0,1883941
ПАМ'ЯТЬ	0,1429	0,333333333	1	0,04762	0,3625	0,0809612
					4,477	1

n	3
N*ЦІНА	3,0649
N*ПІДТРИМКА	3,0649
N*ПАМ'ЯТЬ	3,0649
n*	3,0649
H	0,0324
RH	0,66
HR	0,0492

Рисунок 2.35 – Матриця парних порівнянь критеріїв

Далі перейдемо до оцінки та вибору найкращого кандидата з порівняних плат керування. Створюємо узагальнюючу матрицю з кожною моделлю плат керування, кожним критерієм та вагою критеріїв. В таблицю вносимо дані ваг відносно кожної моделі плати керування до кожного критерію, які були отримані раніше, показано на рисунку 2.36.

Узагальнююча оцінка кандидатів				
	ЦІНА	ПІДТРИМКА	ПАМ'ЯТЬ	Vi
UNO	0,4286	0,636985572	0,104729	0,44162
ESP32	0,1429	0,104729434	0,636986	0,17568
STM32	0,4286	0,258284994	0,258285	0,3827
Вага критеріїв	0,7306	0,188394097	0,080961	1

Рисунок 2.36 – Узагальнююча оцінка кандидатів

Згідно з розрахунками методу аналізу ієрархій плата Arduino UNO є найкращим кандидатом. Це зумовлено її бюджетною вартістю, стабільним рівнем підтримки та достатнім об’ємом пам’яті для реалізації поставлених завдань перед біометричною системою контролю доступу. В сукупності це забезпечує найкраще співвідношення вартості та функціональності, що робить плату Arduino UNO найбільш доцільним вибором серед проаналізованих плат.

2.7 Опис та технічні характеристики елементів системи

2.7.1 Оптичний сканер R307

Оптичний сканер моделі R307 призначений для зчитування та обробки відбитків пальців у системах контролю доступу та ідентифікації. Він обладнаний вбудованим процесором та флеш-пам’яттю, що дозволяє виконувати основні операції, такі як зчитування, формування шаблону, порівняння за схемою 1:1 та пошук за схемою 1:N без використання зовнішніх ресурсів. Завдяки простоті інтеграції, модуль широко застосовується у замках, сейфах, системах обліку та електронних макетах. Сканер R307 показано на рисунку 2.37 [18].

Рисунок 2.37 – Сканер R307

Основні технічні характеристики сканера R307:

- Робоча напруга живлення: 4,2 – 6,0 В;
- Споживаний струм: ≈50 мА (типовий), до 80 мА (піковий);
- Час отримання зображення: < 0,3 с;
- Розмір вікна сканування: 14 × 18 мм;
- Об’єм відбитків: до 1000 шаблонів відбитків пальців;
- Формат шаблону: 512 байт;
- Інтерфейс обміну: UART;
- Режими роботи: 1:1 (верифікація), 1:N (ідентифікація);
- Рівень помилкового допуску (FAR): < 0,001 %;
- Рівень помилкового відхилення (FRR): < 1 %;
- Час пошуку в базі (до 1000 шаблонів): < 1 с;
- Робочий діапазон температур: від –20 °C до +40 °C.

2.7.2 Плата керування Arduino UNO

Arduino UNO — це одна з найпопулярніших плат серед розробників та студентів, яка використовується для створення прототипів електронних пристроїв. Вона побудована на мікроконтролері ATmega328P та відзначається простотою використання завдяки відкритому середовищу програмування Arduino IDE та великій кількості готових бібліотек.

UNO підтримує роботу з широким спектром датчиків і модулів, що робить її універсальною платформою для навчальних і дослідницьких проєктів. Плату керування Arduino UNO показано на рисунку 2.38 [22].

Рисунок 2.38 – Плата керування Arduino UNO

Основні технічні характеристики Arduino UNO:

- Мікроконтролер: ATmega328P;
- Тактова частота: 16 МГц;
- Оперативна пам’ять (SRAM): 2 КБ;
- Постійна пам’ять (Flash): 32 КБ, з яких 0,5 КБ використовується завантажувачем;
- EEPROM: 1 КБ;
- Кількість цифрових входів/виходів: 14;
- Кількість аналогових входів: 6;
- Робоча напруга: 5 В;
- Живлення: через USB або від зовнішнього джерела 7–12 В;
- Струм на вивід GPIO: до 20 мА (40 мА макс.);
- Комунікаційні інтерфейси: UART, I2C, SPI;
- Розміри плати: 68,6 × 53,4 мм.

2.7.3 Опис портів Arduino UNO

Плата керування має 14 цифрових входів і виходів, які керують функціями pinMode(), digitalWrite() і digitalRead(). Рівень напруги на виходах обмежений 5В. Максимальний струм на цифрових виходах становить 40 мА.

Виходи можуть бути переконфігуровані в інші функції:

– Послідовний інтерфейс: виводи 0 (RX) та 1 (TX). Використовуються для отримання (RX) та передачі (TX) даних за послідовним інтерфейсом. Ці виводи з'єднані з відповідними виводами мікросхеми ATmega8U2, яка виконує роль USB-UART-перетворювача;

– Зовнішні переривання: виводи 2 і 3. Можуть бути джерелами переривань, що виникають при фронті, спаді або низькому рівні сигналу на цих виводах;

– ШІМ: виводи 3, 5, 6, 9, 10 та 11. За допомогою функції analogWrite() можуть виводити 8-бітові аналогові значення у вигляді ШІМ-сигналу;

– Інтерфейс SPI: виводи 10 (SS), 11 (MOSI), 12 (MISO), 13 (SCK);

– Світлодіод: 13. Вбудований світлодіод, приєднаний до виводу 13. При надсиланні значення HIGH світлодіод вмикається, при відправленні LOW - вимикається.

Arduino UNO має 6 аналогових входів (A0 - A5), кожен з яких може представити аналогову напругу у вигляді 10-бітного числа. За замовчуванням, вимірювання напруги здійснюється відносно діапазону від 0 до 5 В. Проте верхню межу цього діапазону можна змінити, використовуючи вивід AREF і функцію analogReference().

Крім цього, деякі з аналогових входів мають додаткові функції: TWI: вивід A4 або SDA та вивід A5 або SCL. З використанням бібліотеки Wire ці виводи можуть здійснювати зв'язок за інтерфейсом TWI [25].

Порти плати керування Arduino UNO показано на рисунку 2.39.

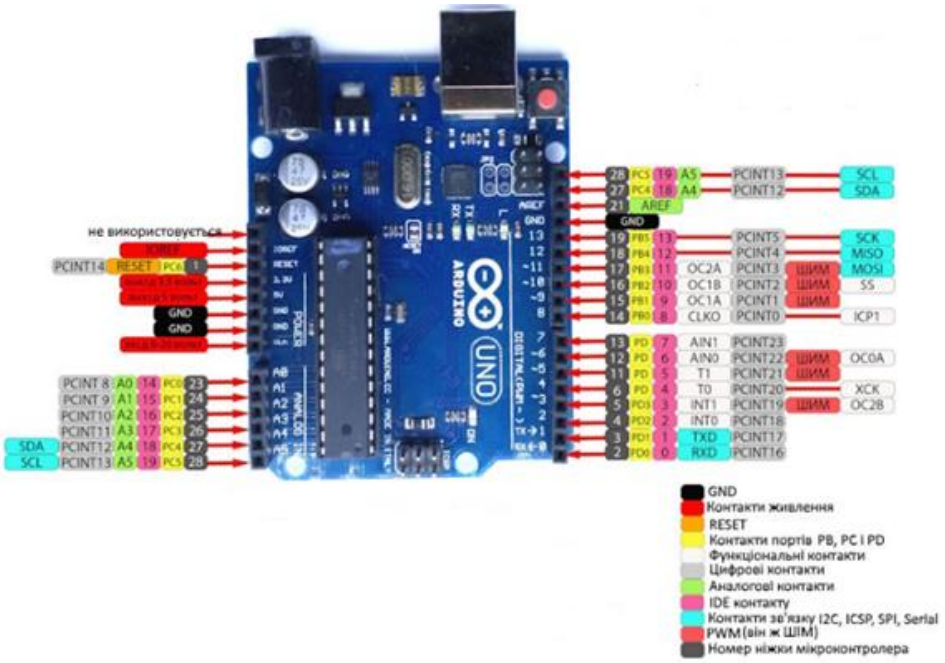


Рисунок 2.39 – Порти плати керування Arduino UNO

2.7.4 Транзистор

IRFZ44N — це n-канальний силовий MOSFET транзистор, призначений для роботи у низьковольтних високострумових схемах. Завдяки низькому опору відкритого каналу та високій швидкодії перемикання, він широко використовується у схемах живлення, інверторах, контролерах двигунів та у проєктах для керування потужним навантаженням, наприклад, електромагнітними замками. Транзистор показано на рисунку 2.40 [26].

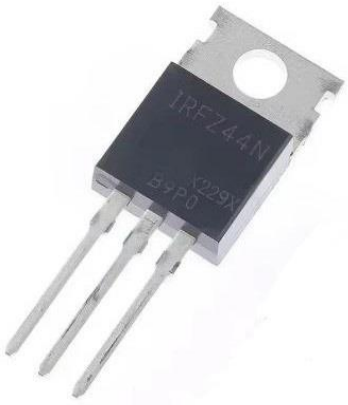


Рисунок 2.40 – Транзистор IRFZ44N

Основні технічні характеристики IRFZ44N:

- Тип транзистора: n-канальний MOSFET;
- Максимальна напруга: 55 В;
- Максимальний струм: 49 А;
- Потужність розсіювання: 94 Вт;
- Робоча температура: –55 °C … +175 °C;

2.7.5 Електромеханічний замок

Електромеханічний замок використовується для дистанційного керування доступом до об’єкта. Принцип роботи базується на електромагніті: при подачі живлення на котушку соленоїда висувається або втягується засувка, що забезпечує блокування чи розблокування дверей. Такий тип замків простий у використанні, має компактні розміри та добре підходить для інтеграції з системами контролю доступу. Показано на рисунку 2.41 [27].

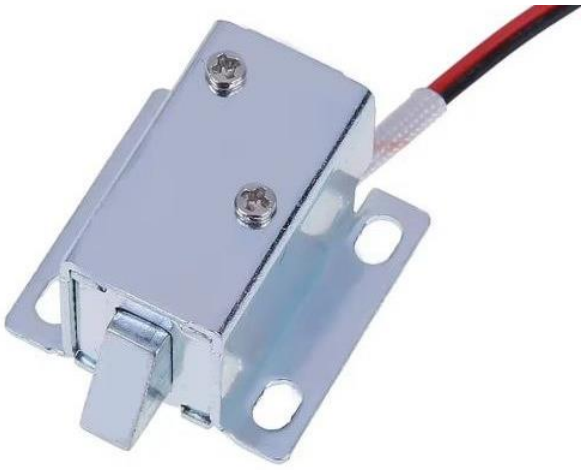


Рисунок 2.41 – Електромеханічний замок

Основні технічні характеристики:

- Робоча напруга: 12 В;
- Робочий струм: 0,5-1 А;
- Споживана потужність: ≈ 5-10 Вт;

- Режим роботи: короткочасний (при подачі напруги відбувається відпускання/замикання засувки);
- Матеріал корпусу: метал;
- Тип приводу: соленоїд з механічною пружиною.

2.7.6 Блок живлення

Імпульсний адаптер живлення 12 В призначений для перетворення змінної напруги електромережі 220 В у стабілізовану постійну напругу 12 В. Використовується для живлення низьковольтних електронних пристроїв: мікроконтролерів, модулів, електромагнітних замків, датчиків тощо. Завдяки компактним розмірам і стандартному роз'єму DC, адаптер зручний у застосуванні. Показано на рисунку 2.20 [42].

Рисунок 2.42 – Блок живлення 12 В

Основні технічні характеристики:

- Вхідна напруга: AC 100–240 В, 50/60 Гц;
- Вихідна напруга: DC 12 В;
- Вихідний струм: 2 А;
- Потужність: 12Вт;
- Тип конструкції: імпульсний блок живлення;

- ККД: ≈80–85 %;
- Роз’єм підключення: DC 5,5 × 2,1 мм;
- Захист: від короткого замикання, перевантаження та перегріву;
- Робоча температура: -10 °C … +50 °C.

2.8 Висновок по розділу 2

У другому розділі магістерської роботи основну увагу зосереджено на аналізі методів, що використовуються під час розробки біометричних СКД. Проведено детальний огляд і порівняння методів надання доступу в біометричних системах, на основі якого обрано найбільш підходящий метод для подальшої реалізації системи.

Розглянуто основні способи зняття відбитків пальців, проведено їх порівняльний аналіз та аргументовано вибір найкращого методу, який забезпечує високу точність, стабільність та зручність використання. Визначено основні переваги обраного підходу порівняно з альтернативними рішеннями.

Досліджено локальні та глобальні ознаки відбитків пальців, наведено їх класифікацію та приклади. Описано принципи порівняння відбитків за локальними і глобальними характеристиками, наведено етапи процесу ідентифікації та формулу оцінки ступеня відповідності відбитків. Виконано експериментальне зняття власного відбитка пальця, проведено його аналіз і виявлено характерні локальні та глобальні ознаки, що підтверджують працездатність обраного методу.

Також здійснено порівняння за допомогою МАІ найпоширеніших на ринку оптичних сканерів відбитків пальців і плат керування за ключовими критеріями. За результатами МАІ обрано найкращу модель сканера та контролера, які використовуватимуться як основні апаратні компоненти системи. Також обрано джерело живлення системи, виконавчий та стабілізуючий компонент живлення. Для кожного з них наведено детальний опис, технічні характеристики та аргументовано доцільність їх застосування в системі яка буде розроблена.

Підсумовуючи проведену роботу в даному розділі було: проведено аналіз методів зняття та обробки відбитків пальців; досліджено особливості локальних та глобальних ознак відбитків; для подальшої розробки обрано оптичний метод зняття відбитків, це зумовлено високою якістю зображень, надійністю, довговічністю та зручністю використання; проведено порівняння МАІ та аргументовано вибір компонентів системи, наведені їх технічні характеристики.

Отримані результати створюють основу для розроблення практичної частини біометричної системи контролю доступу на основі відбитків пальців, яка буде реалізована в наступному розділі магістерської роботи.

3. ПРОЄКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ

3.1 Загальна концепція проєкту

Сучасний розвиток захищених систем вимагає створення доступних, надійних та простих у використанні систем контролю доступу. Існуючі на ринку України комерційні рішення біометричних систем контролю доступу є дуже дорогими та зазвичай орієнтованими на корпоративний сектор, що зменшує можливість їх застосування у простих побутових умовах. Саме тому актуальним є розробка бюджетної біометричної системи контролю доступу, яка буде реалізована на основі недорогих апаратних компонентів.

Метою даного проєкту є створення універсальної та економічно вигідної системи контролю доступу, яка буде здійснювати ідентифікацію користувача за відбитком пальця. Система такого типу повинна забезпечувати високий рівень безпеки, зручність використання та бюджетну вартість реалізації, що зробить її придатною для використання у приватних квартирах або будинках, невеликих офісах та складах.

Основна ідея полягає у побудові автономної системи, яка здійснює біометричну ідентифікацію користувача за допомогою сенсора відбитків пальців. Отримані дані порівнюються з шаблонами, збереженими в пам’яті. У разі успішного збігу система подає сигнал для розблокування електромеханічного замка.

Дана розробка спроєктована з недорогих, широко доступних компонентів, таких як плата керування Arduino UNO, сканера відбитків пальців R307, транзистор IRFZ44N, електромагнітний замок та блок живлення.

Таким чином, загальна концепція проєкту полягає у створенні простої, енергоефективної та бюджетної системи біометричного контролю доступу, яка поєднує в собі функціональність і доступність. Реалізація такого рішення

сприятиме популяризації біометричних технологій серед широкого кола користувачів і дозволить застосовувати їх у повсякденному житті.

3.2 Структурна схема пристрою

Структурна схема – це графічна модель, яка показує основні функціональні частини системи, та їх взаємодію між собою. Вона показує загальну структуру пристрою, його основні компоненти, а також зв'язки між ними, щоб у загальних рисах зрозуміти як працює пристрій.

На рисунку 3.1 наведено структурну схему біометричної системи контролю доступу на основі відбитків пальців.

