Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

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

Кафедра комп'ютерної інженерії та безпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «МАГІСТР»

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ДОСТУПУ З БАГАТОРІВНЕВОЮ БІОМЕТРИЧНОЮ ІДЕНТИФІКАЦІЄЮ КОРИСТУВАЧІВ НА RASPBERRY PI

INTELLIGENT ACCESS SYSTEM WITH MULTI-LEVEL BIOMETRIC USER IDENTIFICATION ON RASPBERRY PI

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

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІм-21
Будко Денис Сергійович

(підпис)

Керівник:
к.т.н., доцент
Костючко Сергій Миколайович

(підпис)

Кваліфікаційну роботу
допущено до захисту
« _____» грудня _____ 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Гринюк Сергій Васильович

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *магістр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т.ТЕРЛЕЦЬКИЙ
«_____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Будко Денис Сергійович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Інтелектуальна система доступу з багаторівневою біометричною ідентифікацією користувачів на Raspberry Pi*

Керівник роботи *к.т.н., доцент Костючко Сергій Миколайович*

затверджені наказом закладу вищої освіти від «17» червня 2025 року № 290/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 09.12.2025р.

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

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Теоретичні основи систем біометричної ідентифікації та контролю доступу
Розробка інтелектуальної системи доступу
Реалізація та дослідження роботи системи багаторівневої аутентифікації
Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз проблеми за темою роботи та постановка завдань дослідження	*Костючко С.М., доцент*		
Теоретичне дослідження та практична реалізація	*Костючко С.М., доцент*		
Практична реалізація об'єкта проектування	*Костючко С.М., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Гринюк С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І., ст.викладач*		

7. Дата видачі завдання 18.06.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Огляд літератури із досліджуваної проблеми*	До 01.08.2025 р.	
2.	*Аналіз загальної проблеми і вибір напрямків дослідження*	До 20.08.2025 р.	
3.	*Розробка функціональної схему роботи програмно-апаратного продукту*	До 25.09.2025 р.	
4.	*Практична реалізація та дослідження роботи об'єкта проектування*	До 20.10.2025 р.	
5.	*Висновки та пропозиції*	До 25.10.2025 р	
6.	*Формування списку використаних джерел*	До 27.10.2025 р.	
7.	*Формування додатків*	До 30.10.2025 р.	
8.	*Оформлення ілюстративного матеріалу*	До 05.11.2025 р.	
9.	*Представлення остаточного варіанту кваліфікаційної роботи керівникові*	До 11.11.2025 р.	
10.	*Нормоконтроль*	До 29.11.2025 р.	
11.	*Інструментальна перевірка на академічний плагіат*	До 02.12.2025 р.	
12.	*Здача кваліфікаційної роботи та всіх супровідних документів на кафедру*	До 09.12.2025 р.	

Здобувач вищої освіти _____ Будко Д.С.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Костючко С.М
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Будко Д. С. Інтелектуальна система доступу з багаторівневою біометричною ідентифікацією користувачів на Raspberry Pi.

Кваліфікаційна робота магістра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота магістра складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Робота присвячена розробці та практичній реалізації інтелектуальної системи контролю доступу з використанням біометричних технологій та апаратної платформи Raspberry Pi.

У першому розділі проведено аналіз інтелектуальних систем доступу. Розглянуто принципи побудови багаторівневих систем аутентифікації та можливості застосування одноплатних комп'ютерів у сфері безпеки.

У другому розділі здійснено вибір апаратних та програмних засобів для побудови системи. Побудовано архітектуру системи багаторівневої аутентифікації та описано алгоритм взаємодії апаратних і програмних модулів.

Третій розділ присвячено практичній реалізації розробленої системи. Проведено тестування точності та швидкодії системи при різних сценаріях аутентифікації. Наведено результати досліджень та виконано оцінку ефективності.

Ключові слова: біометрія, Raspberry Pi, розпізнавання обличчя, відбиток пальця, ESP32-CAM, R307, PIN-код, система контролю доступу, багаторівнева аунтефікація.

ANNOTATION

Budko D. Intelligent Access System with Multi-Level Biometric User Identification on Raspberry Pi

Qualifying work of a Master's of EP «Computer Engineering» specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The master's qualification work consists of an introduction, three sections, conclusions, a list of sources used and appendices. The work is devoted to the development and practical implementation of an intelligent access control system using biometric technologies and the Raspberry Pi hardware platform.

The first section analyzes intelligent access systems. The principles of building multi-level authentication systems and the possibilities of using single-board computers in the security sector are considered.

The second section selects hardware and software tools for building the system. The architecture of the multi-level authentication system is built and the algorithm for interaction of hardware and software modules is described.

The third section is devoted to the practical implementation of the developed system. The accuracy and speed of the system are tested in various authentication scenarios. The research results are presented and the effectiveness is assessed.

Keywords: biometrics, Raspberry Pi, face recognition, fingerprint, ESP32-CAM, R307, PIN code, access control system, multi-level authentication.

ЗМІСТ

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій зростає потреба у впровадженні інтелектуальних систем безпеки, здатних забезпечувати надійний контроль доступу до приміщень, інформаційних ресурсів чи обладнання. Класичні методи аутентифікації такі як ключі або паролі уже не гарантують достатнього рівня захисту, адже вони можуть бути втрачені, підроблені або передані третім особам. Саме тому все більшої популярності набувають багаторівневі системи, що поєднують кілька незалежних методів ідентифікації, зокрема біометричні.

Сучасні одноплатні комп’ютери такі як Raspberry Pi у поєднанні з модулями біометричного сканування та камерами дозволяють створювати компактні доступні та високофункціональні системи контролю доступу. Завдяки своїй гнучкості й можливостям інтеграції вони є ефективною платформою для побудови інтелектуальних рішень, які поєднують технології комп’ютерного зору, дактилоскопії та цифрової аутентифікації.

Особливої уваги потребує створення систем, що використовують кілька рівнів перевірки особи, а саме: розпізнавання обличчя, ідентифікацію за відбитком пальця та підтвердження через PIN-код. Такий підхід забезпечує значно вищий рівень захисту порівняно з однофакторними методами та дозволяє мінімізувати ризики несанкціонованого доступу у захищені зони.

Актуальність теми. Актуальність даного дослідження зумовлена необхідністю підвищення рівня безпеки у приміщеннях різного призначення. Зростання кількості пристроїв, що підтримують біометрію, а також доступність модулів та одноплатних комп’ютерів відкривають можливості для створення персоналізованих систем контролю доступу з високим рівнем надійності.

Метою роботи є розробка, програмна реалізація та дослідження багаторівневої системи контролю доступу на базі Raspberry Pi з

використанням технологій розпізнавання обличчя, сканування відбитків пальців та PIN-коду.

Об’єкт дослідження – процес побудови та функціонування багаторівневої системи контролю доступу.

Предмет дослідження – апаратні та програмні методи ідентифікації та аутентифікації користувачів у системах контролю доступу, а також їх інтеграція у єдину інтелектуальну систему.

Завдання дослідження:

– проаналізувати сучасні методи та технології контролю доступу;

– вибрати апаратного та програмного забезпечення;

– реалізувати алгоритм багаторівневої аутентифікації користувача;

– розробити логіку взаємодії між модулями;

– провести тестування та оцінити швидкість, точність і стабільність роботи системи;

– проаналізувати отримані результати та визначити ефективність запропонованого рішення.

Апробація результатів. Результати роботи опубліковані в науковому журналі «Технічні вісті» 2025/1(61), 2(62). С. 66-68. [1].

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА КОНТРОЛЮ ДОСТУПУ

1.1 Основна ідея багаторівневої системи аутентифікації користувачів

У сучасних умовах цифрової безпеки та зростання обсягів конфіденційної інформації надзвичайно важливо забезпечити надійний контроль доступу до ресурсів як у корпоративних, так і у приватних системах. Багаторівнева аутентифікація користувачів є одним із ключових інструментів, що дозволяє значно підвищити рівень безпеки. Основна ідея цієї системи полягає у поєднанні кількох незалежних факторів, що підтверджують особу користувача [2]. Це дозволяє створити надійний механізм захисту, який складніше обійти, ніж одиночні методи перевірки.

Традиційно фактори аутентифікації поділяються на три основні категорії. Перша категорія – це те, що користувач знає, наприклад, пароль або ПІН-код. Ці методи досить прості у впровадженні, однак вони мають низку обмежень, зокрема схильність до підбору або компрометації. Друга категорія – це те, що користувач має, наприклад, смарт-карта, апаратний токен або ключ доступу. Такі засоби більш надійні, оскільки фізичне володіння необхідним пристроєм робить несанкціонований доступ складнішим. Третя категорія – це те, ким користувач є, тобто біометричні характеристики, наприклад відбитки пальців, розпізнавання обличчя, сітківка ока або голос. Біометричні методи відзначаються високою унікальністю та практичною неможливістю підробки.

Використання одночасно двох або більше факторів формує багаторівневу систему аутентифікації. Наприклад, у сучасних офісах часто застосовується комбінація пароля та біометричного сканера: користувач спершу вводить пароль, після чого система перевіряє його відбиток пальця або обличчя. Така послідовність дій забезпечує подвійний рівень перевірки, який значно ускладнює спроби зловмисників отримати доступ. У фінансових

установах або лабораторіях високого рівня безпеки можливе додавання третього рівня – фізичного носія доступу, наприклад смарт-карти або токена, що робить систему ще більш захищеною (рис. 1.1).

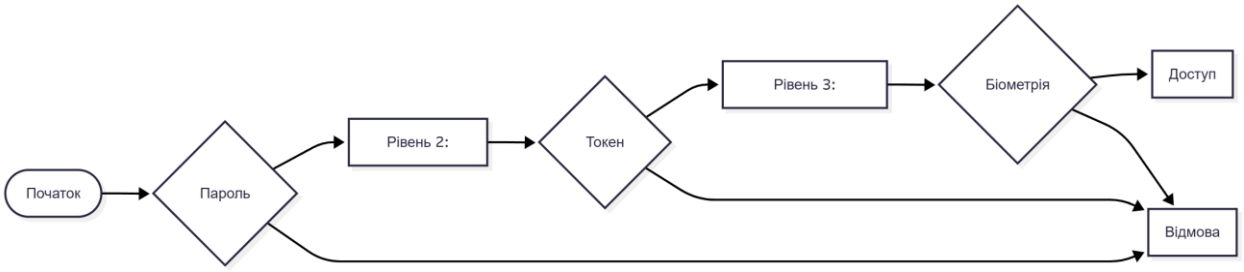


Рисунок 1.1 – Багаторівнева аутентифікація користувача

Багаторівнева аутентифікація має низку важливих переваг [3]. Вона значно ускладнює роботу зловмисників, оскільки для отримання повного доступу необхідно подолати кожен рівень незалежно. Цей підхід знижує ризик компрометації, навіть якщо один із факторів було зламано або викрадено. Крім того, багаторівнева система дозволяє вести контроль та аудит дій користувачів, фіксувати спроби доступу та виявляти підозрілі активності, що підвищує загальний рівень безпеки та керованості системи.