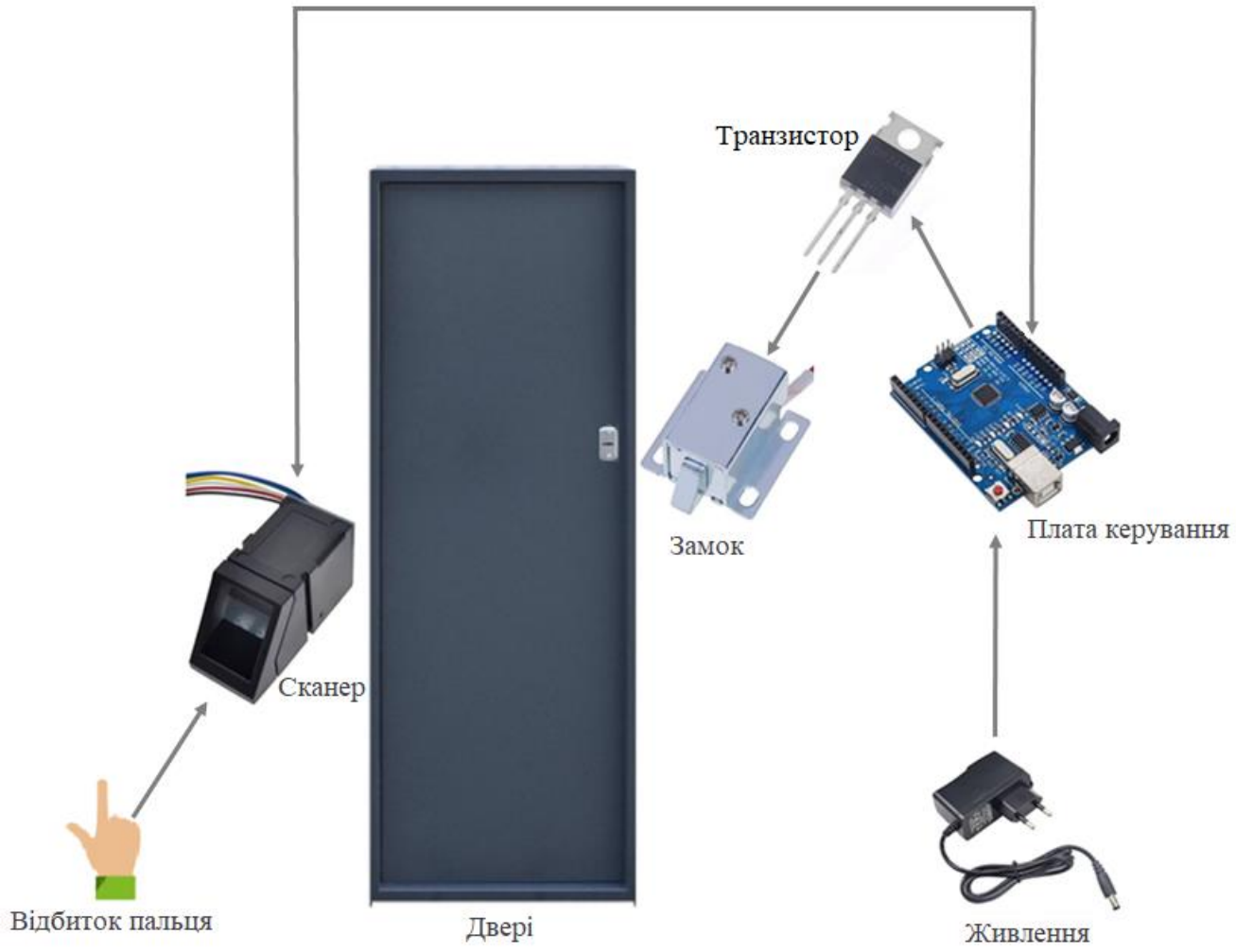


Рисунок 3.1 – Схема пристрою структурна

Система складається з таких основних елементів:

– Сканер – елемент системи, який здійснює зчитування біометричних даних користувача, формує цифровий шаблон та передає його до плати керування для подальшої обробки;

– Плата керування – центральний елемент системи, на якому реалізовано алгоритм ідентифікації користувача, обробка даних, прийняття рішень щодо надання або відмови у доступі, а також це елемент який керує виконавчими пристроями;

– Транзистор – елемент який забезпечує розв’язку між низьковольтною схемою керування та силовим колом живлення електромагнітного замка;

– Електромагнітний замок – виконуючий елемент системи, який утримує двері в положенні «Зачинено» та відкриває їх лише після отримання дозволу від системи;

– Блок живлення – елемент живлення системи, який постачає електричну енергію всім елементам системи.

Обмін даними між сканером та платою керування здійснюється через послідовний інтерфейс UART, який забезпечує надійну передачу інформації про результати біометричної ідентифікації. Транзистор підключається до цифрового виходу плати керування, отримуючи сигнал керування при успішному розпізнаванні користувача.

3.3 Алгоритм функціонування біометричної системи контролю доступу

Алгоритм функціонування системи описує логічну послідовність операцій, які забезпечують процес ідентифікації користувача за допомогою біометричних даних та прийняття рішення щодо надання або відмови в доступі. У даному алгоритмі відображено основні етапи роботи системи – від ініціалізації пристрою до активації виконавчого механізму.

На рисунку 3.2 подано схему алгоритму функціонування біометричної системи контролю доступу.

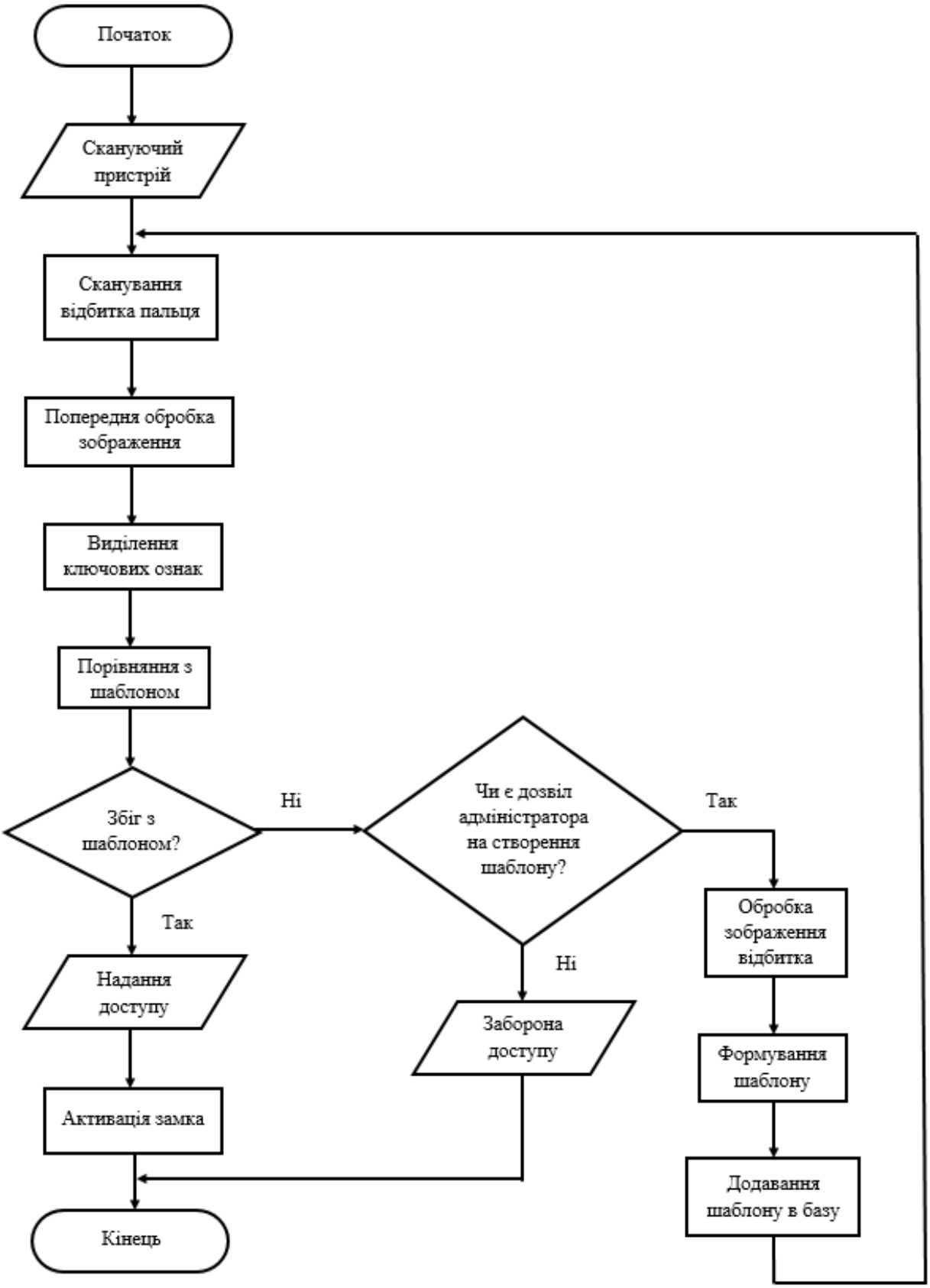


Рисунок 3.2 – Алгоритм роботи біометричної системи контролю доступу

Робота системи починається з подачі на неї живлення. Після подачі живлення на систему здійснюється перевірка всіх компонентів та їхня готовність до роботи.

Скануючий пристрій перебуває в очікуванні відбитка пальця. Після того як користувач прикладе палець до скануючого пристрою відбувається **сканування відбитка пальця**. Отримане зображення відбитка проходить **попередню обробку**, **виділення ключових ознак** та **порівняння з збереженим шаблоном** в пам'яті.

На основі результатів порівняння з шаблоном відбувається перевірка – **збіг з шаблоном**, в якої є два результати:

– **Результат збігу відбитка з шаблоном «Так»** – якщо відбиток співпадає з шаблоном система приймає рішення про надання доступу. У цьому випадку плата керування формує сигнал, який подається на транзистор, а вже він в свою чергу активує електромагнітний замок, що дозволяє користувачу відкрити двері.

– **Результат збігу відбитка з шаблоном «Ні»** – якщо відбиток не співпадає з збереженим шаблоном, тоді система чекає **дозвіл адміністратора на створення шаблону**, якщо **адміністратор надає відповідь «Ні»** – система забороняє доступ. Якщо **відповідь адміністратора «Так»** – тоді відбувається **обробка зображення відбитка**, **формування шаблону**, та **додавання отриманого шаблону до пам'яті пристрою**.

Після завершення циклу перевірки система повертається у стан очікування наступного запиту від користувача.

Таким чином наведений алгоритм описує послідовність процесів зчитування відбитка, його обробки та перевірки біометричних даних, що забезпечує автоматичне прийняття рішення щодо надання доступу користувачу. Запропонований підхід дозволяє підвищити рівень безпеки, усуває необхідність у використанні фізичних ключів, які можуть бути підроблені або загублені.

3.4 Принципова електрична схема пристрою біометричного контролю доступу

Схема електрична принципова – це графічне представлення, яке показує всі електричні елементи та зв'язки між ними у виробі, використовуючи графічне позначення. Даний тип схем дає найповніше уявлення про принцип роботи пристрою, його компоненти і зв'язки між ними, але не враховує розташування деталей та їх розміри. Цю схему використовують для складання монтажної схеми. Схему електричну принципову системи показано на рисунку 3.3.

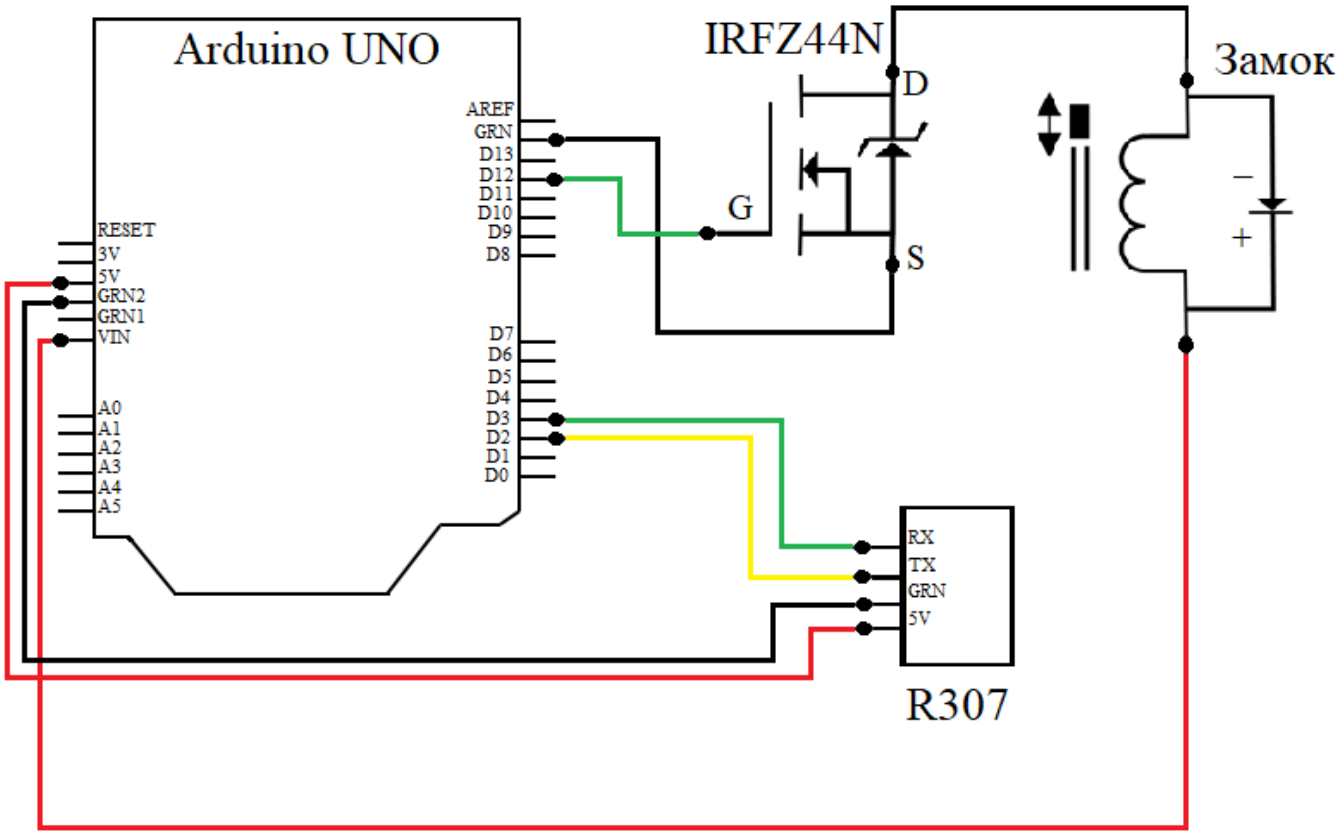


Рисунок 3.3 – Принципова електрична схема біометричної системи

Зображеними елементам на схемі є:

– **Плата Arduino UNO**, яка є центральним керуючим пристроєм всієї системи. Вона забезпечує обробку даних, які отримує від сканера відбитків, та формує сигнали керування для виконавчих пристроїв;

– **Сканер відбитків пальців R307**, який здійснює зчитування біометричних даних користувача. Сканер підключається до плати Arduino через інтерфейс UART:

- Вивід TX сканера під’єднаний до порту D2 на платі Arduino;
- Вивід RX сканера під’єднаний до порті D3 на платі Arduino;
- Живлення сканера здійснюється від лінії +5V;
- Контакт GRN з’єднано із загальною шиною заземлення.

– **Транзистор IRFZ44N**, виконує роль електронного перемикача сигналу, який керує живленням електромагнітного замка. Сигнал на затвор транзистора (вивід G) надходить з цифрового сходу D12 плати Arduino;

– **Електромагнітний замок**, живиться від зовнішнього джерела струму 12В через плату Arduino. Підключення здійснюється таким чином, щоб коли сигнал з Arduino подається на транзистор IRFZ44N відбувалось замкнення електричного кола і замок розблоковував двері;

– **Блок живлення**, забезпечує стабільше живлення 5В для плати Arduino та сканера R307, а також 12В для електромагнітного замка.

Принцип роботи схеми простий, після подачі живлення система переходить у режим очікування користувача. Коли користувач прикладає палець до сканера R307 формується цифровий відбиток, який порівнюється з збереженим шаблоном у пам’яті системи. У разі збігу мікроконтролер подає логічну одиницю на вихід D12, активуючи транзистор IRFZ44N. Через відкритий затвор транзистора подається живлення на електромагнітний замок, що призводить до розблокування дверей та надання доступу користувачу. Через визначений часовий інтервал сигнал перестає надходити, транзистор закривається, і замок повертається у початковий (закритий) стан.

Таким чином, принципова електрична схема демонструє взаємодію між апаратними компонентами системи та забезпечує логічну узгодженість між мікроконтролером, сканером, транзистором і замком.

3.5 Збірка макету біометричної системи контролю доступу

Наступним етапом виконання магістерського дипломного проєкту є збірка макету системи біометричного контролю доступу на основі відбитків пальців. З'єднання всіх компонентів системи виконується відповідно до схеми електричної монтажної, яка була створена за допомогою програмного продукту Fritzing [29].

Схема електрична монтажна – це детальне графічне зображення, яке показує розташування компонентів пристрою та їх з'єднання між собою. На відміну від принципової схеми, монтажна показує, як саме будуть прокладатись кабелі з'єднання, а не лише функціональні зв'язки між компонентами. Дана схема використовується для полегшення та правильності виконання збірки пристрою. Схему електричну монтажну системи контролю доступу показано на рисунку 3.4.

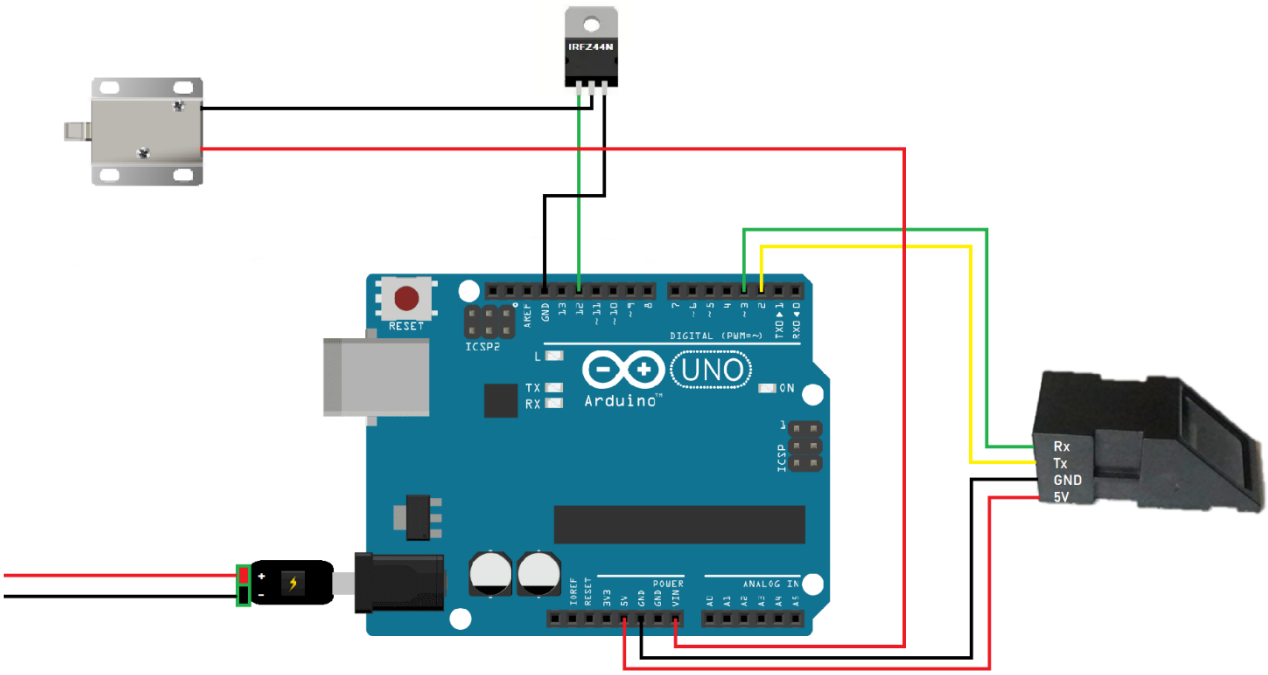


Рисунок 3.4 – Схема електрична монтажна біометричної системи контролю доступу

Збірка макету системи здійснюється за допомогою проводів-перемичок типу «тато-тато» та «мама-тато», це полегшує процес збірки та зменшує затрати на проєктування.

За корпус пристрою було взято пластиковий контейнер. Зібраний та готовий до програмування пристрій зображено на рисунку 3.5.

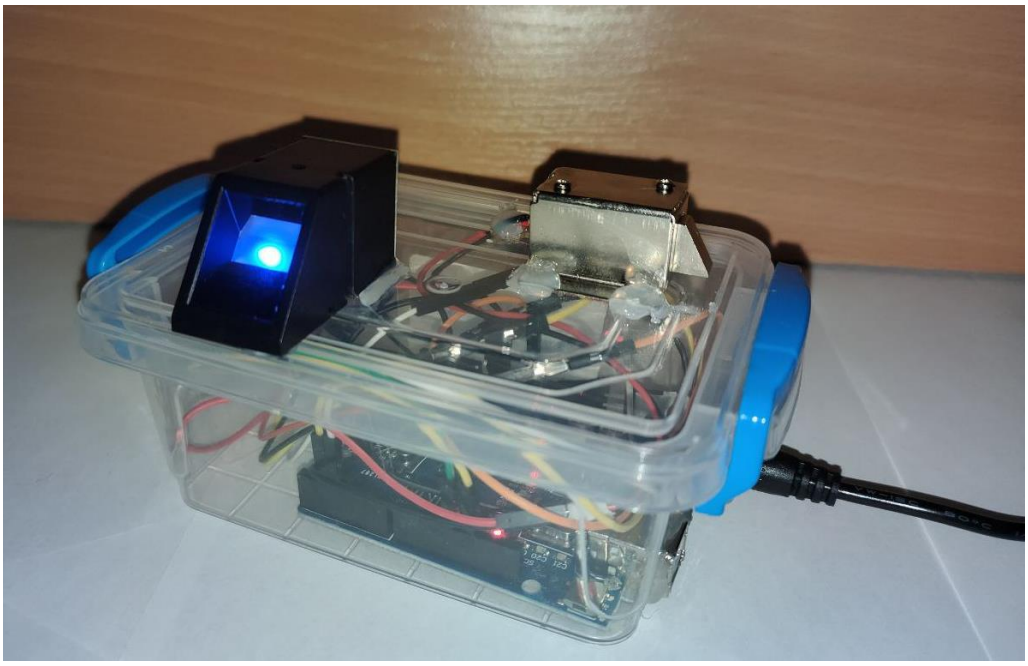


Рисунок 3.5 – Готовий пристрій

3.6 Розробка програмного забезпечення для системи біометричного контролю доступу на основі відбитків пальців

Для розробки програмного забезпечення системи біометричного контролю доступу було обрано середовище розробки Arduino IDE [30] від розробників Arduino Software.

Arduino IDE – це спеціалізоване програмне забезпечення, яке використовується для програмування мікроконтролерів сімейства Arduino. Дане середовище надає зручний і зрозумілий інтерфейс для написання, компіляції, перевірки та завантаження коду програми на плати сімейства Arduino через USB-порт за допомогою спеціалізованого кабелю. Середовище підтримує великий набір готових бібліотек, які значно спрощують взаємодію з електронними компонентами: датчиками, дисплеями, виконавчими модулями, модулями бездротового зв’язку тощо. Являється одним з найпопулярніших середовищ розробки серед початківців у сфері вбудованих систем та робототехніки.

Мова програмування Arduino базується на синтаксисі C/C++, що дає можливість реалізовувати як прості алгоритми керування, так і складні програмні логічні модулі з використанням функцій, структур, масивів, класів.

Програмна частина легко адаптується під зміну конфігурації або розширення апаратної частини, що забезпечує гнучкість і масштабованість при подальшому розвитку системи контролю доступу. Завдяки цьому розробка програмного забезпечення на базі Arduino IDE є ефективним рішенням для прототипування та створення практичних макетів біометричних систем.

Програма керування системою біометричного контролю доступу по відбитку пальця була розділена на два різні коди, перша частина коду відповідає за додавання відбитків пальців, а друга за перевірку відбитків та надання доступу. Ці дві частини коду побудовані на спеціальних бібліотека. Бібліотека Adafruit_Fingerprint.h [31] використовується для роботи з датчиком відбитків пальців, а бібліотека SoftwareSerial.h додана для створення програмного послідовного порту.

Розглянемо першу частину коду: необхідні бібліотеки підключаються на початку створення програмного коду, на рисунку 3.6 показано початок програми, підключення бібліотек та створення програмного послідовного порту на пінах 2 та 3.

sketch_code1.ino

```
1
2   #include <Adafruit_Fingerprint.h>
3   #include <SoftwareSerial.h>
4   SoftwareSerial mySerial(2, 3);
5
6   Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
7
8   uint8_t id;
```

Рисунок 3.6 – Початок програми та підключення бібліотек

Наступна частина коду програми зосереджена на реєстрації датчика відбитка пальця. Проводиться процес ініціалізації датчика, встановлюється швидкість передачі даних. Якщо датчик відбитка знайдено на екрані з'явиться напис «Знайдено датчик відбитків пальців», якщо датчик несправний, або не правильно підключений з'явиться напис «Незнайдено датчик відбитка пальців» і програма зупиниться. На рисунку 3.7 показано частину коду яка відповідає за ініціалізацію з'єднання з датчиком відбитків.

```
10  void setup()
11  {
12    Serial.begin(9600);
13    while (!Serial);
14    delay(100);
15    Serial.println("Реєстрація датчика відбитків пальців");
16
17    // встановити швидкість передачі даних для послідовного порту датчика
18    finger.begin(57600);
19
20    if (finger.verifyPassword()) {
21      Serial.println("Знайдено датчик відбитків пальців");
22    } else {
23      Serial.println("Незнайдено датчик відбитків пальців :(");
24      while (1) { delay(1); }
25    }
26  }
```

Рисунок 3.7 – Процес ініціалізації датчика відбитків пальців

Після перевірки зв'язку з датчиком відбитків переходимо до частини коду яка буде виконувати додавання відбитків пальців. Для того щоб додати відбиток користувач повинен ввести номер під яким хоче його зберегти (від 1 до 127), не цілі числа та число «0» не приймаються системою. Частину коду яка відповідає за ці дії показано на рисунку 3.8.

```
uint8_t readnumber(void) {
  uint8_t num = 0;

  while (num == 0) {
    while (! Serial.available());
    num = Serial.parseInt();
  }
  return num;
}

void loop()
{
  Serial.println("Готовність до реєстрації відбиткі пальця");
  Serial.println("Будь ласка, введіть ідентифікатор № (від 1 до 127), під яким ви хочете зберегти цей палець");
  id = readnumber();
  if (id == 0) {// № 0 не дозволено, спробйте ще раз
     return;
  }
  Serial.print("Ідентифікатор реєстрації №");
  Serial.println(id);

  while (!  getFingerprintEnroll() );
}
```

Рисунок 3.8 – Встановлення номеру відбитка

Після введення номеру під яким буде збережено відбиток переходимо до введення відбитку. Прикладаємо палець до сканера, якщо отримане зображення є коректним то переходимо на наступний етап, якщо ж зображення не є чітким отримаємо напис «Помилка зображення». Якщо виникли проблеми зі зв’язком отримаємо напис «Помилка зв’язку». Процес реєстрації відбитка показано на рисунку 3.9.

```
uint8_t getFingerprintEnroll() {

  int p = -1;
  Serial.print("Очікування реєстрації відбитка №"); Serial.println(id);
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Зображення зроблено");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.println(".");
      break;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Помилка зв'язку");
      break;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Помилка зображення");
      break;
    default:
      Serial.println("Невідома помилка");
      break;
    }
  }
```

Рисунок 3.9 – Процес реєстрації відитка пальця

Далі отримане зображення відбитка перетворюється в цифрову форму та здійснюється зняття повторного зображення. Повторне зображення порівнюється з цифровим шаблоном, якщо два зображення однакові відбиток зберігається в пам’яті сканера, якщо різні збереження не відбудеться. Частина коду яка відповідає за порівняння відбитків та їх збереження показано на рисунку 3.10.

```
78   p = finger.image2Tz(1);
79   switch (p) {
80     case FINGERPRINT_OK:
81       Serial.println("Зображення перетворене");
82       break;
83     case FINGERPRINT_IMAGEMESS:
84       Serial.println("Зображення низької якості");
85       return p;
86     case FINGERPRINT_PACKETRECIEVEERR:
87       Serial.println("Помилка зв'язку");
88       return p;
89     case FINGERPRINT_FEATUREFAIL:
90       Serial.println("Невдалось знайти відбитки пальців");
91       return p;
92     case FINGERPRINT_INVALIDIMAGE:
93       Serial.println("Невдалось знайти відбитки пальців");
94       return p;
95     default:
96       Serial.println("Невідома помилка");
97       return p;
98   }
99
154  Serial.print("Створення шаблону для №");  Serial.println(id);
155
156  p = finger.createModel();
157  if (p == FINGERPRINT_OK) {
158    Serial.println("Відбитки збігаються");
159  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
160    Serial.println("Помилка зв'язку");
161    return p;
162  } else if (p == FINGERPRINT_ENROLLMISMATCH) {
163    Serial.println("Відбитки пальців не збігаються");
164    return p;
165  } else {
166    Serial.println("Невідома помилка");
167    return p;
168  }
169
170  Serial.print("№"); Serial.println(id);
171  p = finger.storeModel(id);
172  if (p == FINGERPRINT_OK) {
173    Serial.println("Збережено");
174  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
175    Serial.println("Помилка зв'язку");
176    return p;
177  } else if (p == FINGERPRINT_BADLOCATION) {
178    Serial.println("Невділось зберегти в цьому місці");
179    return p;
180  } else if (p == FINGERPRINT_FLASHERR) {
181    Serial.println("Помилка запису на флеш-пам'ять");
182    return p;
183  } else {
184    Serial.println("Невідома помилка");
185    return p;
186  }
187 }
```

Рисунок 3.10 – Порівняння та збереження відбитків пальців

Перейдемо до другої частини коду. Проводимо підключення необхідних бібліотек, створюємо програмний послідовний порт на пінах 2 та 3, показано на рисунку 3.11.

sketch_code2.ino

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

SoftwareSerial mySerial(2, 3);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup()
{
  Serial.begin(9600);
  while (!Serial);
  delay(100);
  Serial.println("Тест відбитком");
  pinMode(12, OUTPUT);
```

Рисунок 3.11 – Початок другої частини коду

Далі проводиться перевірка підключення на функціонування датчика відбитків пальців, якщо датчик знайдено система видає напис «Знайдено датчик відбитків пальців» та переходить на наступний етап, якщо датчик не знайдено система видає напис «Незнайдено датчик відбитків пальців» та зупиняє виконання програми, цю частину коду зображено на рисунку 3.12.

```
  finger.begin(57600);

  if (finger.verifyPassword()) {
    Serial.println("Знайдено датчик відбитків пальців");
  } else {
    Serial.println("Незнайдено датчик відбитків пальців(");
    while (1) { delay(1); }
  }

  finger.getTemplateCount();
  Serial.print("Датчик містить"); Serial.print(finger.templateCount); Serial.println("шаблони");
  Serial.println("Очікування відбитка пальця");
}
```

Рисунок 3.12 – Перевірка підключення датчика

Після цього активується функція пошуку та ідентифікації відбитків. Коли користувач доторкається сканера система знімає відбиток пальця, якщо зображення немає дефектів система видає напис «Зображення зроблене» та переходить на наступний етап. Якщо зображення з дефектами або низької якості система видає напис «Помилка зображення» та просить повторити спробу. Ця частина коду показана на рисунку 3.13.

```
33  void loop()
34
35  {
36    getFingerprintIDez();
37    delay(50);
38    digitalWrite(12, LOW);
39  }
40
41  uint8_t getFingerprintID() {
42    uint8_t p = finger.getImage();
43    switch (p) {
44      case FINGERPRINT_OK:
45        Serial.println("Зображення зроблено");
46        break;
47      case FINGERPRINT_NOFINGER:
48        Serial.println("Палець не виявлено");
49        return p;
50      case FINGERPRINT_PACKETRECIEVEERR:
51        Serial.println("Помилка зв'язку");
52        return p;
53      case FINGERPRINT_IMAGEFAIL:
54        Serial.println("Помилка зображення");
55        return p;
56      default:
57        Serial.println("Невідома помилка");
58        return p;
59    }
```

Рисунок 3.13 – Зняття відбитка пальця

Далі отримане зображення перетворюється в цифрову форму та виконується порівняння шаблонів в пам’яті датчика, якщо є збіг відбитка з шаблоном система видає напис «Знайдено ідентифікатор №» подається сигнал на електромагнітний замок та відбувається відчинення замка. Якщо збіг не виявлено система видає «Невдалось знайти відбиток пальця» і далі не працює, цю частину коду показано на рисунку 3.14.

sketch_code2.ino

```
  p = finger.image2Tz();
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Зображення перетворено");
      break;
    case FINGERPRINT_IMAGEMESS:
      Serial.println("Зображення низької якості");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Помилка зв'язку");
      return p;
    case FINGERPRINT_FEATUREFAIL:
      Serial.println("Невдалось знайти відбиток пальця");
      return p;
    case FINGERPRINT_INVALIDIMAGE:
      Serial.println("Невдалось знайти відбиток пальця");
      return p;
    default:
      Serial.println("Невідома помилка");
      return p;
  }

  p = finger.fingerFastSearch();
  if (p == FINGERPRINT_OK) {
    Serial.println("Знайдено збіг відбитків");
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Помилка зв'язку");
    return p;
  } else if (p == FINGERPRINT_NOTFOUND) {
    Serial.println("Незнайдено відповідності");
    return p;
  } else {
    Serial.println("Невідома помилка");
    return p;
  }


  Serial.print("Знайдено ідентифікатор №"); Serial.print(finger.fingerID);
  Serial.print(" з упевненістю "); Serial.println(finger.confidence);

  return finger.fingerID;
}
int getFingerprintIDez() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK)  return -1;

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

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



  digitalWrite(12, HIGH);
  delay(3000);
  digitalWrite(12, LOW);