Кожен із факторів аутентифікації має свої особливості та недоліки. Паролі та ПІН-коди зручні та швидкі у використанні, але легко піддаються атакам [4], наприклад підбору або фішингу. Фізичні носії доступу підвищують безпеку, але можуть бути втрачені або викрадені. Біометричні методи забезпечують високий рівень унікальності, проте потребують спеціального обладнання і іноді схильні до помилкових спрацьовувань, особливо при низькій якості сенсорів або зміні умов освітлення.

Застосування багаторівневої аутентифікації стає особливо актуальним у контексті сучасних технологій і програмно-апаратних рішень. Такі системи дозволяють не лише підвищити рівень захисту, але й забезпечують гнучкість конфігурації під конкретні завдання. Наприклад, у житлових приміщеннях можна обмежитися поєднанням пароля та біометрії, у офісах – додати

смарт-карту для контролю входу до окремих зон, а у лабораторіях високого рівня безпеки – підключати централізовану систему моніторингу, яка відслідковує всі дії користувачів.

Багаторівнева система аутентифікації користувачів є ефективним механізмом захисту, що дозволяє об’єднати різні методи перевірки особи, мінімізувати ризики несанкціонованого доступу та забезпечити надійний контроль над доступом до ресурсів будь-якого рівня важливості.

1.2 Методи та принципи біометричної ідентифікації

Біометрична ідентифікація користувачів є ключовим елементом сучасних систем контролю доступу, оскільки вона дозволяє визначити особу на основі фізичних або поведінкових характеристик. Принцип біометрії ґрунтується на тому, що кожна людина має унікальні ознаки, які практично неможливо підробити або повторити. Основні категорії біометричних характеристик включають фізичні параметри, такі як відбитки пальців, геометрія обличчя, структура сітківки ока, голос, а також поведінкові ознаки, наприклад почерк або манера ходьби (рис. 1.2).

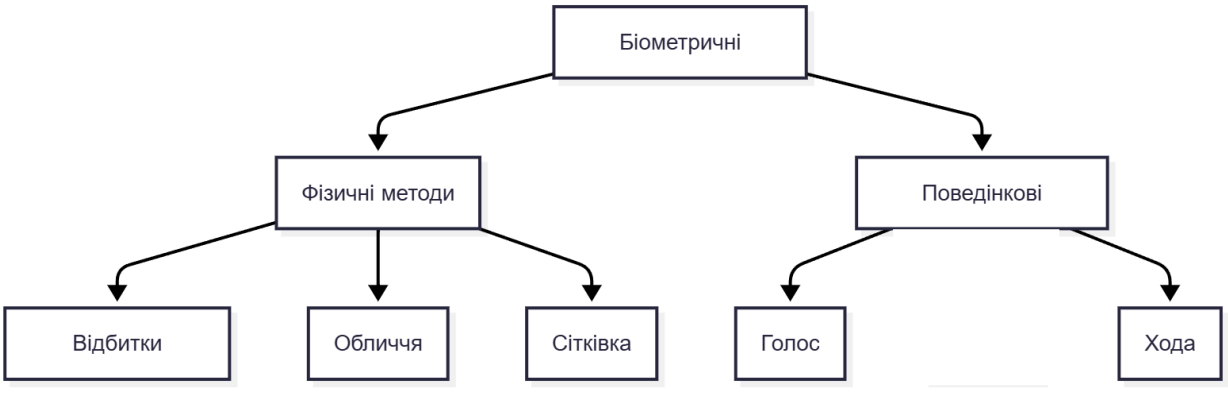


Рисунок 1.2 – Класифікація біометричних методів аутентифікації

Сучасні системи біометричної аутентифікації застосовують декілька методів для підвищення точності та надійності [5]. Найпоширенішим і водночас ефективним є сканування відбитків пальців. Цей метод

використовує унікальні візерунки ліній та гребенів на шкірі пальця, які обробляються спеціальним сенсором і порівнюються з еталонними даними у базі. Висока точність і швидкість розпізнавання роблять його оптимальним для систем з масовим доступом, таких як офіси або банківські установи.

Ще одним популярним методом є розпізнавання обличчя. Технологія працює на основі аналізу геометрії обличчя, відстані між ключовими точками (очі, ніс, рот) та формування цифрового шаблону. Цей метод зручний, оскільки не потребує фізичного контакту з сенсором і може використовуватися для безконтактного контролю доступу. Водночас розпізнавання обличчя має деякі обмеження, пов’язані з освітленням, зміною зовнішнього вигляду користувача або використанням масок.

Крім того, у системах високої безпеки застосовують сканування сітківки або райдужної оболонки ока. Ці методи відзначаються надзвичайною точністю, оскільки структура ока унікальна для кожної людини і майже не змінюється протягом життя. Однак високі вимоги до обладнання і комфорт користувача обмежують широке використання цих методів у побутових системах [6].

Інші методи біометричної ідентифікації включають аналіз голосу та поведінкових ознак. Розпізнавання голосу враховує частоту, тембр, ритм мовлення, а поведінкові ознаки – стиль письма, манеру ходи або ж швидкість набору тексту. Хоч ці методи менш точні, вони добре інтегруються з іншими факторами багаторівневої аутентифікації, створюючи додатковий рівень захисту.

Важливо зазначити, що ефективність біометричних систем визначається двома показниками: рівнем помилкових відмов (False Rejection Rate, FRR) та рівнем помилкових прийомів (False Acceptance Rate, FAR). FRR показує, наскільки часто легітимний користувач не може пройти аутентифікацію, а FAR – наскільки часто система помилково приймає сторонню особу. Ідеальна система має низькі значення обох показників, що забезпечує баланс між безпекою і зручністю користувача.

Методи біометричної ідентифікації дозволяють створювати надійні системи контролю доступу, які практично неможливо обійти без фізичного чи поведінкового збігу з даними користувача. Комбінація декількох біометричних факторів у багаторівневій системі підвищує безпеку, мінімізує ризик компрометації та забезпечує ефективний контроль над доступом у різних сферах застосування: від офісів і лабораторій до житлових приміщень і державних установ.

1.3 Аналіз сучасних систем контролю доступу

Системи контролю доступу (СКД) сьогодні є ключовим елементом забезпечення безпеки як у корпоративних структурах, так і в приватних приміщеннях. Їхнє головне завдання полягає у регулюванні доступу користувачів до ресурсів або територій відповідно до встановлених правил та політик безпеки. На відміну від традиційних механічних замків, сучасні СКД використовують електроніку, програмне забезпечення та інтеграцію з іншими системами безпеки, такими як відеоспостереження, сигналізація та аналітика подій[7].

Сучасні СКД можна класифікувати за способом аутентифікації користувача. Це може бути класичний пароль або ПІН-код, фізичні носії доступу (смарт-карти, токени), біометричні методи або комбіновані багаторівневі рішення. Поєднання декількох методів підвищує рівень безпеки та зменшує ризик несанкціонованого доступу (рис. 1.3).

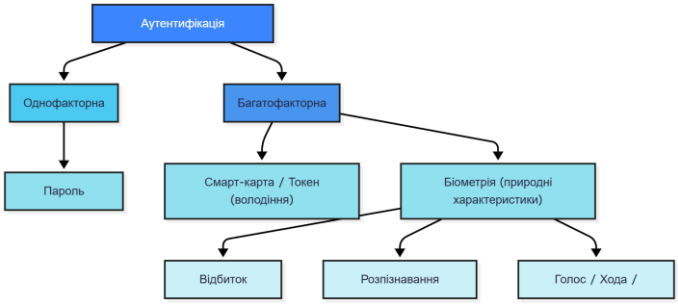


Рисунок 1.3 – Типи аутентифікації у сучасних системах контролю доступу

Ще один важливий критерій – архітектура системи. СКД можуть бути централізованими або децентралізованими. У централізованих системах всі дані про користувачів та події зберігаються на сервері, що забезпечує легкий контроль, аудит і можливість інтеграції з іншими системами безпеки. Децентралізовані системи працюють автономно на рівні окремих пристроїв і не залежать від мережевого підключення, що підвищує їхню стійкість до відмов, але обмежує централізоване управління (рис. 1.4).

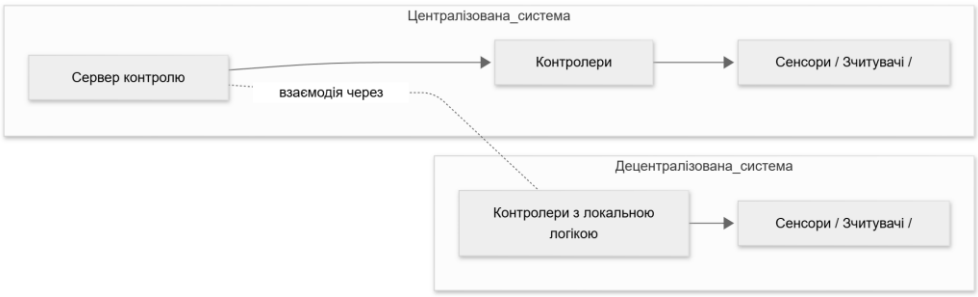


Рисунок 1.4 – Архітектура систем контролю доступу: централізована та децентралізована моделі

Сучасні СКД також відрізняються типом інтеграції та управління. Найпоширенішими є системи з безконтактними картками або токенами, які забезпечують швидкий доступ і ведення історії подій. Біометричні системи, що використовують відбитки пальців, обличчя або сітківку ока, надають високий рівень захисту та практично не піддаються підробці. Комбіновані системи, які поєднують декілька методів аутентифікації, забезпечують максимальний рівень безпеки, особливо у середовищах із підвищеними вимогами до доступу (рис. 1.5).

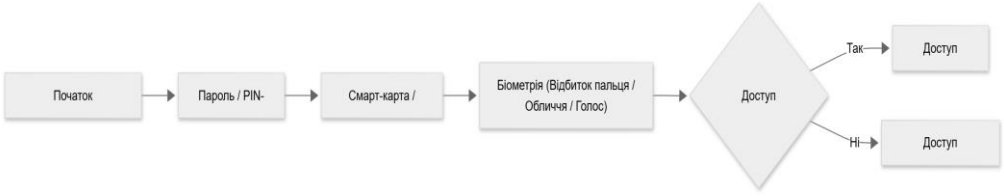


Рисунок 1.5 – Комбінована система контролю доступу: багаторівнева перевірка користувача

Важливим аспектом є інтеграція СКД з іншими технологіями. Системи можуть передавати дані на централізований сервер, синхронізуватися з базами даних співробітників, інтегруватися з відеоспостереженням для підтвердження дій користувачів або використовувати мобільні додатки для дистанційного керування доступом. Така інтеграція підвищує зручність, дозволяє автоматизувати процеси та робить систему гнучкою.

Крім того, сучасні системи контролю доступу мають розвинені аналітичні функції: відстеження часу входу та виходу, журнал подій, аналіз спроб несанкціонованого доступу та формування звітів для керівництва. Такі можливості дозволяють оперативно реагувати на порушення та прогнозувати потенційні загрози, оптимізуючи політики доступу у різних підрозділах організації (рис. 1.6).

Рисунок 1.6 – Статистика доступу користувачів у відділах

Аналіз сучасних систем контролю доступу показує, що ефективна СКД повинна поєднувати різні методи аутентифікації, мати адаптивну архітектуру, інтегруватися з іншими системами безпеки та забезпечувати аналітичні функції для контролю і управління. Використання таких

комплексних рішень дозволяє підвищити рівень безпеки, мінімізувати ризики несанкціонованого проникнення та забезпечити надійний контроль над доступом до ресурсів будь-якого рівня важливості.

1.4 Технології розпізнавання обличчя та відбитків пальців

Сучасні технології біометричної ідентифікації здатні значно підвищити рівень безпеки, забезпечуючи точне та швидке визначення особи користувача. Два найпоширеніших методи – це розпізнавання обличчя та сканування відбитків пальців, які широко використовуються у корпоративних системах контролю доступу, мобільних пристроях та IoT-рішеннях.

Розпізнавання обличчя ґрунтується на аналізі унікальних геометричних характеристик обличчя користувача, таких як відстань між очима, форма носа, контури щелепи та інші параметри. Сучасні алгоритми використовують глибокі нейронні мережі**,** які дозволяють точно відрізняти особи навіть за зміненого освітлення, пози обличчя чи часткового перекриття. Висока точність розпізнавання робить цю технологію популярною для безконтактного контролю доступу, що особливо важливо в умовах сучасних гігієнічних норм (рис. 1.7).

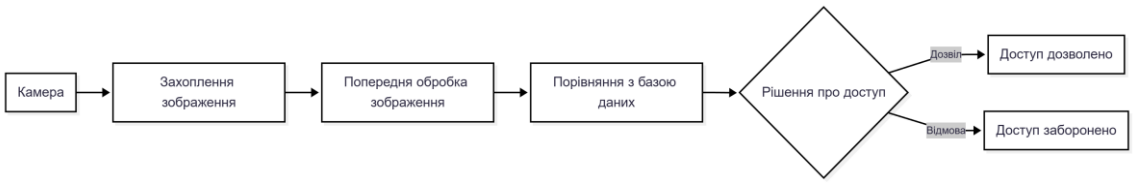


Рисунок 1.7 – Схема роботи розпізнавання обличчя

Сканери відбитків пальців працюють на основі унікальних візерунків шкірних гребенів. Вони можуть використовувати різні методи зчитування: оптичний, ємнісний або ультразвуковий. Оптичні сканери створюють зображення відбитка за допомогою світла, ємнісні – визначають структуру

рельєфу пальця через електричні заряди, а ультразвукові – точніше відтворюють деталі гребенів навіть через легкі забруднення чи вологу. Завдяки цьому відбиток пальця стає надійним та стабільним фактором аутентифікації (рис. 1.8).

Рисунок 1.8 – Схема роботи розпізнавання відбитку

Обидві технології часто комбінують у багаторівневих системах контролю доступу, що дозволяє підвищити безпеку, адже злам одного фактора не дає можливості пройти аутентифікацію. Наприклад, система може спочатку виконати швидку перевірку обличчя, а потім вимагати підтвердження через сканер відбитків.

Ключовим аспектом є точність та надійність: сучасні алгоритми обробки зображень і шаблонів відбитків забезпечують високий рівень розпізнавання, зменшуючи кількість помилкових спрацьовувань та пропусків. Водночас, технології постійно вдосконалюються завдяки розвитку машинного навчання, що дозволяє адаптувати систему до різних умов освітлення, зношеності сенсорів або зміни зовнішності користувачів (рис. 1.9).

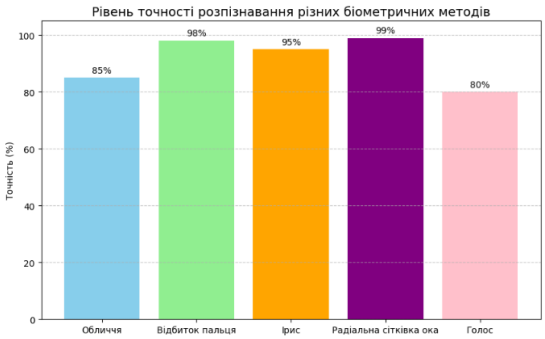


Рисунок 1.9 – Рівень точності розпізнавання різних біометричних методів

Розпізнавання обличчя та відбитків пальців є надійними і взаємодоповнюючими методами біометричної аутентифікації. Вони дозволяють організувати безконтактний і безпечний доступ, швидко ідентифікувати користувача та інтегруватися у багаторівневі системи контролю доступу, що є особливо актуальним у сучасних умовах підвищених вимог до безпеки.

1.5 Застосування одноплатних комп'ютерів Raspberry Pi у системах безпеки

Одноплатні комп'ютери, зокрема Raspberry Pi**,** сьогодні широко застосовуються у різноманітних системах безпеки завдяки своїй компактності, низькій вартості та великій функціональності. Завдяки роз'ємам GPIO, підтримці камер та сенсорів, а також можливості працювати з різними операційними системами та мовами програмування, Raspberry Pi дозволяє реалізувати прототипи і навіть готові рішення для контролю доступу, відеоспостереження та моніторингу подій.

Однією з переваг Raspberry Pi (рис. 1.10), є гнучкість підключення різних периферійних пристроїв. До плати можна підключати модулі камер, сенсори відбитків пальців, дисплеї та кнопки, що дозволяє створювати багаторівневі системи аутентифікації [8]. Завдяки відкритій архітектурі, розробник може швидко інтегрувати різні алгоритми розпізнавання обличчя чи обробки сигналів з сенсорів, що робить систему персоналізованою та масштабованою.

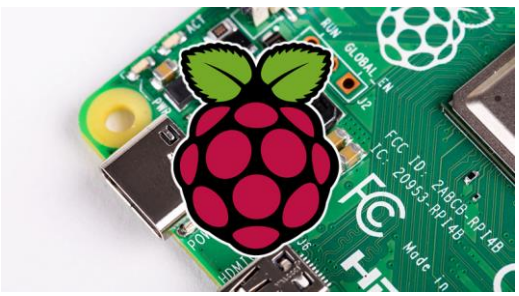


Рисунок 1.10 – Зображення логотипу Raspberry

Raspberry Pi також забезпечує підтримку мережевих протоколів, що дозволяє підключати систему до локальної мережі або інтернету. Це відкриває можливості для централізованого моніторингу, віддаленого керування та зберігання журналів доступу на сервері. Таким чином, навіть компактна платформа може стати ядром складної системи безпеки, яка включає відеоспостереження, логування подій та аналітику поведінки користувачів (рис. 1.11).

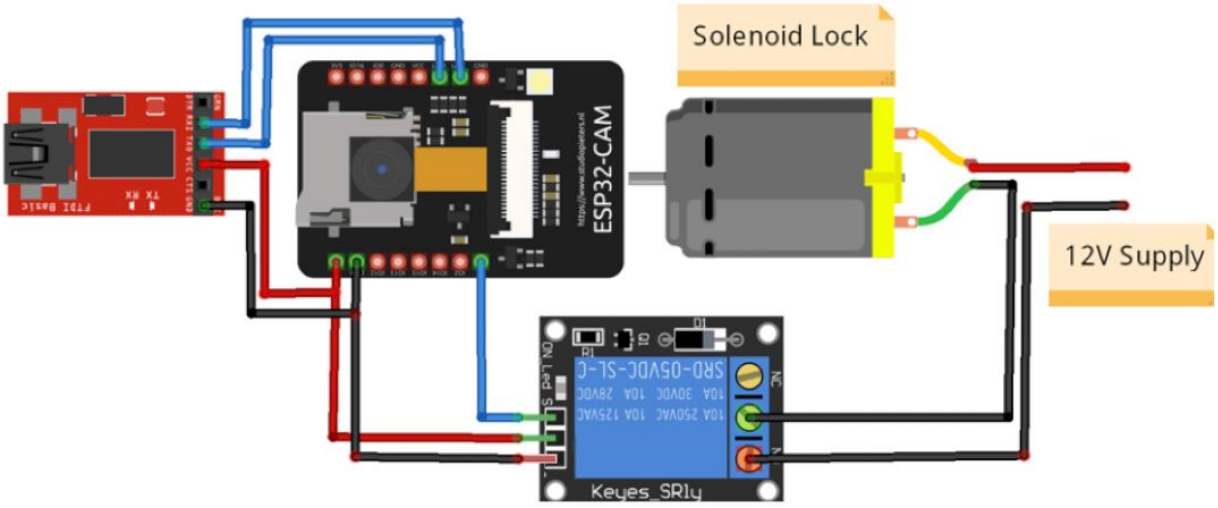


Рисунок 1.11 – Raspberry Pi у складі системи контролю доступу

Ще однією важливою перевагою є підтримка різних операційних систем та бібліотек, що дозволяє використовувати Python, C/C++, а також спеціалізовані бібліотеки для обробки зображень та керування сенсорами. Це забезпечує швидку розробку алгоритмів біометричної аутентифікації та логіки доступу, без необхідності складного апаратного програмування.