  Serial.print("Знайдено ідентифікатор №"); Serial.print(finger.fingerID);
  Serial.print("  з упевненістю "); Serial.println(finger.confidence);
  return finger.fingerID;
}
```

Рисунок 3.14 – Перевірка відбитка та надання доступу

3.7 Програмування плати системи біометричного контролю доступу на основі відбитків пальців

Після написання програмного коду для системи біометричного контролю доступу наступним кроком є його перевірка, компіляція та завантаження на плату керування Arduino UNO. Всі перераховані етапи буде виконано в середовищі Arduino IDE.

Щоб провести перевірку коду на панелі інструментів в середовищі Arduino IDE шукаємо пункт Verify, натискаємо його та чекаємо результатів перевірки коду, ці дії показано на рисунку 3.15.

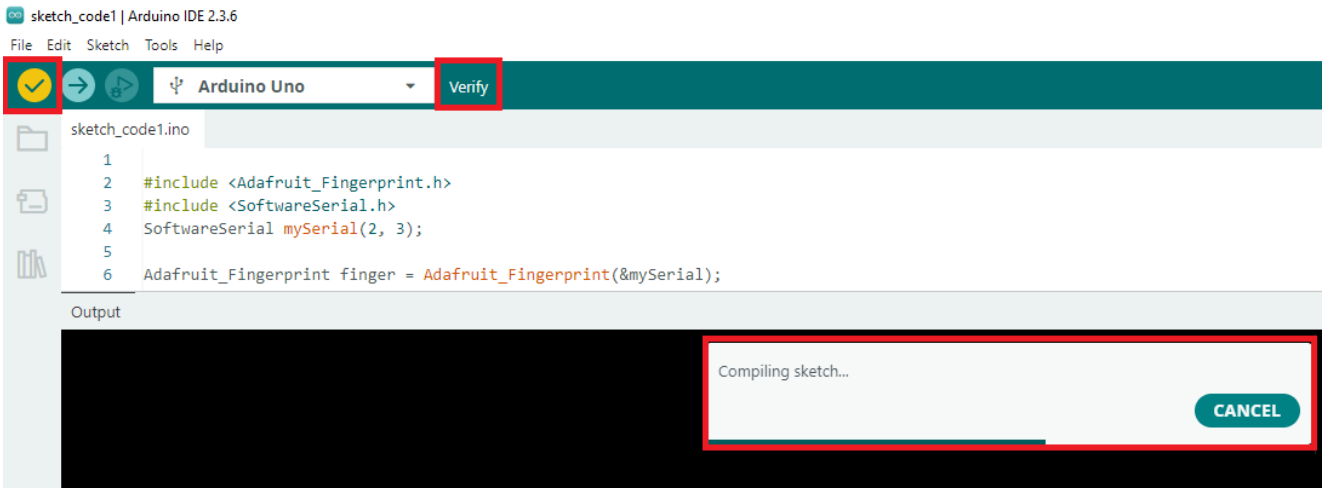


Рисунок 3.15 – Процес перевірки коду

Якщо в написаному коді немає помилок, завантажені необхідні бібліотеки і синтаксис написання коду правильний, тільки тоді перевірка коду пройде успішно. В результаті перевірки коду середовище розробки покаже скільки місця займає код на платі керування. Успішна перевірка програмного коду показана на рисунку 3.16.

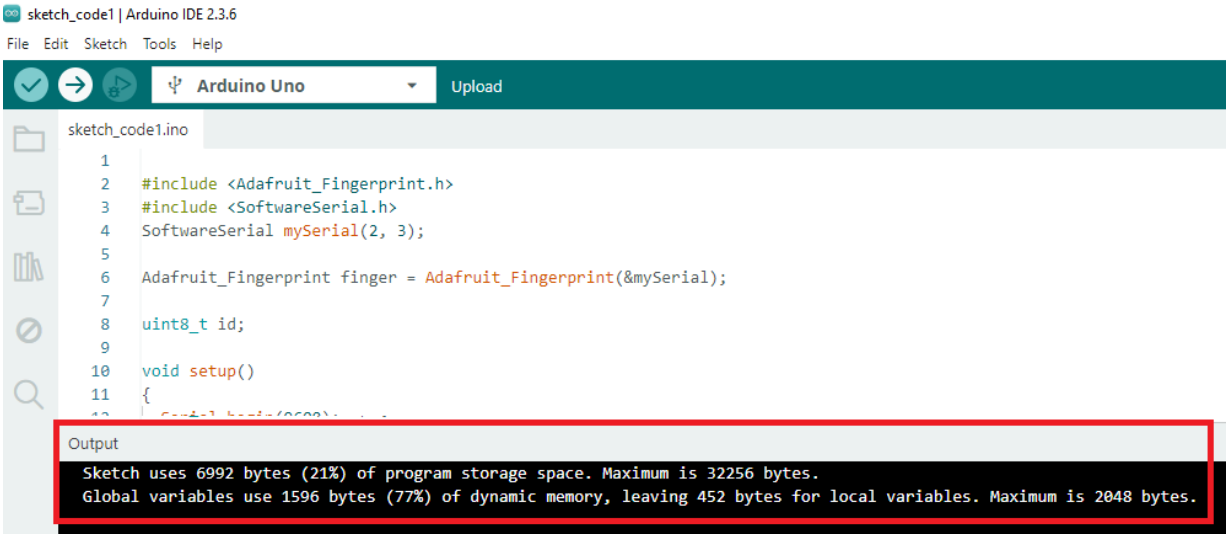


Рисунок 3.16 – Результат успішної перевірки програмного коду

Після успішно проведеної перевірки коду можна переходити до програмування плати Arduino UNO. Для початку проводимо підключення плати до ПК за допомогою спеціального дата кабелю, як показано на рисунку 3.17.

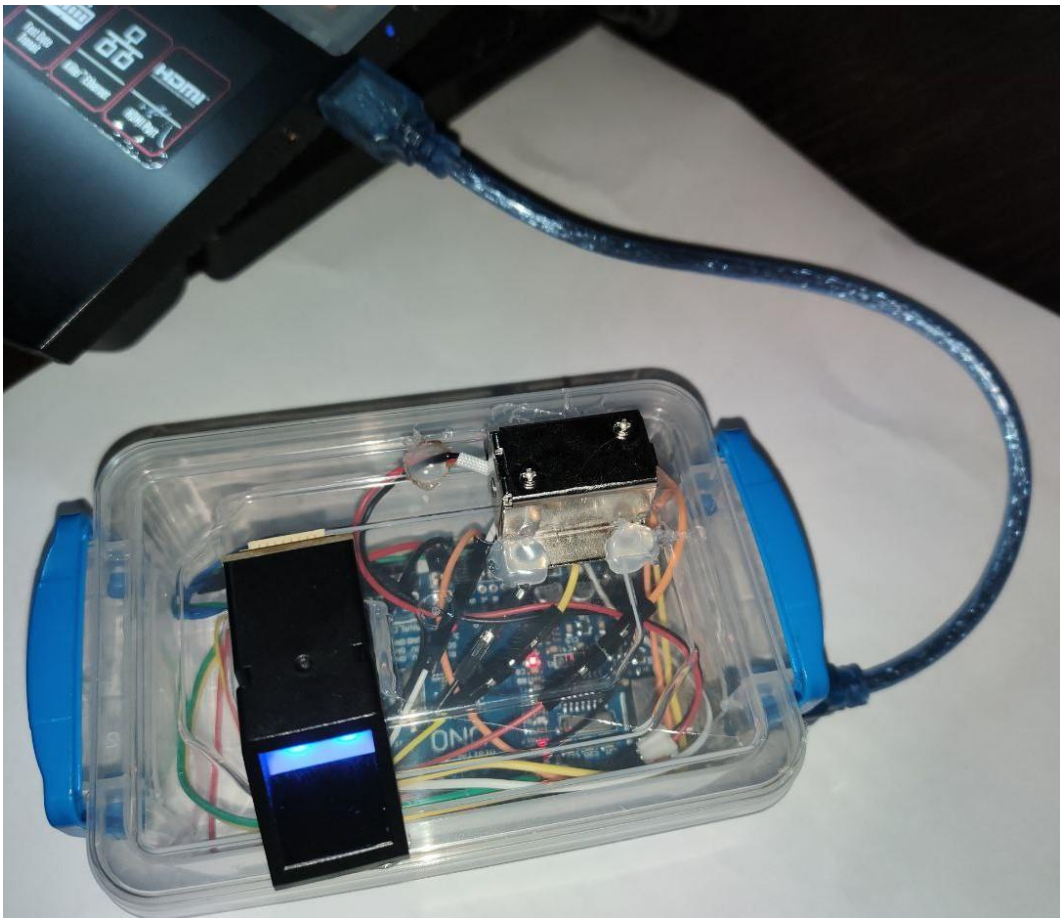


Рисунок 3.17 – Підключення плати для програмування

Якщо підключення пройшло успішно можна переходити до процесу вибору порту, моделі плати та програмування. Зазвичай середовище саме покаже до якого порту на ПК підключена ваша плата керування, для цього необхідно на панелі середовища Arduino IDE обрати «Tools» → «Port» та обрати порт до якого підключена плата, ці дії показано на рисунку 3.18.

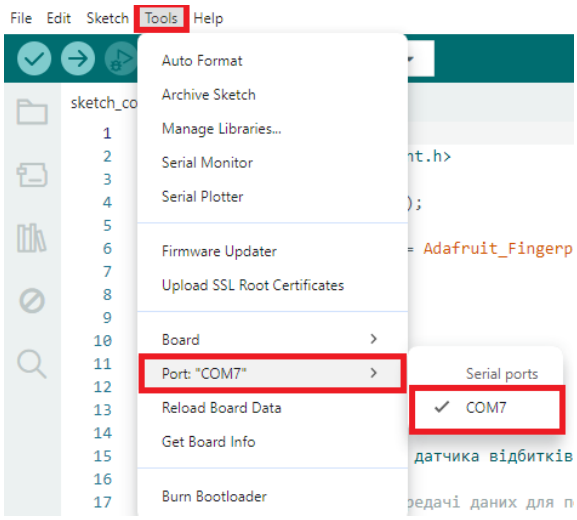


Рисунок 3.18 – Процес вибору порту

Для вибору моделі плати яку ви хочете програмувати є два способи:

– на панелі середовища Arduino IDE обрати «Select Board» → натиснути на порт через який підключена плата і середовище саме автоматично підтягне необхідну модель плати, це показано на рисунку 3.19;

– або ж натиснути «Select Board» та у вікні що з'явилось самостійно ввести модель та обрати плату, показано на рисунку 3.20.

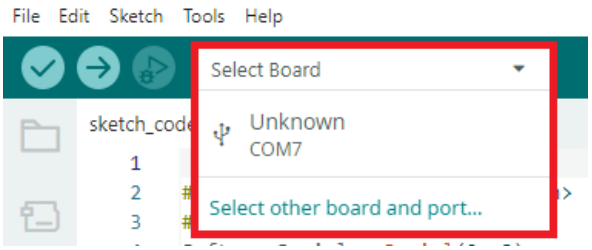


Рисунок 3.19 – Автоматичний вибір моделі плати

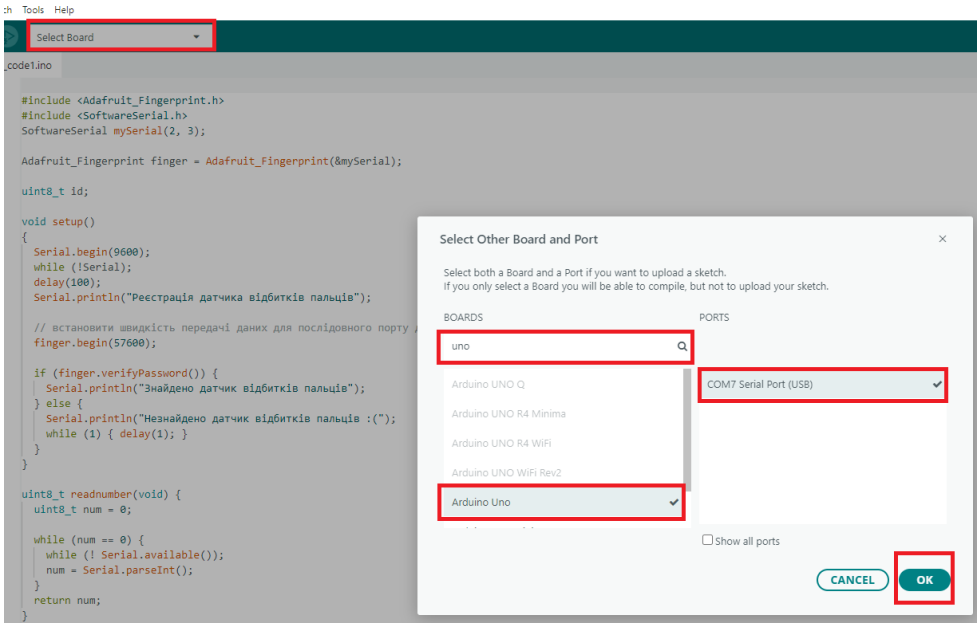


Рисунок 3.20 – Самостійний вибір моделі плати

Коли всі параметри обрані переходимо до завантаження першої частини коду програми на плату. На панелі інструментів обираємо значок «→» та очікуємо кінця завантаження коду на плату, дії показані на рисунку 3.21.

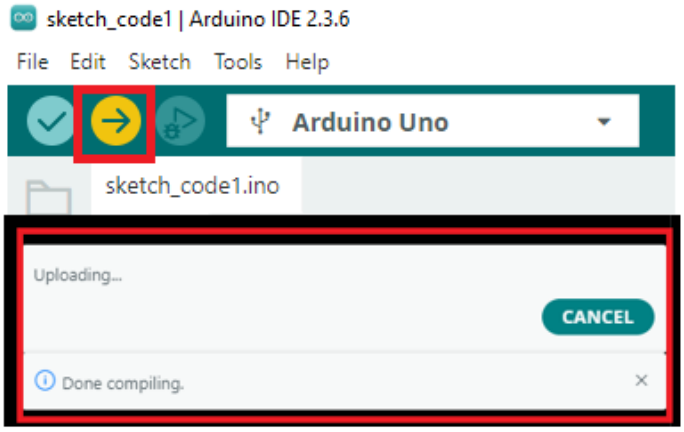


Рисунок 3.21 – Процес завантаження коду

Після завантаження першої частини коду на плату переходимо до завантаження відбитків пальців користувачів системою. Для цього необхідно в програмному середовищі обрати «Serial Monitor» дочекатись повідомлення що датчик відбитків пальців знайдено, обрати номер під яким буде збережено палець, це показано на рисунку 3.22.

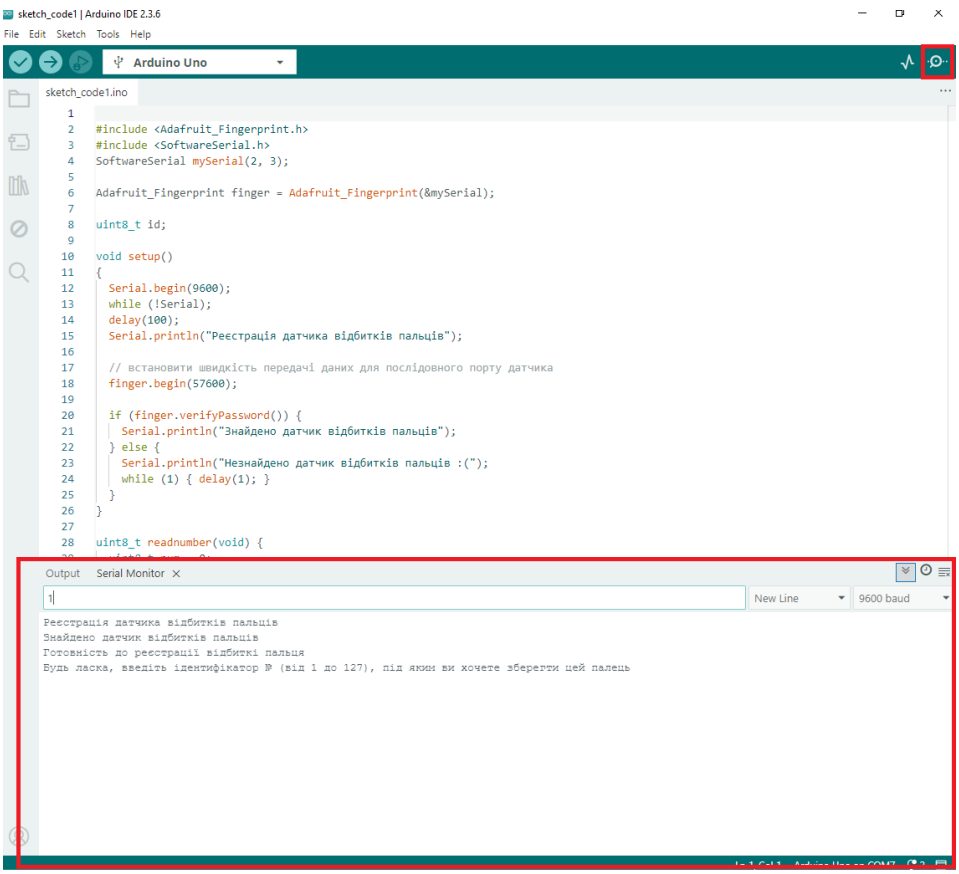


Рисунок 3.22 – Початок додавання відбитків

Після вибору номера відбитка натискаємо на клавіатурі «Enter» система буде очікувати поки користувач прикладе відповідний палець до сканера відбитків, показано на рисунку 3.23.

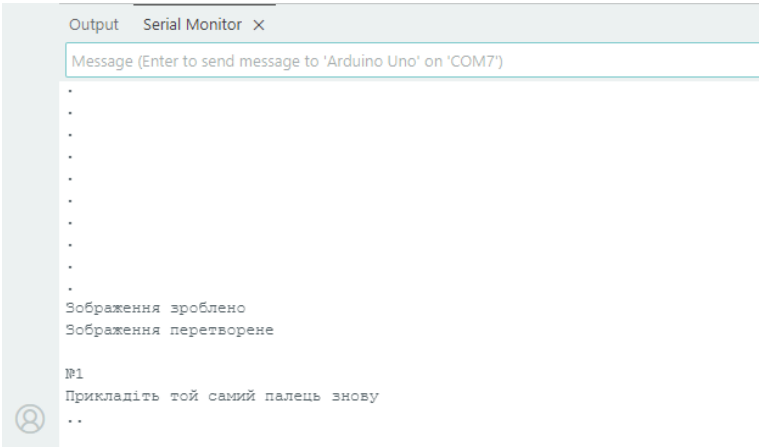


Рисунок 3.23 – Додавання відбитка пальця

Після додавання відбитків пальців переходимо до другої частини програмного коду, завантажуємо її в плату керування Arduino UNO як це було і з першою частиною, заходимо в пункт «Serial Monitor» доторкуємось пальцем відбиток якого додали в першій частині та дивимось за результатом, показано на рисунку 3.24.

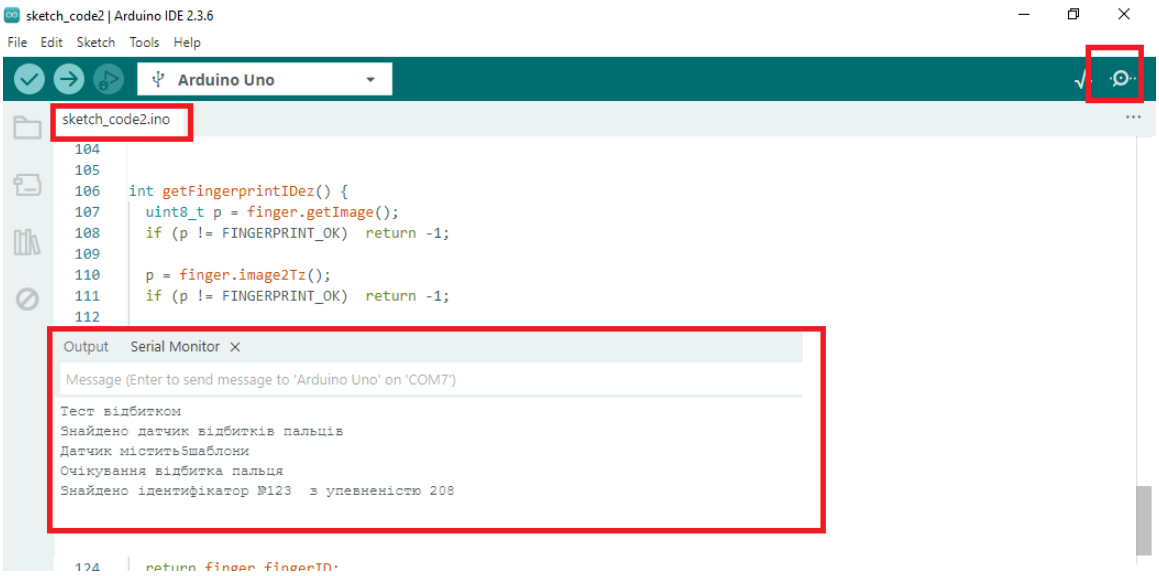


Рисунок 3.24 – Робота другої частини коду

Після того як користувач доторкнувся пальцем відбиток якого був доданий до системи, вона перевірила його знайшла збіг видала на екран номер під яким збережений цей відбиток та надала доступ цьому користувачу у вигляді відкритого замка.

3.8 Економічний аналіз проєкту біометричної системи контролю доступу

Ця частина проєкту спрямована на визначення собівартості розробки системи біометричного контролю доступу на основі відбитків пальців, а також на аналізі доцільності її створення шляхом порівняння з існуючими комерційними рішеннями.

Розглянемо витрати на компоненти системи та матеріали для її збірки, перелік використаних компонентів, їх кількість та вартість наведено в таблиці 3.1.

Таблиця 3.1 – Вартість компонентів системи

Компонент	**Кількість**	**Вартість**
Arduino UNO	1	160 грн.
R307	1	380 грн.
IRFZ44N	1	15 грн.
Електронний замок	1	140 грн.
Блок живлення 12 В	1	130 грн.
Перемички для збірки	1 комплект	114 грн.
Сума		**939 грн.**

Провівши розрахунок, маємо вартість матеріалів, необхідних для створення макета системи, яка становить 939 гривень.

Так як проєктування прототипу, збірка макету, розробка програми та тестування макету виконувались власноруч в рамках виконання дипломного проєкту, тому додаткові фінансові вкладення не передбачались. У вище вказаних розрахунках враховано тільки фактичні витрати на матеріали для створення працездатного прототипу системи.

Хоч у процесі створення системи не було задіяно витрат на оплату праці, було б доцільно оцінити також ринкову вартість виконаних робіт. Це дозволить об’єктивно порівняти собівартість розробки прототипу з комерційними рішеннями та визначити економічну доцільність його впровадження.

До складу робіт, які потрібно виконати для отримання діючої системи входить: проєктування системи, створення програмного продукту та тестування системи. Загальна трудомісткість зазначених робіт приблизно становить 50 годин, виходячи з обсягу необхідних до проведення робіт.

Середня ринкова вартість роботи проєктувальника аналогічних робіт в Україні становить 200 грн/год., приблизний час на проєктування становить 30 годин.

Середня ринкова вартість роботи програміста який працює з СКУД в Україні становить 234 грн/год., приблизний час затрачений на написання програми становить 10 годин.

Середня ринкова вартість роботи тестувальника в Україні становить 200 грн/год., приблизний ас тестування системи 10 годин.

Таким чином проводимо розрахунки витрат на оплату праці.

$$ЗП_{проєкт.} = Н \times R, \quad (3.1)$$

де Н – кількість годин,

R – годинна ставка

$$ЗП_{проєкт.} = 30 \times 200 = 6000 \text{ грн.},$$

$$ЗП_{програм.} = Н \times R, \quad (3.2)$$

де Н – кількість годин,

R – годинна ставка

$$ЗП_{програм.} = 10 \times 234 = 2340 \text{ грн.},$$

$$ЗП_{тестув.} = Н \times R, \quad (3.3)$$

де Н – кількість годин,

R – годинна ставка

$$ЗП_{тестув.} = 10 \times 200 = 2000 \text{ грн.},$$

$$С_{загальна} = ЗП_{проєкт.} + ЗП_{програм.} + ЗП_{тестув.} + С_{матеріали}, \quad (3.4)$$

де $ЗП_{проєкт}$ – заробітна плата проєктувальника,

$ЗП_{програм.}$ – заробітна плата програміста,

$ЗП_{тестув.}$ – заробітна плата тестувальника,

$С_{матеріали}$ – сума затрат на матеріали

$$С_{загальна} = 6000 + 2340 + 2000 + 939 = 11279 \text{ грн.}$$

Таким чином, після проведення розрахунків на оплату праці проєктувальника, програміста, тестувальника та матеріали для збірки системи загальна вартість складає 11279 гривень.

Далі є доцільним провести економічне порівняння з комерційними рішеннями які представлені на ринку України. Проаналізувавши представлені на нашому ринку моделі біометричних терміналів які працюють на відбитку пальця можемо виділити декілька бюджетних, середньо бюджетних та дорогих моделей, таких як:

- бюджетні (до 2000 грн)
  - ZKTeco X6 All-in-One Access Machine;
- середньо бюджетні (до 6000 грн)
  - Network Fingerprint Access Controller;
  - Hikvision K1T804A Fingerprint Terminal;
  - ZKTeco F18 Fingerprint Reader;
- дорогі (до 12000 грн)
  - ZKTeco ZK-UA760 Time & Attendance Terminal.

Треба зауважити що вище перераховані моделі та вартість тільки терміналів зняття відбитків пальців, які є однією з складових частин біометричної системи контролю доступу, але не є повноцінною системою. Для повноцінного функціонування ще необхідна низка інших складових, таких як: замок, блок живлення, контролер доступу, кнопки виходу, програмне забезпечення. Також не варто забувати про монтаж та налаштування системи.

Склавши всі ці компоненти вартість середньо бюджетної системи контролю доступу стане від 15000 до 30000 гривень [32].

Визначимо переваги та недоліки впровадження власної системи контролю доступу.

Переваги власної системи:

- нижча собівартість;
- можливість самостійної модернізації та розширення системи;
- можливість проведення ремонту власноруч;

– освітня цінність.

Недоліки власної системи:

– відсутність сертифікації та гарантії;

– менша надійність у порівнянні з промисловими терміналами;

– обмежена можливість масштабування системи;

– відсутність підтримки та оновлень від виробника.

Аналіз який був проведений показує, що собівартість виготовлення прототипу біометричної системи контролю доступу є суттєво нижчою, ніж вартість готових комерційних пристроїв. Навіть у разі врахування витрат на оплату праці розробника, загальна вартість системи залишається конкурентною.

Отже, створення власного прототипу є економічно доцільним у навчальних, експериментальних та наукових цілях, а також у проєктах, де пристрій потребує тестування або індивідуального налаштування. Для масового виробництва комерційні рішення залишаються вигіднішими, так як впровадження чогось авторського завжди дорожче ніж рішення які вже є на ринку. Однак розроблений пристрій має переваги в гнучкості, адаптивності та більшій варіативності змін.

3.9 Тестування та оцінка ефективності роботи системи

Для оцінки ефективності та надійності розробленої біометричної системи контролю доступу було проведене комплексне експериментальне тестування. Основна мета даного тестування полягає в визначенні показників якості роботи системи, а також її працездатності в умовах наближених до реальних.

В процесі тестування застосовані ключові показники продуктивності біометричних систем, такі як: FAR (False Acceptance Rate) – рівень помилкового прийняття, FRR (False Rejection Rate) – рівень помилкової відмови, TAR (True Acceptance Rate) – рівень правильного прийняття.

Так як доступ до біометричних даних сторонніх осіб був обмежений, тестування було вирішено проводити за методом імітації користувачів, тобто використання відбитків різних пальців як кожного окремого користувача.

Оцінка ефективності проводиться в кількох групах тестів:

- рівень правильного прийняття (TAR), показано в таблиці 3.2;
- рівень помилкових відмов (FRR), показано в таблиці 3.3;
- рівень помилкового прийняття (FAR), показано в таблиці 3.4.

Таблиця 3.2 – Рівень правильного прийняття

Критерії	**Кількість успішних ідентифікацій**		
	1 користувач	2 користувач	3 користувач
10 разів піднести палець	10	10	10
10 разів піднести палець при повороті	10	10	10
10 разів піднести палець з різною силою натиску	10	10	10
Середній час ідентифікації	до 1 секунди	до 1 секунди	до 1 секунди

В таблиці показаній вище наведені дані по тестуванню системи з різними критеріями, це зроблено для того щоб зрозуміти наскільки система правильно приймає користувачів. Проведемо розрахунок показника TAR для кожного користувача.

$$\text{TAR} = \frac{(\text{кількість коректних прийнять})}{(\text{загальна кількість спроб})} \times 100\%, \qquad (3.5)$$

$$1\_\text{TAR} = \frac{30}{30} \times 100\% = 1$$

$$2\_\text{TAR} = \frac{30}{30} \times 100\% = 1$$

$$3\_\text{TAR} = \frac{30}{30} \times 100\% = 1$$

Таблиця 3.3 – Рівень помилкових відмов

Критерії	**Кількість успішних ідентифікацій**		
	1 користувач	2 користувач	3 користувач
10 разів коли шкіра волога	10	9	10
10 разів з дуже швидким прикладанням пальця	9	8	8

В цій таблиці наведені дані тестування при несприятливих факторах, це зроблено для щоб зрозуміти наскільки коректно система надасть доступ користувачу з умовами які можуть заважати ідентифікації. Проведемо розрахунок показника FRR для кожного користувача.

$$\text{FRR} = \frac{(\text{кількість хибних відмов})}{(\text{загальна кількість спроб})} \times 100\%, \tag{3.6}$$

$$1\_\text{FRR} = \frac{1}{20} \times 100\% = 0{,}05$$

$$2\_\text{FRR} = \frac{3}{20} \times 100\% = 0{,}15$$

$$3\_\text{FRR} = \frac{2}{20} \times 100\% = 0{,}10$$

Таблиця 3.4 – Рівень помилкового прийняття

Критерії	**Кількість успішних ідентифікацій**	
	Незареєстрований користувач 1	Незареєстрований користувач 2
10 спроб доступу з різних положень пальця	0	0

В даній таблиці показано дані про спробу доступу двох незареєстрованих користувачів. Проведемо розрахунок показника FAR для двох незареєстрованих користувачів.

$$FAR = \frac{(\text{кількість хибних прийнять})}{(\text{загальна кількість спроб})} \times 100\%, \quad (3.7)$$

$$1\_FAR = \frac{0}{10} \times 100\% = 0$$

$$2\_FAR = \frac{0}{10} \times 100\% = 0$$

Результати проведених тестувань наведені в таблиці 3.5.

Таблиця 3.5 – Результати тестування

Показник	**Результат**	**Статус**
TAR	100%/ 100% /100%	Коректний
FRR	0,05/ 0,15/ 0,10	Коректний
FAR	0/0	Коректний

Проведене тестування біометричної СКД на основі відбитків пальців показало високий рівень коректності роботи системи. За результатами тестів система продемонструвала 100% показник TAR (рівень правильного прийняття), що свідчить про коректне та стабільне розпізнавання зареєстрованих користувачів у стандартних умовах експлуатації.

Аналіз стійкості до несприятливих факторів, які ускладнюють зчитування, показав, що значення FRR (рівень помилкової відмови) знаходяться в межах 0, 05 – 0, 15, це є прийнятним для недорогих оптичних сенсорів та характеризує систему як достатньо надійну.

Перевірка здатності системи протидіяти несанкціонованому доступу встановила, що FAR (рівень помилкового прийняття) = 0, тобто в ході тестів не було зафіксовано жодного випадку помилкового прийняття сторонніх користувачів. Це підтверджує належний рівень безпеки та мінімальний ризик надання доступу незареєстрованому користувачу.

За результати тестування можна сказати, що розроблена система характеризується високою точністю, надійністю та ефективністю. Поєднання нульового рівня FAR та низьких значень FRR вказує на коректну реалізацію алгоритмів розпізнавання та достатню якість сенсора. Отримані дані дозволяють зробити висновок про відповідність системи вимогам, що висуваються до сучасних біометричних систем контролю доступу.

Також під час вище вказаних тестувань було проведено «стрес-тестування» система працювала без перерви 15-20 хвилин, за цей час проведено більше 160 сканувань відбитків. На початку тестування система показувала себе стабільно та без нарікань, але ближче до кінця тестувань електромагнітний замок став помітно нагріватись та його робота стала погіршуватись.

3.10 Висновок по розділу 3

У третьому розділі магістерської роботи основну увагу зосереджено на проєктуванні та реалізації біометричної системи контролю доступу на основі відбитків пальців. На початку даного розділу сформована загальна концепція проєкту, яка передбачає створення доступної, функціональної та надійної системи. Розроблено структурну схему пристрою, яка визначила взаємодію основних компонентів системи між собою. Також наведено та описано алгоритм функціонування системи, який показує послідовність виконання процесів сканування відбитків, формування шаблонів та автентифікації користувачів.

Було побудовано принципову електричну схему пристрою, яка показує всі компоненти системи та описує їх головні ролі в системі. Далі була проведена збірка прототипу системи, з’єднання всіх компонентів системи виконується відповідно до схеми електричної монтажної, яка була створена.

Паралельно було виконано розробку програмного забезпечення, яке реалізує основні функції біометричної системи контролю доступу на основі відбитків пальців. Здійснено програмування плати керування.

Проведено економічний аналіз доцільності створення власної системи та порівняння її з комерційними рішеннями представленими на ринку України. Результати підтвердили доцільність і економічну доступність створеного рішення. В кінці розділу проведено тестування системи, яке було зосереджене на точності, швидкодії та надійності системи. Отримані результати підтвердили ефективність розробленої системи та відповідність її основним вимогам, визначеним на етапі проєктування.

Підсумовуючи проведену роботу в даному розділі було: виконано проєктування системи, створено її апаратну та програмну частини, здійснено економічний аналіз розробки та проведено тестування, що дозволило підтвердити працездатність і ефективність запропонованого рішення.

ВИСНОВОК

Метою дослідження є розв’язання актуальної задачі – створення ефективного та бюджетного варіанта технології біометричного контролю доступу, яка буде відповідати сучасним вимогам функціонування та забезпечувати надійний рівень безпеки для широкого кола користувачів.

Для розв’язання цієї задачі проведено порівняльний аналіз існуючих СКУД: Особливу увагу приділено біометричним методам ідентифікації, порівняно статичні та динамічні методи, за результатами порівняння обрано метод відбитків пальців для подальших досліджень.

З метою побудови ефективного варіанту технології проведений багатокритерійний аналіз ефективності ключових компонентів системи. Порівняно підходи, способи, інструментарії надання доступу та методи зняття відбитків пальців. Порівняння проведено на основі аналізу ієрархії критеріїв ефективності в умовах кількісного та якісного представлення порівняльних характеристик та з урахуванням пріоритету для користувача з точки зору визначених вимог.

Розроблений проєкт та виконана програмно-апаратна реалізація технології на основі наступних етапів: формування концепції розробки, структурну й принципову схеми, алгоритм роботи та програмну складову системи. Виконано збірку та налаштування прототипу, проведено тестування системи.

Науково-практична новизна отриманих результатів полягає в отриманні комплексної технології бюджетної біометричної системи контролю доступу, орієнтовану на автономну роботу без підключення до неї серверних баз даних. Удосконалено метод побудови апаратно-програмної частини проєкту з використанням бюджетних та відкритих платформ, що дозволяє адаптувати систему під різні умови використання.

Результати тестування демонструють, що розроблена система є ефективною, стабільною, економічно доцільною та придатною для практичного використання в реальних умовах. Наукові та практичні результати, які були отримані в ході виконання роботи, можуть бути використані для подальшого вдосконалення

біометричних рішень, а також як основа для розширення функціональності системи в майбутньому.

Результати роботи мають практичне значення для приватних будинків, навчальних закладів, офісів та малих підприємств, яким необхідно забезпечити персоналізований доступ до приміщень або інформації. Запропоновану систему можна реалізувати у вигляді окремого пристрою або як модуль у складі більш складних комплексів.

Додатковим матеріалом до проведених досліджень є наукові публікації, які безпосередньо стосуються теми магістерської роботи. Теза «Проблеми надійності та безпеки системи контролю доступу на основі біометрії», що надана для публікації в збірнику конференції «БУД-МАЙСТЕР-КЛАС-2025» містить аналіз ключових факторів, що впливають на ефективність та захищеність біометричних систем. У роботі визначено основні проблеми надійності та загрози безпеки. Отримані результати слугують важливою основою для формування рекомендацій щодо підвищення стійкості та безпеки сучасних біометричних систем контролю доступу [33].

Окрім очевидних недоліків біометричних методів автентифікації, суттєву роль відіграють загрози від шкідливого програмного забезпечення. З огляду на це, важливо розуміти особливості роботи шкідливих програм, механізми їхнього впливу на системи та можливі вектори атак. Саме з цією метою була опублікована теза на конференції «БУД-МАЙСТЕР-КЛАС-2024» на тему «Аналіз сучасного шкідливого програмного забезпечення та методи боротьби з ним» [34].

Напрямки подальшого удосконалення можуть бути такі:

- підвищення функціональності та точності за рахунок застосування більш сучасних компонентів;
- додавання централізованої бази даних користувачів; впровадження багатофакторної автентифікації;
- розширення системи шляхом додавання журналу поді, системи оповіщення та системи відеонагляду;

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Системи контролю доступу ZKTeco [Електронний ресурс] – Режим доступу: https://zkstore.com.ua/ua/g1402214-sistemy-kontrolya-dostupa

2. Системи контролю доступу HID Global [Електронний ресурс] – Режим доступу: https://www.hidglobal.com/products

3. Системи контролю доступу Suprema [Електронний ресурс] – Режим доступу: https://supremainc.com.ua/produkty-suprema/

4. Arduino-driver smart door lock with fingerprint authentication and Bluetooth control [Електронний ресурс] – Режим доступу: https://www.ijesat.com/ijesat/files/V20I301_1750330419.pdf

5. Intelligent Fingerprint-Based Access System with Camera / Marina Daniela SAS [Електронний ресурс] /Carpathian Journal of Electrical Engineering. 2021. Vol. 15, – Режим доступу: https://oaji.net/articles/2023/3162-1687874301.pdf

6. Design of Arduino-Based Fingerprint Security System in the Financial Archive Room / T. M. Tamtelahitu, R. Siwalette. – 2025. Journal of Artificial Intelligence and Engineering Applications. Vol. 4, – Режим доступу: https://www.researchgate.net/publication/389027060_Design_of_Arduino-Based_Fingerprint_Security_System_in_the_Financial_Archive_Room_Dinas_Pariwisata_Kabupaten_Maluku_Tengah

7. Писаренко Д. Г. Сучасна система контролю та управління доступом / Д. Г. Писаренко, Ю. Ю. Нестюк, А. С. Васюра [Електронний ресурс] – Режим доступу: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/29344/9077.pdf

8. Автоматизація та комп’ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції – Черкаси, 2024. – 384 с. – Режим доступу: https://conference.ikto.net/pub/akit_2024_11-17march_1.pdf

9. Як працює система контролю доступу (СКД або СКУД) [Електронний ресурс] – Режим доступу: https://u-prox.systems/yak-praczyuye-sistema-kontrolyu-dostupu-skd-abo-skud/

10. Системи контролю доступу: що це таке і як працює [Електронний ресурс] – Режим доступу: https://zakarpattya.net.ua/News/200909-Systemy-kontroliu-dostupu-shcho-tse-take-i-iak-pratsiuie

11. Захаров В.П Біометричні технології в XXI столітті та їх використання правоохоронними органами/ В.П Захаров, В.І. Рудешко– Львів 2015. – 492 с.

12. Технологічні тренди в контролі фізичного доступу: розвиток біометрії, штучного інтелекту та мобільних рішень [Електронний ресурс] – Режим доступу: https://greenvision.ua/ua/blog/tekhnolohichni-trendy-v-kontroli-fizychnoho-dostupu-rozvytok-biometriyi-shtuchnoho-intelektu-ta-mobilnykh-rishen

13. Biometric System Market [Електронний ресурс] – Режим доступу: https://www.globalgrowthinsights.com/market-reports/biometric-system-market-115022

14. Сучасні уявлення про біометрію, біометричні технології та біометричні характеристики. [Електронний ресурс] – Режим доступу: http://4ua.co.ua/pravo/kriminalistika/suchasni-uyavlennya-biometriyu-biometrichni-tehnologiyi-biometrichni-harakteristiki.html

15. Система контролю доступу (СКУД). Принцип дії, склад, особливості застосування. [Електронний ресурс] – Режим доступу: https://imperia.org.ua/article/sistema-kontrolyu-dostupu-skud-princip-dii-sklad-osoblivosti-zastosuvannya

16. Сканер відбитків пальців: як це працює? Який краще — ємнісний, оптичний чи ультразвуковий? [Електронний ресурс] – Режим доступу: https://ktc.ua/blog/skaner_vidbitkiv_palciv_yak_ce_pracyuye_yakij_krashhe__yemnisnij_optichnij_chi_ultrazvukovij_.html

17. Шабала Є.Є. Курс лекцій «Біометричні системи автентифікації» / Шабала Є.Є. – Київ 2024.

18. Сканер відбитка пальця R307 [Електронний ресурс] – Режим доступу: https://www.rajguruelectronics.com/Product/1276/R307%20Fingerprint%20Module.pdf

19. Сканер відбитка пальця оптичний AS608 [Електронний ресурс] – Режим доступу: https://radiostore.com.ua/ua/p2400596688-skaner-otpechatka-paltsa.html

20. Сканер відбитка пальця FPM10A [Електронний ресурс] – Режим доступу: https://robostore.com.ua/otladochnye-platy/esp-moduli/skaner-otpechatka-palca-fpm10a/?srsltid=AfmBOoqssQgM5g-GjgY29gTFCwCzbZksVqU2SrWF4tk6rQMudOcJBGEA

21. Ізмайлова О.В. Методичні вказівки до виконання циклу робіт «Метод аналізу ієрархії»/ О.В. Ізмайлова – Київ 2024. – 29 с.

22. Arduino UNO [Електронний ресурс] – Режим доступу: https://doc.arduino.ua/ru/hardware/Uno

23. Плата розробника ESP32 [Електронний ресурс] – Режим доступу: https://ardushop.in.ua/arduino/developer-board-esp-wroom-32-esp-32-wi-fi-bluetooth

24. Плата розробника STM32 [Електронний ресурс] – Режим доступу: https://arduino.ua/prod1328-plata-razrabotchika-stm32f103c8t6-arm-stm32-minimalnaya-konfigyraciya

25. Arduino UNO - популярна плата розробки [Електронний ресурс] – Режим доступу: https://itmaster.biz.ua/directory/kits-nabory/arduino-uno.html

26. Транзистор IRFZ44N [Електронний ресурс] – Режим доступу: https://myproject.com.ua/tranzystor-irfz44n-korpus-to-220.html

27. Соленоїд 12 v [Електронний ресурс] – Режим доступу: https://arduino-kit.com.ua/solenojd-solenoid-12v.html

28. Блок живлення 12v [Електронний ресурс] – Режим доступу: https://led-svit.com.ua/blok-zhivlennya-12v-1a-12w-plastikoviy/

29. Офіційний сайт Fritzing [Електронний ресурс] – Режим доступу: https://fritzing.org/

30. Офіційний сайт Arduino [Електронний ресурс] – Режим доступу: https://www.arduino.cc/en/software/

31. Бібліотека датчиків відбитків пальців Adafruit [Електронний ресурс] – Режим доступу: https://github.com/adafruit/Adafruit-Fingerprint-Sensor-Library

32. Вартість готового комерційного рішення СКУД [Електронний ресурс] – Режим доступу: https://rozetka.com.ua/ua/332092174/p332092174/

33. Піддубний Д.А. Проблема надійності та безпеки систем контролю доступу на основі біометрії / Д.А. Піддубний, О.В. Ізмайлова // «БУД-МАЙСТЕР-КЛАС-2025». – Київ 2025.

34. Піддубний Д.А. Аналіз сучасного шкідливого програмного забезпечення та методи боротьби з ним / Д.А. Піддубний, Є.Є. Шабала // «БУД-МАЙСТЕР-КЛАС-2024». – Київ 2024. – 465 с.

35. Conrad, J. Exploring Arduino: Tools and Techniques for Engineering Wizardry. – Hoboken: Wiley, 2013. – 400 p.

36. Monk, S. Programming Arduino: Getting Started with Sketches. – New York: McGraw-Hill Education, 2020. – 208 p.

37. Dubois, J-M. C Programming for Arduino. – Birmingham: Packt Publishing, 2012. – 512 p.

38. Monk, S. Fritzing for Inventors: Take Your Electronics Project from Prototype to Product. – New York: McGraw-Hill, 2015. – 240 с.

39. Ізмайлова О.В. Методичні рекомендації до виконання та оформлення атестаційної випускної роботи на здобуття освітнього ступеня магістра зі спеціальності 123 «Комп’ютерна інженерія» та 125 «Кібербезпека та захист інформації». – Київ 2019.

40. Паспорт кваліфікаційної роботи здобувачів другого (магістерського) рівня вищої освіти спеціальності 125 «Кібербезпека та захист інформації» за освітньою програмою «Безпека інформаційних і комунікаційних систем»

41. Положення про кваліфікаційну роботу здобувачів вищої освіти Київського національного університету будівництва і архітектури Київ 2024

ДОДАТОК А

Програмний код 1