Завдяки поєднанню апаратної компактності, доступності та потужності для обробки даних, Raspberry Pi дозволяє створювати як тестові прототипи, так і повноцінні системи контролю доступу з багаторівневою аутентифікацією. Це робить платформу ідеальним інструментом для навчальних лабораторій, дослідницьких проєктів та практичної реалізації інтелектуальних систем безпеки (рис. 1.12).

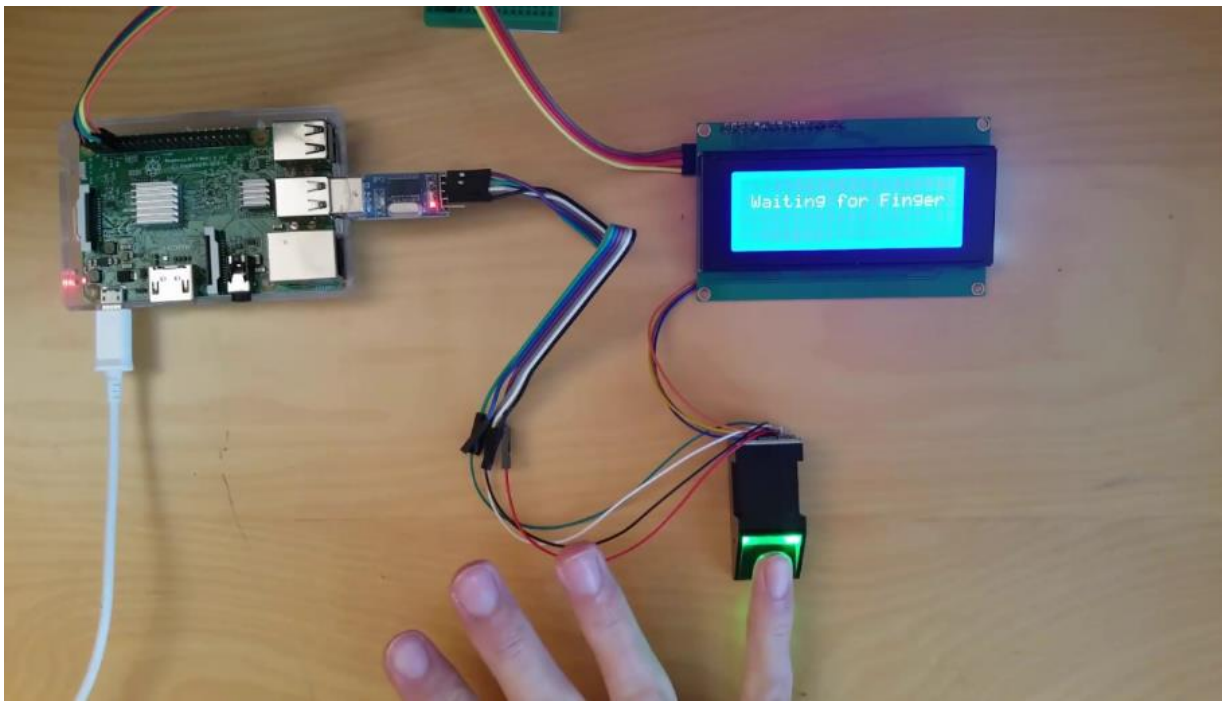


Рисунок 1.12 – Зображення зібраного прототипу

Застосування Raspberry Pi у системах безпеки дозволяє поєднувати теоретичні підходи до біометричної аутентифікації з практичною реалізацією, створюючи доступні, масштабовані та надійні рішення для контролю доступу.

РОЗДІЛ 2
РОЗРОБКА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ ДОСТУПУ НА БАЗІ RASPBERRY PI

2.1 Мета та завдання створення системи

Мета створення інтелектуальної системи доступу полягає у забезпеченні високого рівня безпеки приміщень та ресурсів підприємства при одночасному збереженні зручності та швидкості користування для авторизованих осіб. Сучасні об’єкти, включно з офісними будівлями, лабораторіями та житловими комплексами, потребують комплексного контролю доступу, який дозволяє не лише перевіряти права користувачів, а й здійснювати аналіз поведінки, відстежувати спроби несанкціонованого входу та проводити аудит подій. В умовах постійного розвитку кіберзагроз і фізичних ризиків застосування традиційних методів контролю, таких як ключі або паролі, вже не забезпечує достатнього рівня безпеки, що підкреслює актуальність розробки системи з багаторівневою аутентифікацією [9].

Реалізація системи передбачає використання сучасних біометричних технологій, зокрема розпізнавання обличчя та відбитків пальців, які дозволяють точно ідентифікувати користувача і знизити ймовірність помилкових відмов. Камери та сенсори зчитують біометричні дані користувачів та порівнюють їх із шаблонами, збереженими в базі даних. Такий підхід забезпечує високу точність, швидкість обробки інформації і значно підвищує надійність системи порівняно з однофакторними методами контролю. Крім того, комбінація кількох незалежних факторів перевірки дозволяє створити адаптивну систему, яка регулює рівень контролю залежно від часу доби, рівня ризику або місця доступу [10].

Багаторівнева аутентифікація передбачає послідовне проходження користувачем кількох рівнів перевірки. На першому рівні користувач вводить пароль або PIN-код, що є базовим фактором доступу. Другий рівень включає

перевірку біометричних даних, що здійснюється за допомогою камери або сенсора відбитків. Така послідовність дозволяє істотно зменшити ризик несанкціонованого доступу, адже навіть при компрометації одного рівня доступ до об’єкта неможливий [11]. У разі невідповідності даних система автоматично видає відмову та фіксує подію у журналі, що забезпечує прозорість та контроль за всіма операціями.

Ведення журналу подій є важливою складовою системи. Кожна спроба доступу фіксується з точним зазначенням часу, результату перевірки та ідентифікаційних даних користувача. Така функція дозволяє проводити аудит активності персоналу, виявляти підозрілі дії, вчасно реагувати на потенційні загрози та формувати статистичні звіти. Журнал може зберігатися локально або передаватися на централізований сервер для більш ефективного контролю та аналітики [12].

Система передбачає масштабованість та адаптивність. Вона повинна підтримувати додавання нових користувачів та інтеграцію додаткових апаратних модулів без суттєвої реконфігурації існуючих компонентів. Це дозволяє використовувати систему як у невеликих офісах, так і у великих комплексах з багатьма точками доступу. Додаткові модулі можуть включати камери, сенсори або інтерфейси віддаленого контролю, що розширює функціональні можливості системи та забезпечує гнучкість при зміні умов експлуатації [13].

Особлива увага приділяється зручності користувача та інтерактивності. Система повинна бути інтуїтивно зрозумілою і забезпечувати швидкий доступ. TFT-дисплей або інші інтерфейси відображають результати перевірки, стан системи та повідомлення про помилки в реальному часі. Таке рішення підвищує ефективність роботи користувачів і дозволяє адміністраторам контролювати процес без додаткових затрат часу.

Завдяки реалізації всіх цих завдань система поєднує сучасні підходи до біометричної аутентифікації з практичною реалізацією на компактній апаратній платформі. Вона забезпечує високий рівень безпеки, гнучкість

налаштувань та можливість подальшого розвитку, включаючи інтеграцію нових алгоритмів розпізнавання, аналітики та віддаленого контролю доступу. Така система створює фундамент для практичної реалізації та тестування, що буде детально розглянуто у наступних підрозділах другого розділу.

2.2 Вибір апаратних компонентів системи

При розробці інтелектуальної системи доступу особлива увага приділяється вибору апаратних компонентів, оскільки від них безпосередньо залежить ефективність і надійність роботи системи. Основним елементом є одноплатний комп’ютер Raspberry Pi (рис. 2.1), який обрано через його компактність, високу продуктивність та можливість підключення різноманітних периферійних пристроїв. Raspberry Pi дозволяє запускати необхідне програмне забезпечення для обробки біометричних даних, контролю сенсорів та взаємодії з користувачем через дисплей, одночасно забезпечуючи достатню обчислювальну потужність для роботи алгоритмів розпізнавання обличчя та відбитків пальців [14].

Рисунок 2.1 – Raspberry Pi 4

Для зчитування біометричних даних обрано модуль ESP32-CAM, який забезпечує достатню роздільну здатність для точного розпізнавання обличчя

навіть при різних умовах освітлення. Камера підключається до Raspberry Pi і передає зображення для обробки алгоритмами комп’ютерного зору. Модуль ESP32-CAM (рис. 2.2), також підтримує функції обробки зображень на борту, що дозволяє зменшити затримки при передачі даних і підвищує швидкість ідентифікації [15].

Рисунок 2.2 – ESP32-CAM

Важливим компонентом є сенсор відбитків пальців (рис. 2.3), який забезпечує другий рівень біометричної аутентифікації. Сенсор підключається через послідовний інтерфейс або USB до Raspberry Pi і дозволяє швидко зчитувати відбитки, порівнювати їх із шаблонами та видавати результат перевірки. Такі сенсори зазвичай обладнані алгоритмами детекції «живого» пальця, що запобігає обману системи за допомогою зображень чи відбитків з інших матеріалів.

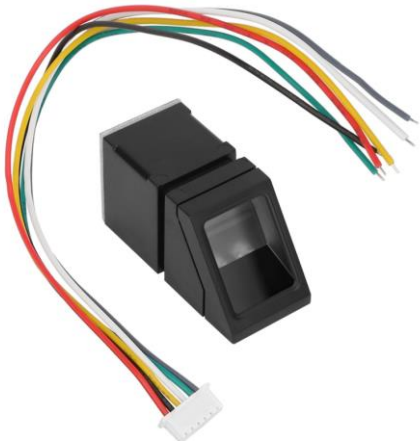


Рисунок 2.3 – Сенсор відбитків пальців R307

Для взаємодії з користувачем використовується TFT-дисплей (рис. 2.4), який дозволяє відображати повідомлення про стан системи, результати перевірки та інструкції. Дисплей підключається через GPIO або SPI інтерфейс, що забезпечує швидку передачу даних і підтримку графічного інтерфейсу з анімаціями та текстовими повідомленнями [16].

Рисунок 2.4 – TFT-дисплей

Для введення PIN-коду використовується клавіатура типу numlock (рис. 2.5), яка підключається до Raspberry Pi через GPIO або USB. Клавіатура дозволяє користувачам швидко та зручно вводити код для авторизації, а система миттєво обробляє його та передає на наступний рівень аутентифікації. Використання клавіатури разом із біометричними модулями забезпечує багаторівневу перевірку та підвищує надійність системи, оскільки навіть при тимчасовій несправності одного з біометричних сенсорів користувач може пройти контроль за допомогою PIN-коду [17].

Клавіатура також може мати підсвічування клавіш для комфортного використання у темний час доби або індикатори натискання, що полегшує введення коду без помилок. При цьому програмне забезпечення обробляє натискання та захищає від повторного введення чи спроб підбору коду, що підвищує безпеку системи. Такий підхід дозволяє комбінувати традиційні

методи аутентифікації з сучасними біометричними технологіями, створюючи надійну та зручну систему доступу.

Рисунок 2.5 – NumLock

Крім основних модулів, система потребує додаткових елементів, таких як кнопки для введення PIN-коду, індикатори стану доступу, а також джерела живлення, які забезпечують стабільну роботу всіх компонентів. Всі апаратні модулі інтегруються з Raspberry Pi, що дозволяє централізовано обробляти дані, керувати інтерфейсом і вести журнал подій.

Вибір апаратних компонентів продиктований прагненням поєднати надійність, компактність та гнучкість системи**.** Кожен модуль має відповідати вимогам швидкої і точної ідентифікації, забезпечувати безперебійну роботу у різних умовах та легко замінюватися або модернізуватися при необхідності (рис. 2.6). Така конфігурація дозволяє реалізувати багаторівневу аутентифікацію з високим рівнем безпеки та зручністю для користувачів [18].

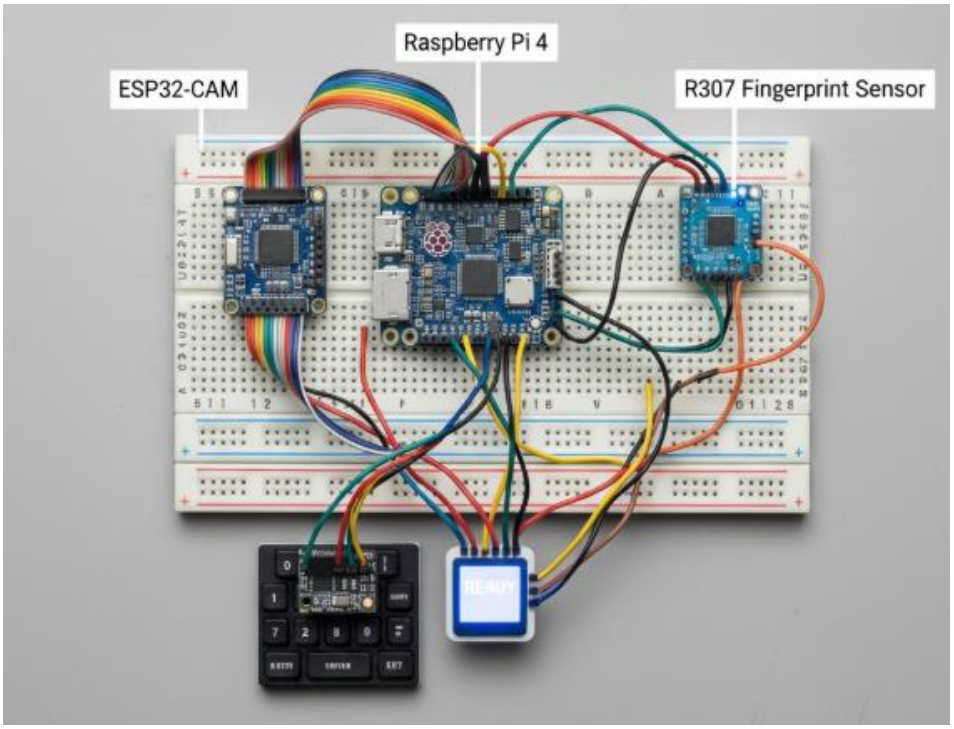
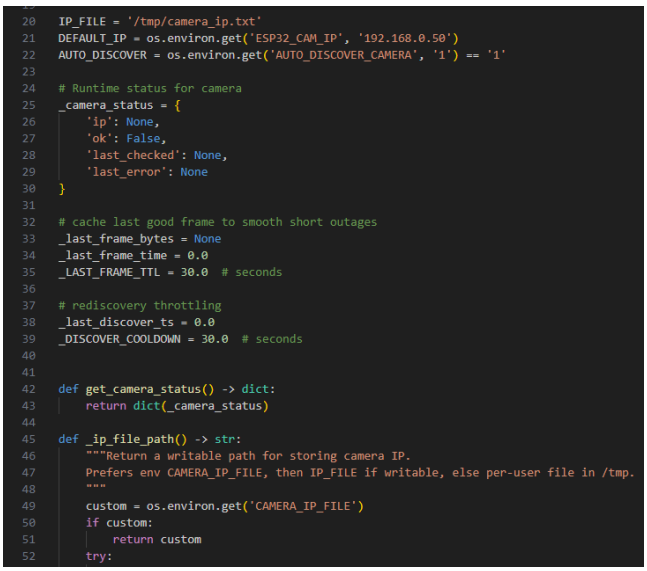


Рисунок 2.6 – Загальна схема проекту

Завдяки ретельно підібраним апаратним компонентам система забезпечує швидку обробку даних, надійність перевірки користувачів, зручність інтерфейсу та масштабованість, що є необхідним для практичної реалізації та подальшої інтеграції нових модулів і алгоритмів.

2.3 Вибір програмних засобів розробки

Для ефективної роботи багаторівневої системи доступу особливе значення має правильний вибір програмних засобів розробки, які забезпечують взаємодію між апаратними модулями та алгоритмами обробки біометричних даних. Основною мовою програмування для реалізації логіки системи обрано Python (рис. 2.7), оскільки вона має широкі можливості для обробки зображень, підтримує роботу з периферійними пристроями Raspberry Pi і ESP32-CAM, а також дозволяє швидко інтегрувати готові бібліотеки для біометрії та машинного навчання [19].



```
IP_FILE = '/tmp/camera_ip.txt'
DEFAULT_IP = os.environ.get('ESP32_CAM_IP', '192.168.0.50')
AUTO_DISCOVER = os.environ.get('AUTO_DISCOVER_CAMERA', '1') == '1'

# Runtime status for camera
_camera_status = {
    'ip': None,
    'ok': False,
    'last_checked': None,
    'last_error': None
}

# cache last good frame to smooth short outages
_last_frame_bytes = None
_last_frame_time = 0.0
_LAST_FRAME_TTL = 30.0  # seconds

# rediscovery throttling
_last_discover_ts = 0.0
_DISCOVER_COOLDOWN = 30.0  # seconds


def get_camera_status() -> dict:
    return dict(_camera_status)

def _ip_file_path() -> str:
    """Return a writable path for storing camera IP.
    Prefers env CAMERA_IP_FILE, then IP_FILE if writable, else per-user file in /tmp.
    """
    custom = os.environ.get('CAMERA_IP_FILE')
    if custom:
        return custom
    try:
```

Рисунок 2.7 – Код Python, який ініціалізує підключення до ESP32-CAM

Для обробки зображень та розпізнавання обличчя використовується бібліотека OpenCV, яка дозволяє здійснювати фільтрацію, детекцію облич, масштабування та нормалізацію зображень, а також інтеграцію з алгоритмами машинного навчання для точного порівняння шаблонів (рис. 2.8). OpenCV забезпечує оптимальну продуктивність при роботі на Raspberry Pi, дозволяючи виконувати розпізнавання облич у реальному часі без значних затримок [20].

```
# Ініціалізація сенсора один раз
try:
    f = PyFingerprint('/dev/serial0', 57600, 0xFFFFFFFF, 0x00000000)
    if f.verifyPassword():
        print("R307S підключено та пароль вірний")
except Exception as e:
    print("Помилка підключення сенсора:", e)
    f = None

def load_user_slots():
    if os.path.exists(USER_SLOTS_FILE):
        with open(USER_SLOTS_FILE, 'r') as fslots:
            return json.load(fslots)
    return {}

def save_user_slots(user_slots):
    with open(USER_SLOTS_FILE, 'w') as fslots:
        json.dump(user_slots, fslots)

def set_user_slot(user_name, slot):
    user_slots = load_user_slots()
    user_slots[user_name] = slot
    save_user_slots(user_slots)

def get_user_slot(user_name):
    user_slots = load_user_slots()
    return user_slots.get(user_name, None)

def get_free_slot():
    if not f:
        print("[ERROR] Сенсор недоступний")
        return -1
```

Рисунок 2.8 – Код з інтерфейсом OpenCV та результатами

Для роботи із сенсором відбитків пальців застосовуються спеціалізовані бібліотеки, які підтримують підключення по послідовному інтерфейсу або USB, зчитування відбитків та порівняння їх із шаблонами у базі даних. Програмні алгоритми обробки даних сенсора передбачають перевірку «живого» пальця (рис. 2.9), обробку помилкових спроб і зберігання журналу подій для подальшого аналізу [21].

```
Перевірка відбитка пальця для користувача "den"...
[DEBUG] Спроба 1/3: Покладіть палець для перевірки...
[OK] Відбиток підтверджено
```

Рисунок 2.9 – Перевірка відбитку пальців

Для управління користувацьким інтерфейсом TFT-дисплея та клавіатури використовується бібліотека Pygame або спеціалізовані модулі для роботи з GPIO на Raspberry Pi [22]. Це дозволяє відображати повідомлення про стан системи, інструкції користувачеві, індикатори успішного або невдалого доступу, а також забезпечувати інтерактивність при введенні PIN-коду (рис. 2.10).

```
Сканування мережі для пошуку ESP32-CAM...
ESP32-CAM знайдено! IP: 192.168.43.27, MAC: 84:0d:8e:23:1b:78
Камера підключена: 192.168.43.27
1. Реєстрація нового користувача
2. Додати/оновити відбиток пальця
3. Додати/оновити фото обличчя
4. Встановити/змінити PIN
5. Запустити 3-факторну авторизацію
6. Сканувати ESP32-CAM у мережі
7. Вказати IP камери вручну
0. Вихід
```

Рисунок 2.10 – CLI меню

Для централізованого зберігання та обробки даних застосовується база даних SQLite або MySQL (рис. 2.11), яка дозволяє зберігати інформацію про користувачів, шаблони біометричних даних, журнали доступу та статистику

спроб авторизації. Програмні засоби взаємодіють з базою даних для швидкого зчитування та оновлення інформації, що забезпечує оперативну обробку подій .