```
#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("Реєстрація датчика відбитків пальців");

  // встановити швидкість передачі даних для послідовного порту датчика
  finger.begin(57600);

  if (finger.verifyPassword()) {
    Serial.println("Знайдено датчик відбитків пальців");
  } else {
    Serial.println("Незнайдено датчик відбитків пальців :(");
    while (1) { delay(1); }
  }
}

uint8_t readnumber(void) {
  uint8_t num = 0;

  while (num == 0) {
    while (! Serial.available());
    num = Serial.parseInt();
  }
  return num;
}

void loop()
{
  Serial.println("Готовність до реєстрації відбиткі пальця");
```

```
  Serial.println("Будь ласка, введіть ідентифікатор № (від 1 до 127), під яким ви
хочете зберегти цей палець");
  id = readnumber();
  if (id == 0) {// № 0 не дозволено, спробйте ще раз
     return;
  }
  Serial.print("Ідентифікатор реєстрації №");
  Serial.println(id);

  while (!  getFingerprintEnroll() );
}

uint8_t getFingerprintEnroll() {

  int p = -1;
  Serial.print("Очікування реєстрації відбитка №"); Serial.println(id);
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Зображення зроблено");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.println(".");
      break;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Помилка зв'язку");
      break;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Помилка зображення");
      break;
    default:
      Serial.println("Невідома помилка");
      break;
    }
  }


  p = finger.image2Tz(1);
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Зображення перетворене");
      break;
    case FINGERPRINT_IMAGEMESS:
```

```
    Serial.println("Зображення низької якості");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Помилка зв'язку");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Невдалось знайти відбитки пальців");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Невдалось знайти відбитки пальців");
    return p;
  default:
    Serial.println("Невідома помилка");
    return p;
}

Serial.println("");
delay(2000);
p = 0;
while (p != FINGERPRINT_NOFINGER) {
  p = finger.getImage();
}
Serial.print("№"); Serial.println(id);
p = -1;
Serial.println("Прикладіть той самий палець знову");
while (p != FINGERPRINT_OK) {
  p = finger.getImage();
  switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Зображення зроблено");
    break;
  case FINGERPRINT_NOFINGER:
    Serial.print(".");
    break;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Помилка зв'язку");
    break;
  case FINGERPRINT_IMAGEFAIL:
    Serial.println("Помилка зображення");
    break;
  default:
    Serial.println("Невідома помилка");
    break;
  }
```

```
}


p = finger.image2Tz(2);
switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Зображення перетворено");
    break;
  case FINGERPRINT_IMAGEMESS:
    Serial.println("Зображення низької якості");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Помилка зв'язку");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Невдалось знайти відбитки пальців");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Невдалось знайти відбитки пальців");
    return p;
  default:
    Serial.println("Невідома помилка");
    return p;
}


Serial.print("Створення шаблону для №");  Serial.println(id);

p = finger.createModel();
if (p == FINGERPRINT_OK) {
  Serial.println("Відбитки збігаються");
} else if (p == FINGERPRINT_PACKETRECIEVEERR) {
  Serial.println("Помилка зв'язку");
  return p;
} else if (p == FINGERPRINT_ENROLLMISMATCH) {
  Serial.println("Відбитки пальців не збігаються");
  return p;
} else {
  Serial.println("Невідома помилка");
  return p;
}

Serial.print("№"); Serial.println(id);
p = finger.storeModel(id);
```

```
  if (p == FINGERPRINT_OK) {
    Serial.println("Збережено");
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Помилка зв'язку");
    return p;
  } else if (p == FINGERPRINT_BADLOCATION) {
    Serial.println("Невділось зберегти в цьому місці");
    return p;
  } else if (p == FINGERPRINT_FLASHERR) {
    Serial.println("Помилка запису на флеш-пам'ять");
    return p;
  } else {
    Serial.println("Невідома помилка");
    return p;
  }
}
```

ДОДАТОК Б

Програмний код 2

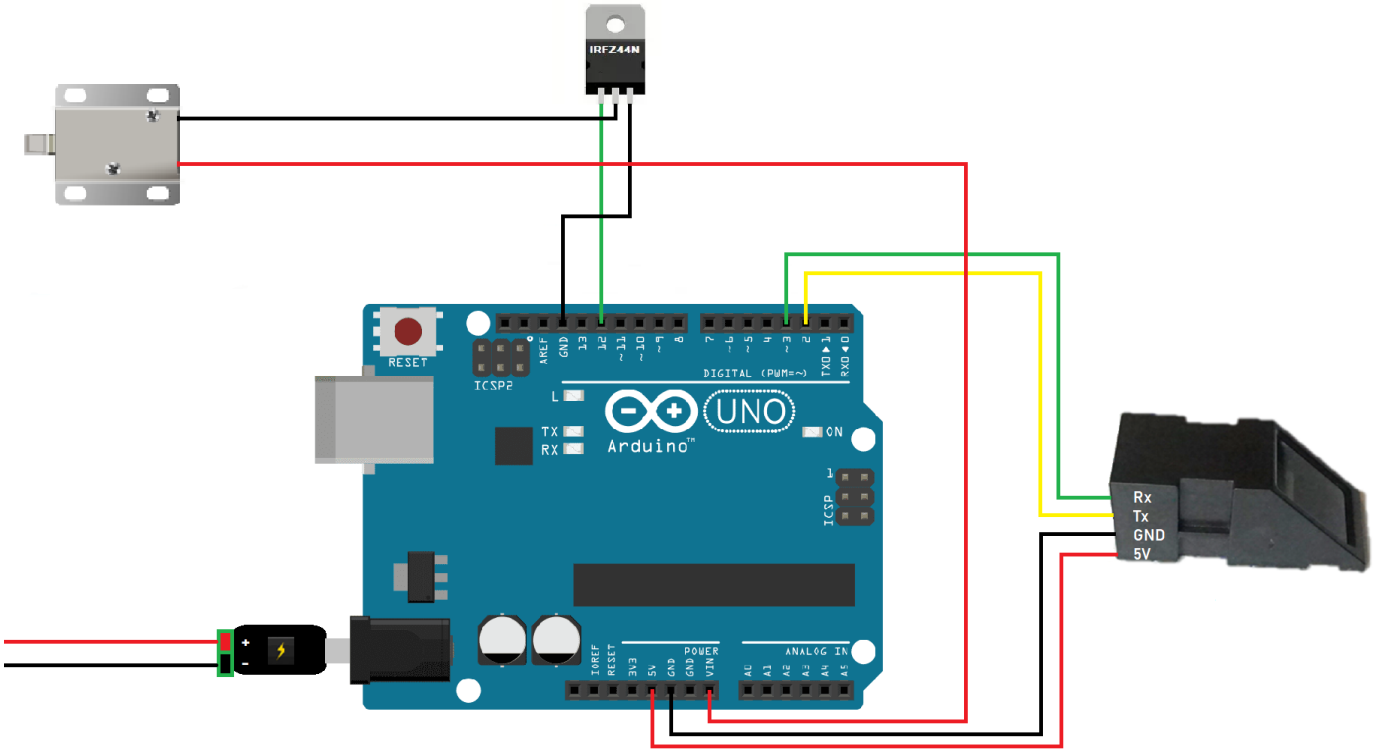
```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>