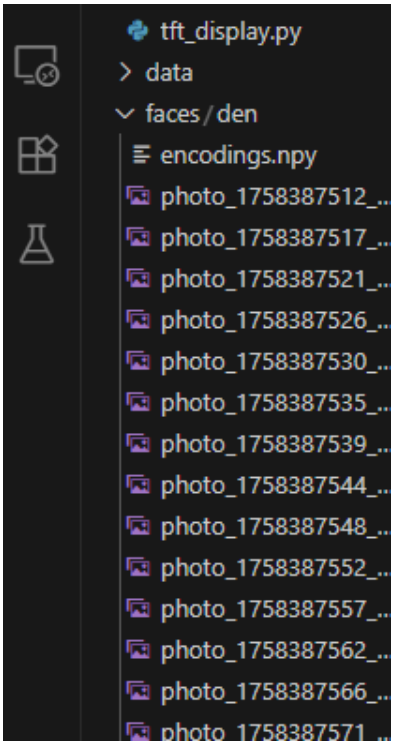


Рисунок 2.11 – Структура бази даних

Завдяки правильному вибору програмних засобів система поєднує надійність, швидкість і гнучкість**,** забезпечує багаторівневу аутентифікацію та зручний інтерфейс для користувачів. Інтеграція Python, OpenCV, бібліотек для роботи з сенсорами, Pygame та бази даних дозволяє швидко впроваджувати нові функції та оптимізувати існуючі алгоритми без значних змін апаратної конфігурації. Це створює надійну платформу для подальшого розвитку системи та її адаптації під конкретні сценарії використання.

2.4 Створення архітектури системи з багаторівневою біометричною ідентифікацією

Архітектура інтелектуальної системи доступу будується за принципом багаторівневої перевірки користувача, що дозволяє забезпечити високий

рівень безпеки та мінімізувати ризики несанкціонованого доступу. Основою системи є одноплатний комп’ютер Raspberry Pi, який виконує роль центрального контролера і координує роботу всіх апаратних та програмних модулів (рис. 2.12).

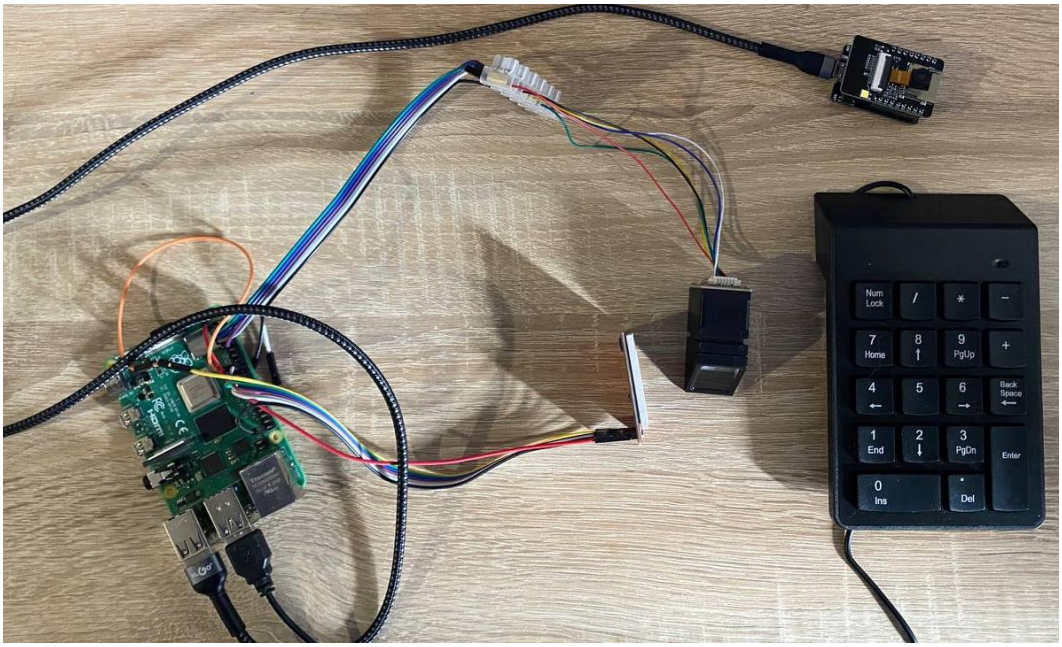


Рисунок 2.12 – Загальна схема проекту з апаратними модулями

Архітектура системи передбачає послідовну обробку даних, де кожен етап виконує конкретну функцію у перевірці користувача. На першому етапі для підтвердження особи використовується ESP32-CAM, яка робить знімок обличчя користувача. Отримане зображення обробляється алгоритмами OpenCV, які виділяють ключові точки обличчя та формують шаблон для порівняння з наявною базою даних. Такий підхід дозволяє з високою точністю визначити, чи відповідає особа власнику облікового запису, і мінімізує можливість несанкціонованого доступу.

На другому етапі активується перевірка відбитка пальця за допомогою сенсора R307. Користувач прикладає палець, і система порівнює отриманий відбиток із базою даних. У разі невідповідності або помилки система повертається до першого етапу, забезпечуючи послідовне та надійне багаторівневе підтвердження доступу.

На третьому етапі користувач вводить PIN-код через фізичну клавіатуру або сенсорну панель. Дані передаються на Raspberry Pi**,** який здійснює перевірку введеного коду та остаточно підтверджує доступ. У разі успішного введення відкривається меню керування на дисплеї, де можна додавати користувачів, переглядати журнал активності та перевіряти базу даних.

Поєднання апаратних та програмних компонентів гарантує високий рівень безпеки, дозволяє контролювати доступ користувачів у режимі реального часу та фіксувати всі події у журналі активності. Кожен етап реалізований у вигляді послідовних блоків, що наочно демонструє блок-схема, вставлена нижче (рис. 2.13).

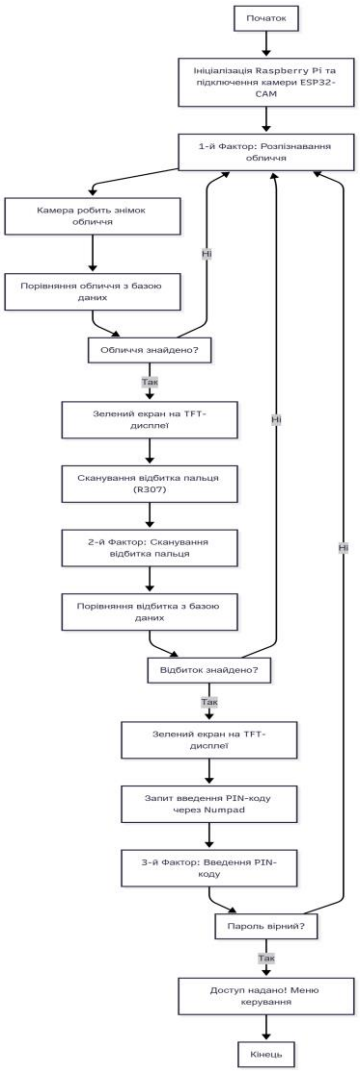


Рисунок 2.13 – Блок-схема алгоритму перевірки користувача

Якщо розпізнавання обличчя не пройдено або сенсор не зчитав відбиток, система пропонує повторну спробу. Такий підхід дозволяє реалізувати адаптивну багаторівневу аутентифікацію, де рівень контролю може змінюватися залежно від часу доби, місця доступу або кількості невдалих спроб.

Програмні модулі обробляють усі отримані дані, ведуть журнал подій, зберігають інформацію про користувачів і шаблони біометрії у базі даних SQLite. База даних є централізованою, що дозволяє швидко виконувати пошук і порівняння шаблонів навіть при великій кількості зареєстрованих користувачів.

Для підвищення надійності система передбачає резервні алгоритми: у разі відмови одного з модулів перевірка може бути перенаправлена на інший сенсор або повторно активована через певний час. Дисплей надає користувачеві повідомлення про стан доступу та підказки при помилках, а додаткові індикатори сигналізують про успішне або невдале сканування.

Архітектура передбачає можливість масштабування: до системи можна підключати нові камери, сенсори, додаткові клавіатури, а також інтегрувати її з централізованими системами безпеки будівлі. Таке рішення дозволяє одночасно забезпечити високий рівень безпеки та гнучкість у налаштуванні системи для різних сценаріїв використання.

Завдяки такій архітектурі система поєднує надійність, швидкість і масштабованість**,** забезпечує багаторівневу перевірку користувачів і гнучко адаптується під конкретні потреби організації. Центральний контролер координує роботу всіх компонентів, обробляє дані з сенсорів і камер, а також веде журнал подій, що створює основу для подальшої аналітики та оптимізації безпеки.

2.5 Алгоритм взаємодії апаратних і програмних модулів

Архітектура розробленої системи багаторівневої аутентифікації передбачає послідовну обробку даних, де кожний етап виконує чітко визначену функцію для перевірки користувача. Після вмикання пристрою система ініціалізує апаратну підсистему та запускає процедуру виявлення модуля камери ESP32-CAM: спочатку здійснюється сканування за IP-адресою, а у разі відсутності відповіді – пошук за MAC-адресою. Результат цієї процедури фіксується у журналі подій; у разі невиявлення камери процедура ініціалізації повторюється до успішного підключення .