SoftwareSerial mySerial(2, 3);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup()
{
  Serial.begin(9600);
  while (!Serial);
  delay(100);
  Serial.println("Тест відбитком");
  pinMode(12, OUTPUT);


  finger.begin(57600);

  if (finger.verifyPassword()) {
    Serial.println("Знайдено датчик відбитків пальців");
  } else {
    Serial.println("Незнайдено датчик відбитків пальців(");
    while (1) { delay(1); }
  }

  finger.getTemplateCount();
  Serial.print("Датчик містить"); Serial.print(finger.templateCount);
Serial.println("шаблони");
  Serial.println("Очікування відбитка пальця");
}

void loop()

{
  getFingerprintIDez();
  delay(50);
  digitalWrite(12, LOW);
}

uint8_t getFingerprintID() {
```

```
uint8_t p = finger.getImage();
switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Зображення зроблено");
    break;
  case FINGERPRINT_NOFINGER:
    Serial.println("Палець не виявлено");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Помилка зв'язку");
    return p;
  case FINGERPRINT_IMAGEFAIL:
    Serial.println("Помилка зображення");
    return p;
  default:
    Serial.println("Невідома помилка");
    return p;
}


p = finger.image2Tz();
switch (p) {
  case FINGERPRINT_OK:
    Serial.println("Зображення перетворено");
    break;
  case FINGERPRINT_IMAGEMESS:
    Serial.println("Зображення низької якості");
    return p;
  case FINGERPRINT_PACKETRECIEVEERR:
    Serial.println("Помилка зв'язку");
    return p;
  case FINGERPRINT_FEATUREFAIL:
    Serial.println("Невдалось знайти відбиток пальця");
    return p;
  case FINGERPRINT_INVALIDIMAGE:
    Serial.println("Невдалось знайти відбиток пальця");
    return p;
  default:
    Serial.println("Невідома помилка");
    return p;
}

p = finger.fingerFastSearch();
if (p == FINGERPRINT_OK) {
```

```
    Serial.println("Знайдено збіг відбитків");
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Помилка зв'язку");
    return p;
  } else if (p == FINGERPRINT_NOTFOUND) {
    Serial.println("Незнайдено відповідності");
    return p;
  } else {
    Serial.println("Невідома помилка");
    return p;
  }


  Serial.print("Знайдено ідентифікатор №"); Serial.print(finger.fingerID);
  Serial.print(" з упевненістю "); Serial.println(finger.confidence);

  return finger.fingerID;
}


int getFingerprintIDez() {
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK)  return -1;

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

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

  digitalWrite(12, HIGH);
  delay(3000);
  digitalWrite(12, LOW);