Першим рівнем аутентифікації є розпізнавання обличчя. Після встановлення зв’язку з камерою ESP32-CAM здійснюється послідовне зняття зображень користувача і передача їх на обробку Raspberry Pi. Зображення аналізуються алгоритмами OpenCV: виконується детектування обличчя, виділення ключових точок і побудова шаблона для подальшого порівняння з базою даних зареєстрованих профілів. Користувачеві надається до 10 спроб для коректного розпізнавання, у випадку позитивного результату на TFT-дисплеї відображається зелений екран, що сигналізує про успішне проходження першого рівня. Якщо ж протягом 10 спроб відповідність не встановлена, подія заноситься до журналу активності, а процес аутентифікації починається заново від етапу ініціалізації.

Другий рівень – верифікація відбитка пальця за допомогою сенсора R307. Після успішного розпізнавання обличчя активується модуль зчитування відбитків: користувач прикладає палець до сенсора, після чого отриманий зразок порівнюється з шаблонами у базі даних. Для цієї операції передбачено до 3 спроб з урахуванням можливих похибок позиціонування чи часткового зчитування. У разі невдалих трьох спроб подія також фіксується в журналі, і система повертається до першого рівня аутентифікації (повторне розпізнавання обличчя). У разі успішної верифікації відбитка система переходить до остаточного рівня перевірки.

Третім рівнем є введення PIN-коду через фізичну клавіатуру або сенсорну панель. Користувач має до 3 спроб для введення правильного коду, введення порівнюється з локальною базою даних, що зберігається на Raspberry Pi. При трьох невдалих спробах процес повертається на перший рівень (розпізнавання обличчя), а інцидент заноситься до журналу подій. У разі успішного введення PIN-коду на TFT-дисплеї відкривається меню керування, де доступні функції додавання/видалення користувачів, перегляд журналу активності та налаштування системи.

На всіх етапах передбачено детальне логування ключових подій: виявлення/втрати зв’язку з камерою, кількість і результати спроб розпізнавання обличчя, результати сканування відбитка, невдалі спроби введення PIN-коду та інші події безпеки. Журнали служать як для оперативного моніторингу, так і для подальшого аудиту та розслідування інцидентів.

Таким чином, послідовний трирівневий підхід (обличчя → відбиток → PIN) із чітко визначеними лімітами спроб (10/3/3) та централізованим логуванням забезпечує баланс між зручністю користувача і високим рівнем безпеки: кожен фактор незалежно підтверджує ідентичність користувача, а повернення до початкового етапу при невдачі унеможливлює локальні спроби обходу системи.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ РОБОТИ СИСТЕМИ БАГАТОРІВНЕВОЇ АУТЕНТИФІКАЦІЇ

3.1 Апаратна частина системи

Апаратна частина інтелектуальної системи доступу на базі Raspberry Pi 4 є фундаментальною складовою для реалізації багаторівневої аутентифікації користувачів. Центральним елементом системи є Raspberry Pi 4, який виконує роль обчислювального ядра та координує роботу всіх периферійних пристроїв (рис. 3.1). Raspberry Pi відповідає за обробку даних з підключених сенсорів, реалізацію алгоритмів аутентифікації та управління роботою системи в реальному часі. Його продуктивність, наявність достатньої кількості GPIO-виходів, підтримка USB-пристроїв та стабільна робота з бездротовими мережами роблять його ідеальним рішенням для побудови інтелектуальних систем контролю доступу.

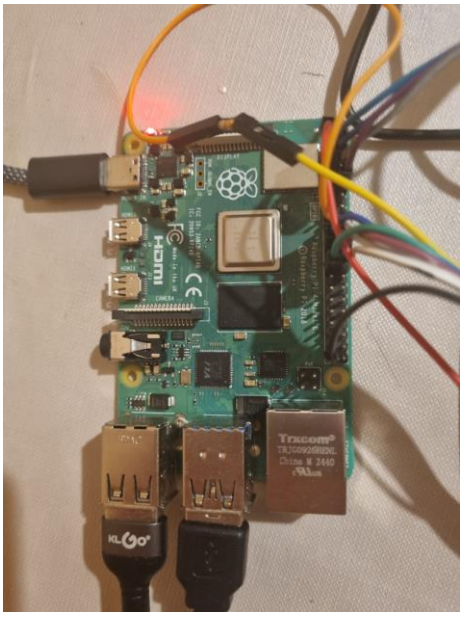


Рисунок 3.1 – Центральний обчислювальний модуль системи

Для першого рівня аутентифікації використовується камера ESP32-CAM, яка підключена до Raspberry Pi через Wi-Fi точку доступу

(рис. 3.2). Камера виконує безконтактну перевірку користувача захоплюючи зображення обличчя та передаючи його на обробку алгоритмами розпізнавання обличь. Камера підтримує роздільну здатність до 2 Мп, що забезпечує достатню чіткість для точного порівняння з шаблонами в базі даних.

Рисунок 3.2 – Камера забезпечення першого рівні аутентифікації

Другий рівень аутентифікації реалізовано за допомогою сканера відбитків пальців R307, який підтримує до 1000 шаблонів для збереження відбитків (рис. 3.3). Сенсор має високу точність і швидкість зчитування до 1 секунди на один відбиток. Після успішного розпізнавання обличчя користувач прикладає палець до сенсора і сканер порівнює відбиток із збереженими шаблонами. Використання сканера R307 дозволяє поєднувати фізичну ідентифікацію та біометричну перевірку, що значно підвищує рівень безпеки системи.

Рисунок 3.3 – Сканер відбитка пальця для забезпечення другого рівня аутентифікації

Для фізичної інтеграції всіх компонентів системи передбачено підключення через GPIO-виходи Raspberry Pi, що дозволяє підключати камеру, сканер відбитків та додаткові сенсори у компактній конфігурації. Це забезпечує зручність монтажу та обслуговування, а також спрощує масштабування системи під нових користувачів або додаткові модулі. Всі провідники надійно зафіксовані, а підключення виконано відповідно до стандартів GPIO Raspberry Pi (рис. 3.4).

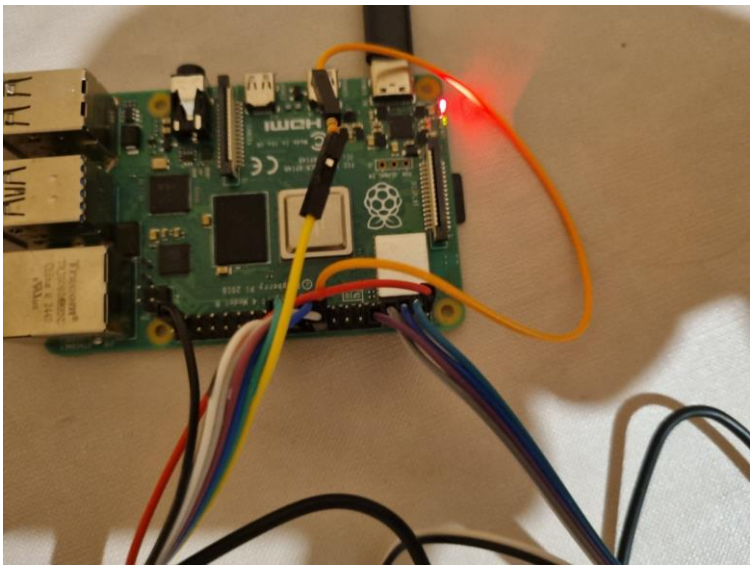


Рисунок 3.4 – Схема підключення камери та сканера до центрального модуля Raspberry Pi

Кожен компонент системи обраний з урахуванням надійності, компактності та економічності. Камера ESP32-CAM забезпечує високу роздільну здатність для точного розпізнавання обличчя, сканер R307 працює швидко та точно, а Raspberry Pi 4 дозволяє обробляти всю інформацію в режимі реального часу без затримок. Компактне розташування компонентів забезпечує легкий доступ для обслуговування та модернізації системи, а також дозволяє інтегрувати додаткові модулі у майбутньому.

Фізичні характеристики компонентів були ретельно підібрані: Raspberry Pi 4 має розміри 88×58×19 мм, камера ESP32-CAM 40×27 мм, сканер R307 60×40×30 мм. Такі розміри дозволяють розмістити всі елементи на невеликій монтажній панелі без ризику механічних пошкоджень. Енергоспоживання системи також оптимізовано: Raspberry Pi 4 споживає до 5 Вт, камера ESP32-CAM до 1 Вт, а сканер R307 до 0,5 Вт, що дозволяє використовувати систему навіть при обмеженому джерелі живлення.

Сумарно, апаратна частина системи забезпечує надійну та стабільну роботу, ефективну багаторівневу перевірку користувача та можливість масштабування під різні потреби користувачів. Всі компоненти пройшли тестування на сумісність, коректність роботи та стабільність функціонування при одночасному підключенні. Така конфігурація дозволяє впровадити повноцінну багаторівневу аутентифікацію, що підвищує загальний рівень безпеки об’єкта.

3.2 Програмна частина системи

Програмна частина інтелектуальної системи доступу на базі Raspberry Pi 4 реалізує повну логіку багаторівневої аутентифікації користувачів та забезпечує взаємодію всіх апаратних компонентів. Система написана мовою Python, що дозволяє легко працювати з камерою ESP32-CAM, сканером відбитків пальців R307 та управляти введенням PIN-коду через користувацький інтерфейс на екрані.

Після подачі живлення Raspberry Pi автоматично запускається програмний модуль аутентифікації. Програма перевіряє доступність камери, встановлює Wi-Fi-зв’язок з ESP32 та готує сенсор відбитків для наступного етапу. Така послідовність забезпечує цілісність обробки даних і мінімізує ймовірність програмних збоїв.

Першим етапом аутентифікації є перевірка обличчя користувача (рис. 3.5). Камера ESP32-CAM захоплює зображення та надсилає його на Raspberry Pi, де алгоритм порівнює отримане зображення з базою даних зареєстрованих обличь. Якщо обличчя знайдено, система переходить до наступного рівня.