  Serial.print("Знайдено ідентифікатор №"); Serial.print(finger.fingerID);
  Serial.print("  з упевненістю "); Serial.println(finger.confidence);
  return finger.fingerID;
}
```

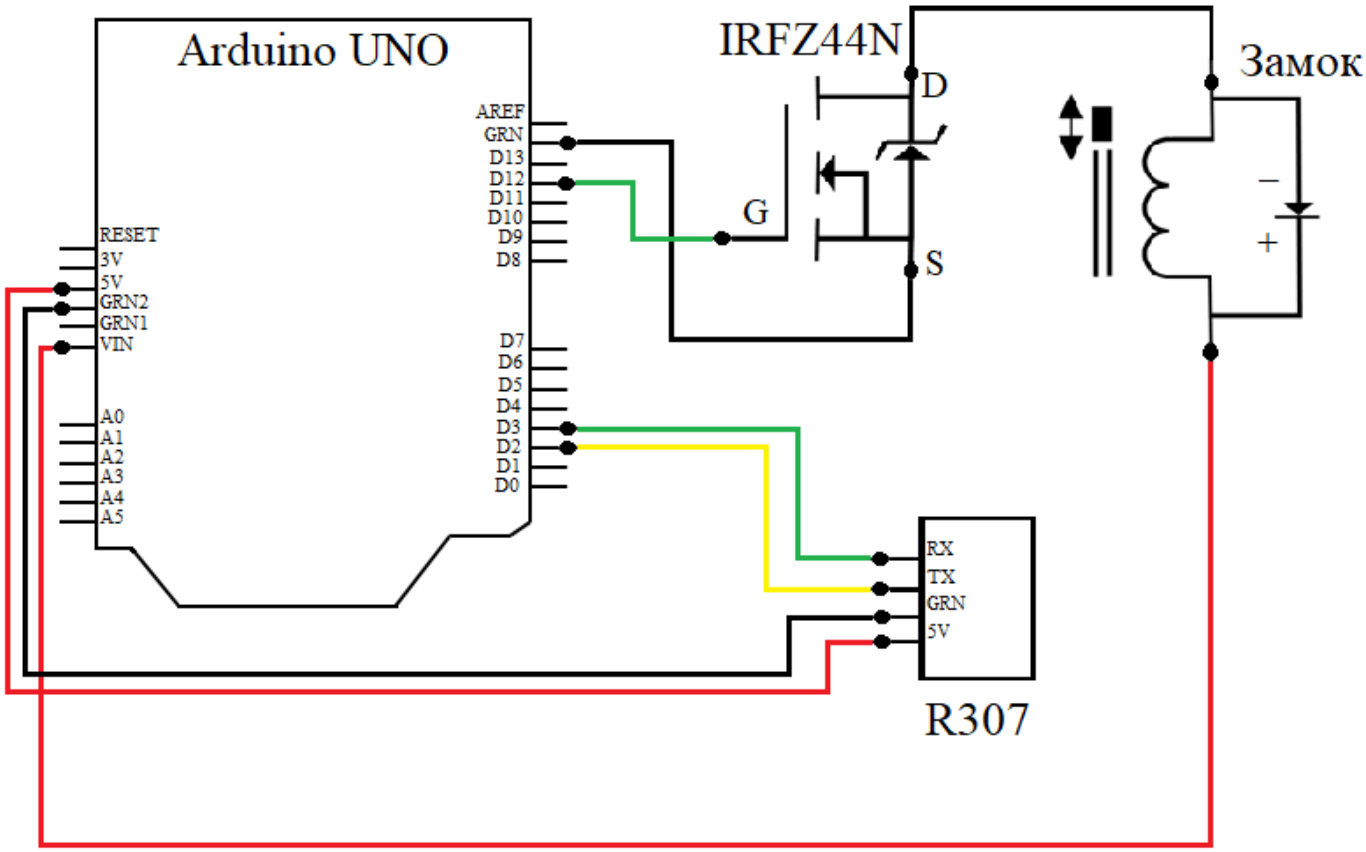
ДОДАТОК В

Схема електрична монтажна



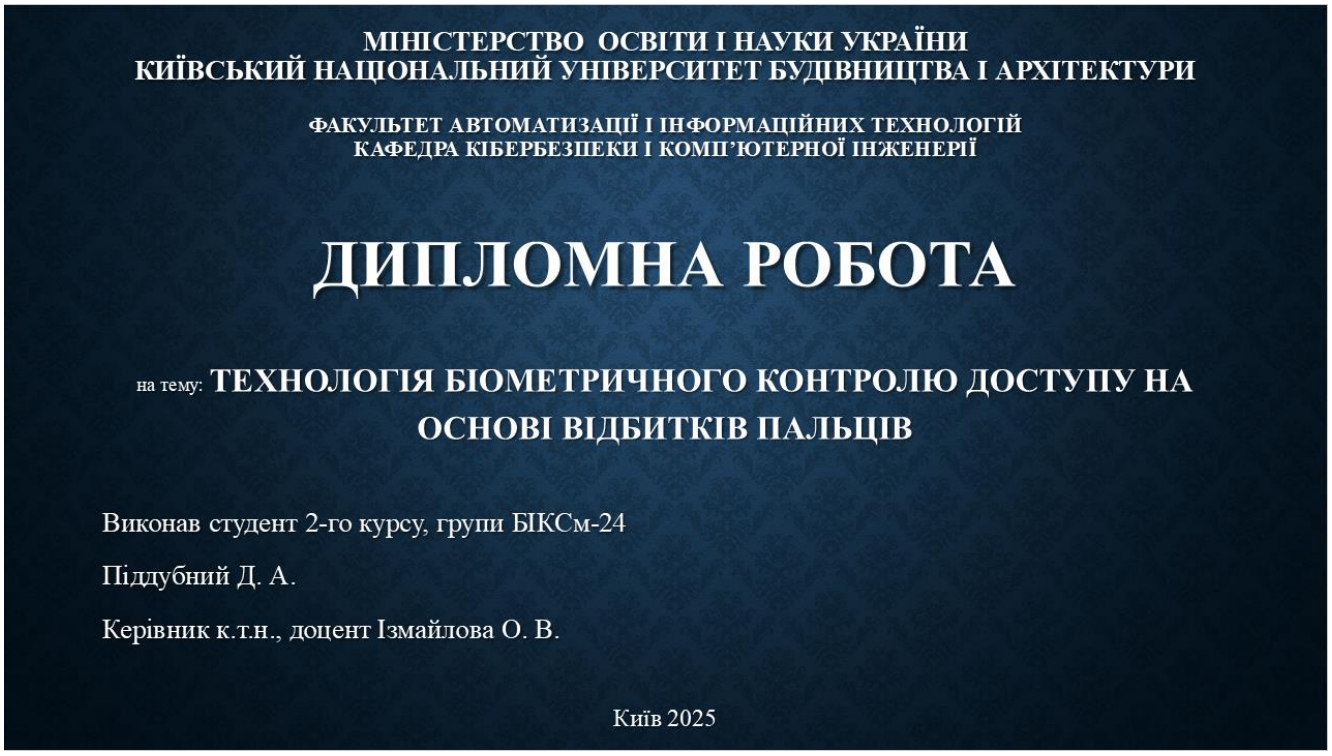
ДОДАТОК Г

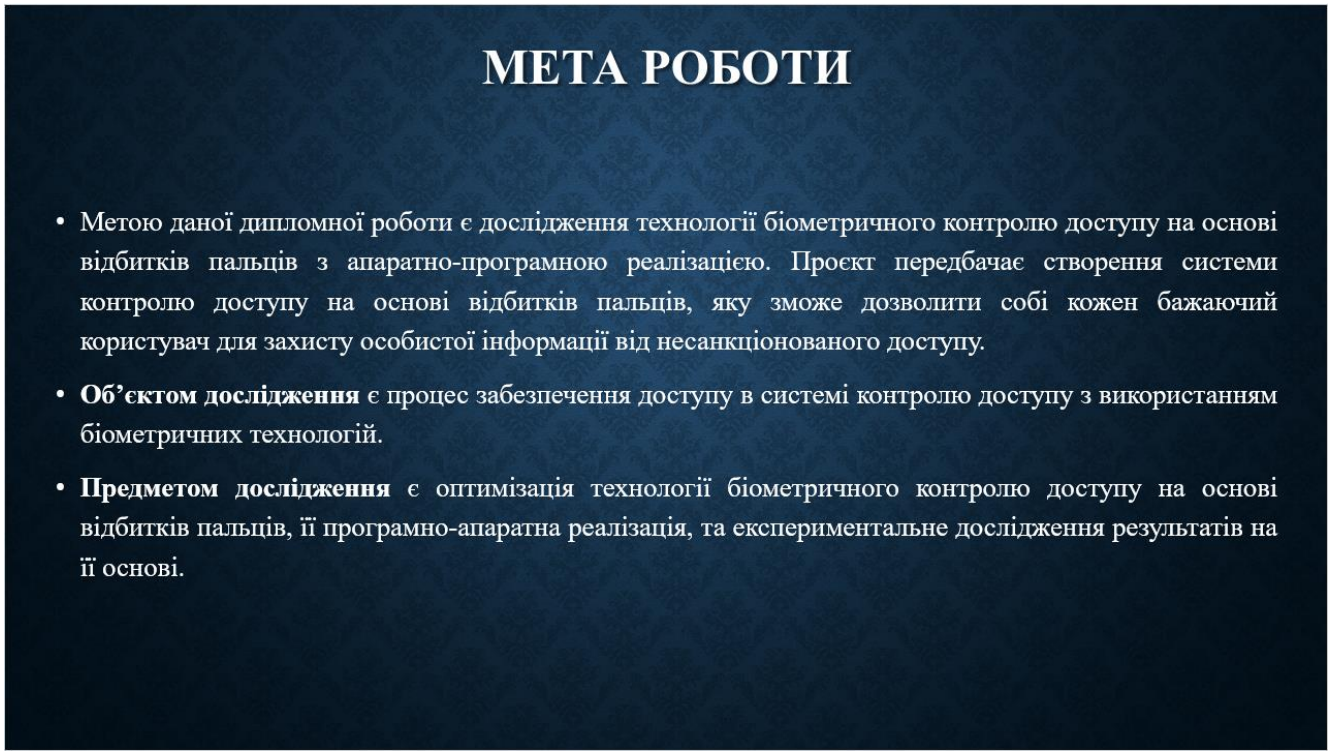
Схема електрична принципова



ДОДАТОК Ґ

Інформаційні слайди



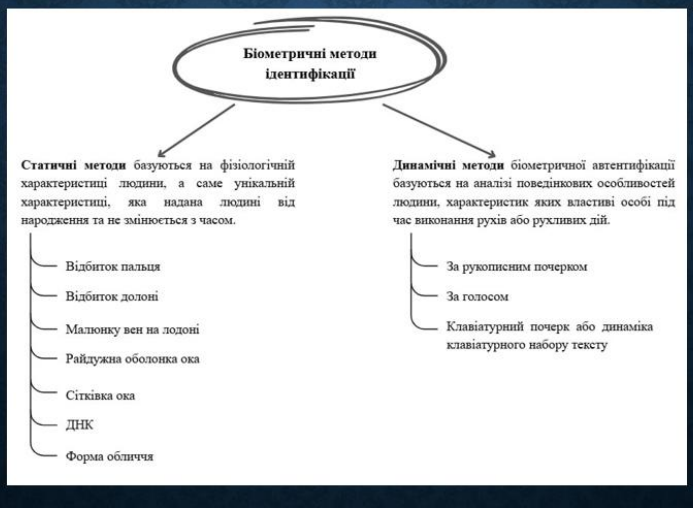


АКТУАЛЬНІСТЬ РОБОТИ

Зростання кількості інформаційних та фізичних загроз вимагає впровадження більш надійних засобів контролю доступу. Традиційні методи ідентифікації, такі як ключі, картки чи паролі, залишаються вразливими до підробки, втрати або несанкціонованого використання. Біометричні технології, зокрема розпізнавання за відбитком пальця, забезпечують високий рівень точності, унікальність та неможливість передачі ідентифікатора іншій особі. Це робить їх актуальним та перспективним рішенням для підвищення безпеки в різних сферах.

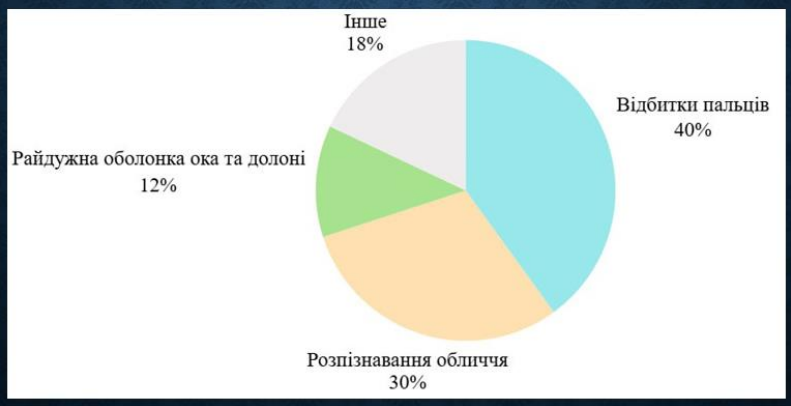
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Система контролю і управління доступом (СКУД або СКД) – це сукупність програмних та апаратних засобів безпеки, що регулюють вхід/вихід людей та забезпечує регулювання прав доступу до ресурсів, приміщень або інформаційних систем.



АНАЛІТИКА ВИКОРИСТАННЯ БІОМЕТРИЧНИХ МЕТОДІВ НА РИНКУ УКРАЇНИ

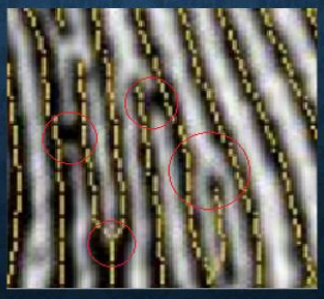
- Згідно зі звітом про стан контролю доступу кількість підприємств, що використовують біометричні дані, продовжує зростати. Якщо два роки тому біометрія використовувалася лише на 30% підприємств, то сьогодні цей показник сягає 39%.
- Світові ж дослідження вказують відсоткові співвідношення застосування різних біометричних методів, де домінує переважно метод відбитків пальців.



ВИДИ ПАПІЛЯРНИХ УЗОРІВ ТА ЇХ ОЗНАКИ

Класифікація папілярних узорів

Глобальні ознаки відбитків



Локальні ознаки відбитків

АНАЛІЗ ВЛАСНОГО ВІДБИТКУ ПАЛЬЦЯ

Власний відбиток

Глобальні ознаки відбитка

Звичайна петля

Змішана ознака

Локальні ознаки відбитка

МЕТОДИ ЗНЯТТЯ ВІДБИТКІВ ПАЛЬЦІВ

Оптичний метод — це спосіб зчитування відбитка пальця через освітлення пальця та фіксацію відбитого світла світлочутливою матрицею.

Ультразвуковий метод — це технологія, яка створює 3D-зображення відбитка за допомогою ультразвукових хвиль, що відбиваються від виступів і заглиблень шкіри.

Методи зняття відбитків пальців

Ємнісний метод — це спосіб зчитування, який визначає відбиток через зміни електричного поля на поверхні сканера при торканні пальцем.

ПОРІВНЯННЯ МЕТОДІВ ЗНЯТТЯ ВІДБИТКІВ

Критерії	Ємнісний	Оптичний	Ультразвуковий
Якість зображення	Середня	Висока	Дуже висока
Вартість	Низька-середня	Середня-висока	Висока
Швидкість сканування	Висока	Висока	Середня-низька
Стійкість сканування до забруднень та вологи	Низька	Середня	Висока
Вразливість до підробок	Висока	Середня	Низька
Чутливість до надлишкової енергії	Висока	Низька	Низька
Довговічність	Низька	Висока	Висока
Переваги	Дешеві; прості у використанні	Є балансом між якістю, надійністю та ціною	Підвищена стійкість, гарний варіант для об'єктів з високими вимогами захисту
Недоліки	Чутливі до надлишкової енергії; легко обманюються; не довговічні	Піддаються спуфінгу; часто відбитки залишаються на поверхні сканера	Дорогі; повільні сканування; важкі в інтегруванні в прототипи
Сфери застосування	Бюджетні СКД; смартфони бюджетного сегменту	Офісні та приватні СКД	Об'єкти з високими вимогами безпеки: банківські установи, преміальні СКД

МАІ ПОРІВНЯННЯ ОПТИЧНИХ СКАНЕРІВ ВІДБИТКІВ ПАЛЬЦЯ

	Моделі оптичних сканерів		
Параметри	R307	AS608	FPM10A
Тип сенсора	Оптичний	Оптичний	Оптичний
Інтерфейс	UART (TTL), USB	UART (TTL), USB	UART (TTL)
Об'єм відбитків	~1000 відбитків	~300 відбитків	~300 відбитків
Роздільна здатність	500dpi	500dpi	500dpi
Швидкість розпізнавання	<1 секунда	<1 секунда	~1 секунда
Швидкість реєстрації	1-2 секунди	1-2 секунди	2-3 секунди
BFAR (False Acceptance Rate)	~0,001%	~0,001%	~0,001%
FRR (False Rejection Rate)	~1%	~1-2%	~2%
Рівень надійність	Високий	Середній	Середній
Вартість	Середня	Низька	Низька-середня
Ресурс сенсора	>1 млн дотиків	~500 тис. дотиків	~500 тис. дотиків
Метод збереження даних	Внутрішня пам'ять	Внутрішня пам'ять	Внутрішня пам'ять

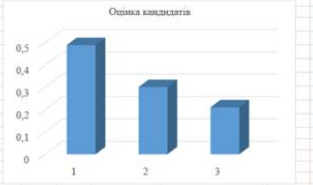
Порівняння оптичних сканерів

	FAR	FFR	ЦІНА	НАДІЙНІСТЬ	МАСШТАБОВАНІСТЬ	Добуток	Вектор	Вага
FAR	1	1	3	5	7	105	2,5365	0,3638
FFR	1	1	3	5	7	105	2,5365	0,3638
ЦІНА	0,333333333	0,3333	1	3	5	1,666667	1,1076	0,1588
НАДІЙНІСТЬ	0,2	0,2	0,3333	1	3	0,04	0,5253	0,0753
МАСШТАБОВАНІСТЬ	0,142857143	0,1429	0,2	0,333333333	1	0,001361	0,2671	0,0383
							6,973	1

	n	1
	N*FAR	5,0827
	N*FFR	5,0827
	N*ЦІНА	5,1556
	N*НАДІЙНІСТЬ	5,1599
	N*МАСШТАБОВАНІСТЬ	5,1975
	n*	5,1357
	H	0,0339
	RH	1,188
	HR	0,0286

Матриця парних порівнянь критеріїв

Узагальнююча оцінка кандидатів						
	FAR	FFR	ЦІНА	НАДІЙНІСТЬ	МАШТАБОВАНІСТЬ	Vi
R307	0,33333	0,7396	0,1047	0,714285714	0,730644671	0,48872
AS608	0,33333	0,1666	0,637	0,142857143	0,188394097	0,30101
FPM10A	0,33333	0,0938	0,2583	0,142857143	0,080961232	0,21027
Вага крит.	0,36376	0,3638	0,1588	0,075333696	0,038310676	1



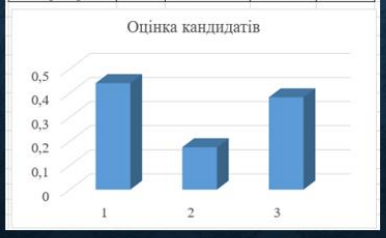
Оцінка кандидатів

МАІ ПОРІВНЯННЯ ПЛАТ КЕРУВАННЯ

	Моделі плат керування		
Параметри	Arduino UNO	ESP32	STM32
Мікроконтролер	ATmega328P	Xtensa LX6	ARM Cortex-M3
Тактова частота	16 МГц	240 МГц	72 МГц
RAM-пам'ять	2 КБ	520 КБ	20 КБ
Flash-пам'ять	32 КБ	4 МБ	від 64 КБ
Робоча напруга	5 В	5 В	3,3 В
Кількість портів	14 цифрових, 6 аналогових	~ 34, залежить від моделі	~ 37, залежить від моделі
Інтерфейси	UART, I2C, SPI	UART, I2C, SPI, CAN, Wi-Fi, Bluetooth	UART, I2C, SPI, CAN, USB
Вартість	Середня	Висока-середня	Середня

Порівняння плат керування

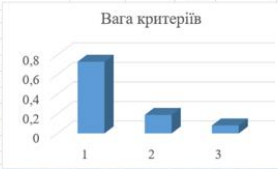
Узагальнююча оцінка кандидатів				
	ЦІНА	ПІДТРИМКА	ПАМ'ЯТЬ	Vi
UNO	0,4286	0,636985572	0,104729	0,44162
ESP32	0,1429	0,104729434	0,636986	0,17568
STM32	0,4286	0,258284994	0,258285	0,3827
Вага критеріїв	0,7306	0,188394097	0,080961	1



Оцінка кандидатів

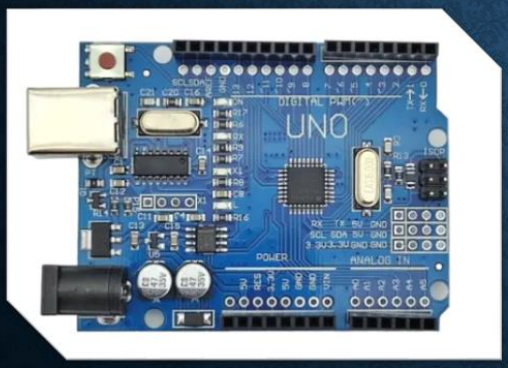
ЦІНА - ПІДТРИМКА ТА НАЛАШТУВАННЯ - ПАМ'ЯТЬ						
	ЦІНА	ПІДТРИМКА	ПАМ'ЯТЬ	Добуток	Вектор	Вага
ЦІНА	1	5	7	35	3,2711	0,7306447
ПІДТРИМКА	0,2	1	3	0,6	0,8434	0,1883941
ПАМ'ЯТЬ	0,1429	0,333333333	1	0,04762	0,3625	0,0809612
					4,477	1

n	3
N*ЦІНА	3,0649
N*ПІДТРИМКА	3,0649
N*ПАМ'ЯТЬ	3,0649
n*	3,0649
H	0,0324
RH	0,66
HR	0,0492



Матриця парних порівнянь критеріїв

КОМПОНЕНТИ СИСТЕМИ

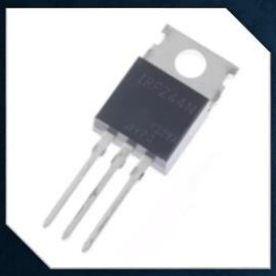


- **Arduino Uno** – центральний елемент системи, що забезпечує обробку даних та керування її роботою. Характеризується простотою використання, надійністю та достатньою продуктивністю для реалізації алгоритмів біометричної ідентифікації.

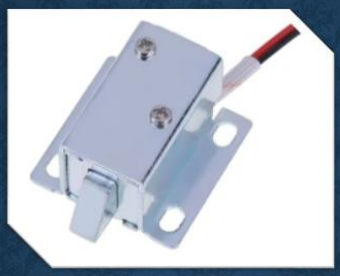
КОМПОНЕНТИ СИСТЕМИ

- **Сканер відбитків пальців R307** – апаратний модуль для зчитування та первинної обробки біометричних даних, який використовується для ідентифікації користувачів у системі контролю доступу.

КОМПОНЕНТИ СИСТЕМИ



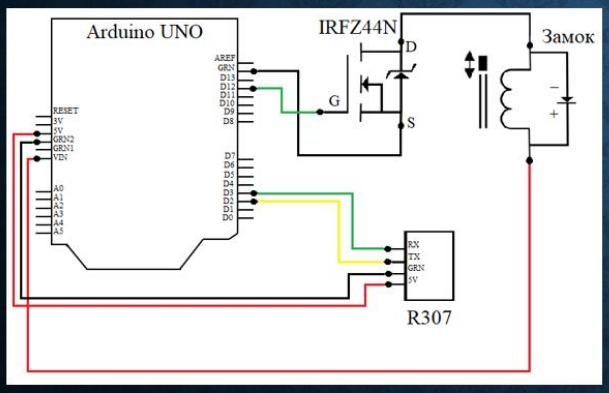
- **Транзистор IRFZ44N** – силовий транзистор, що використовується для керування електронним замком системи контролю доступу.



- **Електромеханічний замок** – виконавчий елемент системи, що забезпечує фізичне блокування або розблокування доступу відповідно до результату біометричної ідентифікації.

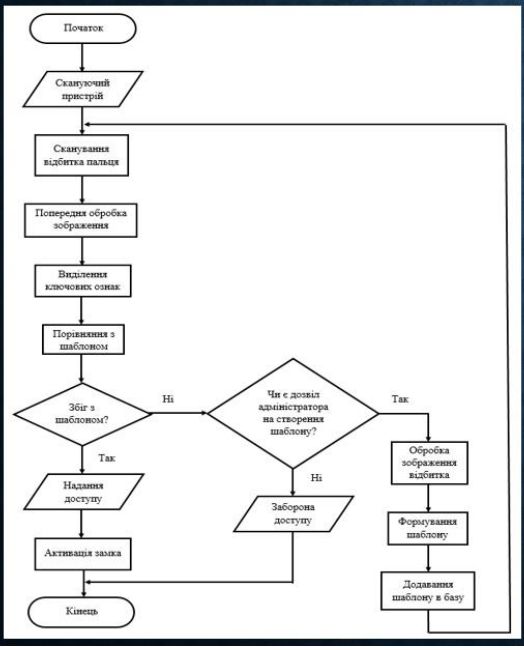
- **Блок живлення** – елемент системи, що забезпечує стабільне електроживлення всіх апаратних компонентів та надійну роботу системи в цілому.

ПРИНЦИПОВА ЕЛЕКТРИЧНА СХЕМА



- Принципова електрична схема відображає взаємодію та з'єднання всіх компонентів системи;
- Мікроконтролер забезпечує обробку сигналів та керування роботою системи;
- Сканер відбитків пальців підключений до мікроконтролера та передає біометричні дані;
- Керування електромеханічним замком здійснюється через силовий елемент.

АЛГОРИТМ РОБОТИ



Робота системи починається з подачі на неї живлення.

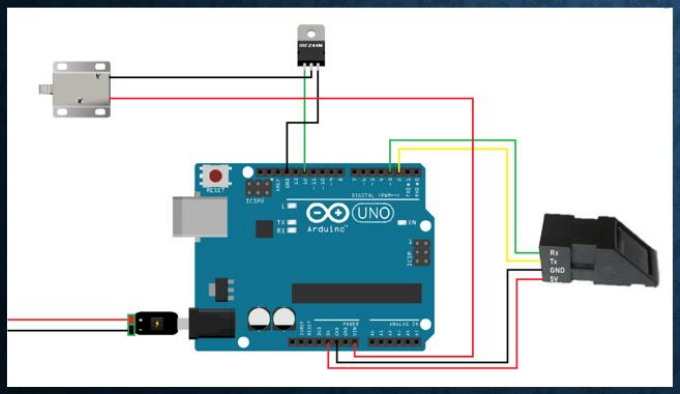
Скануючий пристрій очікує відбиток пальця. Коли користувач прикладе палець до сканера відбувається **сканування відбитка**. Отримане зображення відбитка проходить **попередню обробку**, **виділення ключових ознак** та **порівняння з збереженим шаблоном** в пам'яті.

На основі результатів порівняння з шаблоном відбувається перевірка – **збіг з шаблоном**, в якої є два результати:

- **Результат «Так»** – якщо відбиток співпадає з шаблоном система приймає рішення про надання доступу.
- **Результат «Ні»** – якщо відбиток не співпадає з збереженим шаблоном, тоді система чекає **дозвіл адміністратора на створення шаблону**, якщо **адміністратор надає відповідь «Ні»** – система забороняє доступ. Якщо **відповідь адміністратора «Так»** – тоді відбувається **обробка зображення відбитка**, **формування шаблону**, та **додавання отриманого шаблону до пам'яті пристрою**.

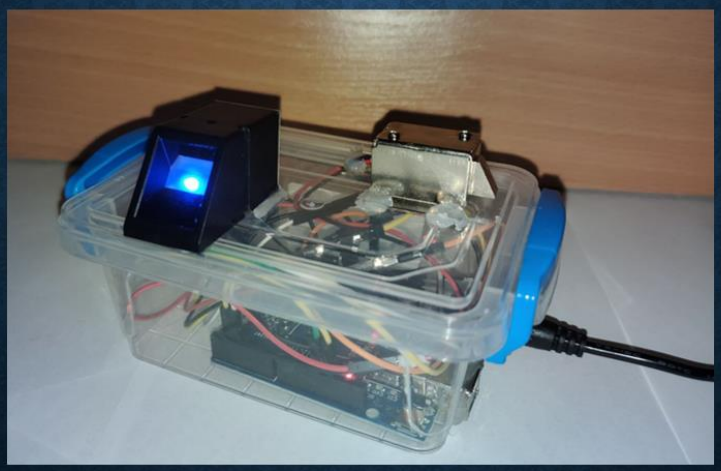
Після завершення циклу перевірки система повертається у стан очікування наступного користувача.

ЗБІРКА ПРОТОТИПУ СИСТЕМИ



- Збірка прототипу проводилась згідно монтажній схемі.
- Монтажна електрична схема відображає фізичне підключення всіх компонентів системи.

ЗІБРАНИЙ ПРОТОТИП СИСТЕМИ



ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

- **Програмне забезпечення для пристрою розроблене мовою C/C++ в середовищі Arduino IDE**
- **Реалізує алгоритм біометричної ідентифікації користувачів**
- **Забезпечує обробку даних зі сканера відбитків пальців**
- **Виконує порівняння збережених біометричних шаблонів**
- **Керує роботою виконавчого механізму відповідно до результату ідентифікації**

ТЕСТУВАННЯ ПРОТОТИПУ

Критерії	Кількість успішних ідентифікацій		
	1 користувач	2 користувач	3 користувач
10 разів піднести палець	10	10	10
10 разів піднести палець при повороті	10	10	10
10 разів піднести палець з різною силою натиску	10	10	10
Середній час ідентифікації	до 1 секунди	до 1 секунди	до 1 секунди

Рівень правильного прийняття (TAR)

Критерії	Кількість успішних ідентифікацій		
	1 користувач	2 користувач	3 користувач
10 разів коли шкіра волога	10	9	10
10 разів з дуже швидким прикладанням пальця	9	8	8

Рівень помилкових відмов (FRR)

Критерії	Кількість успішних ідентифікацій	
	Незареєстрований користувач 1	Незареєстрований користувач 2
10 спроб доступу з різних положень пальця	0	0

Рівень помилкових прийняття (FAR)

Показник	Результат	Статус
TAR	100%/ 100% /100%	Коректний
FRR	0,05/ 0,15/ 0,10	Коректний
FAR	0/0	Коректний

Результати тестування

ВИСНОВКИ

В роботі проведено дослідження та апаратно-програмно реалізацію технології біометричного контролю доступу на основі відбитків пальців.

- Проаналізовано системи контролю доступу;
- Розглянуто методи біометричної ідентифікації людини;
- Охарактеризовано види відбитків пальців, методи їх зняття, глобальні та локальні ознаки відбитків, проведено аналіз власного відбитку пальця;
- Здійснено вибір ключових елементів системи за допомогою МАІ;
- Розроблено структуру та алгоритм роботи системи;
- Реалізовано апаратно-програмний прототип системи;
- Проведено тестування, яку підтвердило працездатність та надійність системи.

Отримані результати підтверджують можливість створення бюджетної, ефективної та масштабованої біометричної СКД на основі відбитків пальців. Отриманий прототип може слугувати основою для вдосконалення та розширення.

ПУБЛІКАЦІЇ

В рамках наукових конференцій мною було представлено наступні наукові роботи:

- Теза «Аналіз сучасного шкідливого програмного забезпечення та методи боротьби з ним» – «БУД-МАЙСТЕР-КЛАС-2024»;
- Теза «Проблеми надійності та безпеки системи контролю доступу на основі біометрії» – «БУД-МАЙСТЕР-КЛАС-2025».

BUILD MASTER CLASS
International Conference

ДЯКУЮ ЗА УВАГУ!