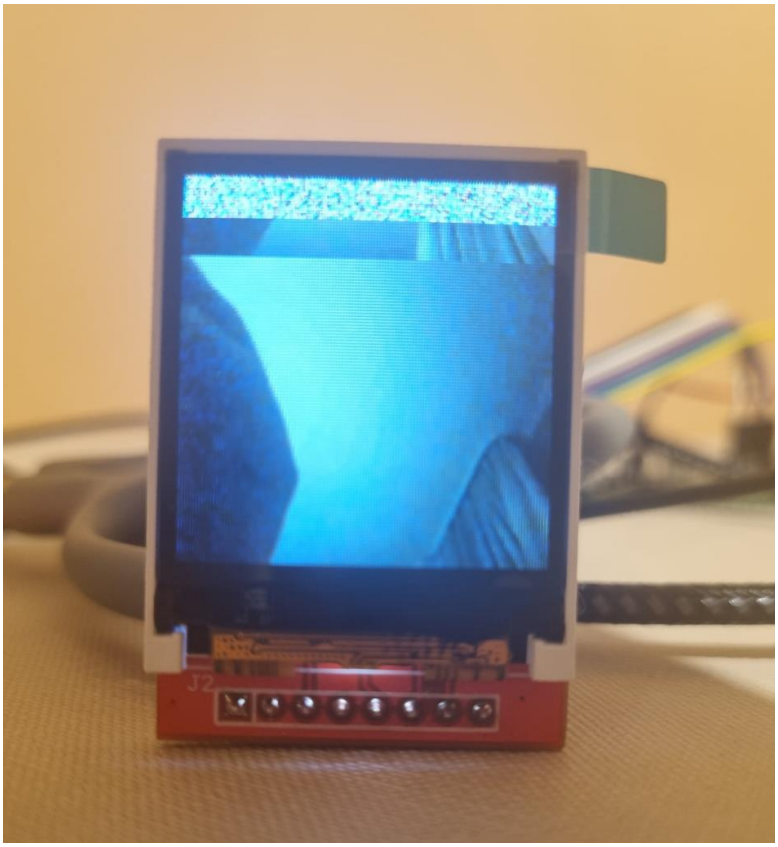


Рисунок 3.5 – Камера захоплює зображення користувача для подальшої перевірки на першому рівні аутентифікації

У разі успішного розпізнавання обличчя користувач бачить повідомлення «Авторизація», що свідчить про успішне проходження першого рівня (рис. 3.6).

Рисунок 3.6 – Підтвердження успішного проходження першого рівня аутентифікації

У випадку коли обличчя не знайдено, система відображає повідомлення «Обличчя не знайдено» і автоматично запускає процес аутентифікації з першого етапу, починаючи з камери (рис. 3.7). На цьому етапі важливим є не лише візуальне інформування користувача, але й фіксація такої події у журналі, оскільки невдале розпізнавання може свідчити як про звичайну помилку позиціонування, так і про потенційну несанкціоновану спробу доступу. Після повідомлення програмний модуль автоматично запускає перезапуск першого етапу, повертаючись до спроби розпізнавання обличчя.

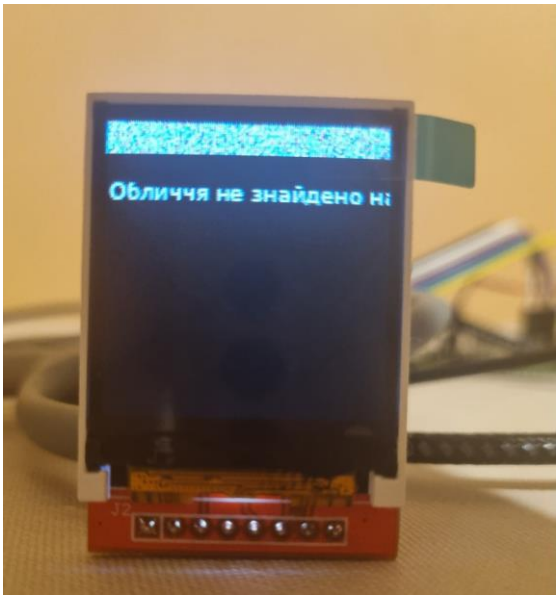


Рисунок 3.7 – Повідомлення про невдалу спробу розпізнавання обличчя

Другий рівень аутентифікації реалізовано на основі сканера відбитків пальців R307. Перед початком роботи програма ініціалізує сенсор, перевіряє наявність шаблонів та готовність до зчитування. Користувачу потрібно прикласти палець до сканера, який виконує захоплення та обробку відбитка. Отриманий шаблон передається на Raspberry Pi, де проводиться порівняння з існуючими записами (рис. 3.8).

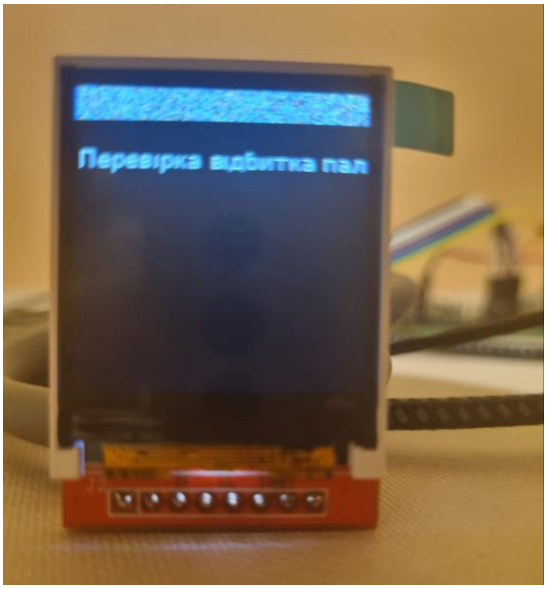


Рисунок 3.8 – Процес порівняння відбитка пальця з шаблонами в базі даних для другого рівня аутентифікації

У разі успішного збігу система переходить до третього рівня про що користувача інформує відповідне повідомлення (рис. 3.9). На цьому етапі система демонструє логічну послідовність переходів, що виключає можливість проходження неповної аутентифікації.

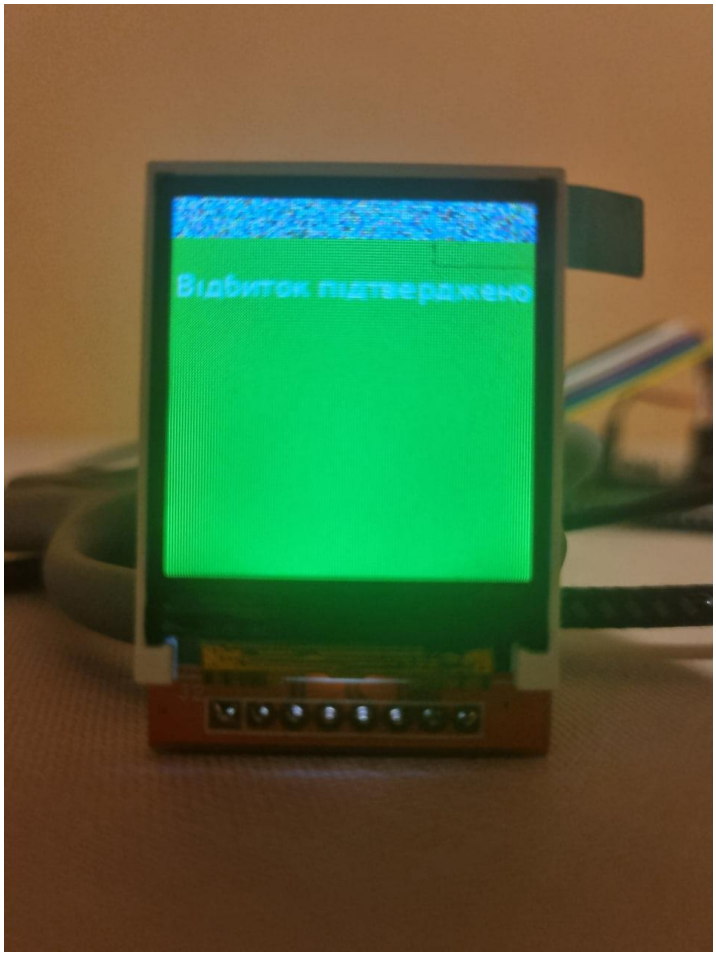


Рисунок 3.9 – Повідомлення про успішну перевірку відбитка пальця підтверджує проходження другого рівня

Важливо відзначити, що коли відбиток прочитати не вдається або він не відповідає жодному з шаблонів. У такому разі на екран виводиться повідомленням «Авторизація не пройдена» (рис. 3.10). Одночасно здійснюється автоматичне журналювання. Після цього система повертається до першого етапу розпізнавання обличчя, забезпечуючи повторний і повністю незалежний цикл аутентифікації.

Рисунок 3.10 – Невдала спроба перевірки відбитка

Третій етап вимагає введення PIN-коду (рис. 3.11). PIN-код виступає додатковим фактором безпеки, що дозволяє запобігти доступу у випадку компрометації попередніх рівнів. Програма перевіряє правильність введеного коду та підтверджує доступ. У разі помилки програма дає можливість ще два рази повторно ввести PIN-код. Після трьох невдалих спроб процес аутентифікації починається з першого етапу. Це забезпечує захист від підбору коду та підсилює загальну стійкість системи.

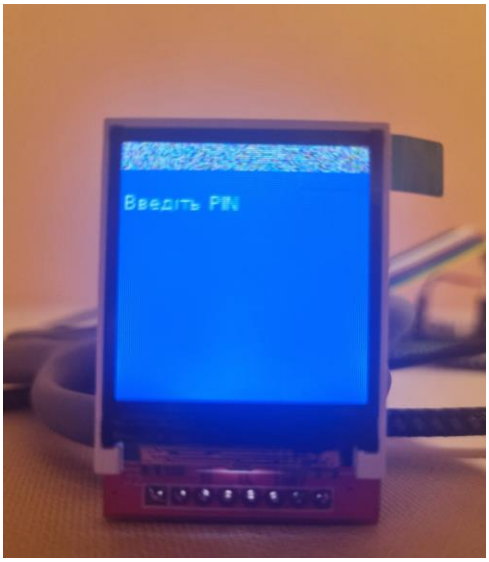


Рисунок 3.11 – Система запитує PIN-код для завершення третього рівня аутентифікації

Програмна частина також реалізує систему управління користувачами, доступну через спеціальне меню (рис. 3.12). За його допомогою є можливість реєструвати нових користувачів, оновлювати їхні фотографії, відбитки пальців, змінювати та відновлювати PIN-коди, а також переглядати журнал спроб доступу.

Рисунок 3.12 – Меню для керування обліковими записами користувачів

Розширений інтерфейс меню містить усі доступні опції керування та зроблений таким чином, щоб забезпечити зручність адміністрування (рис. 3.13).

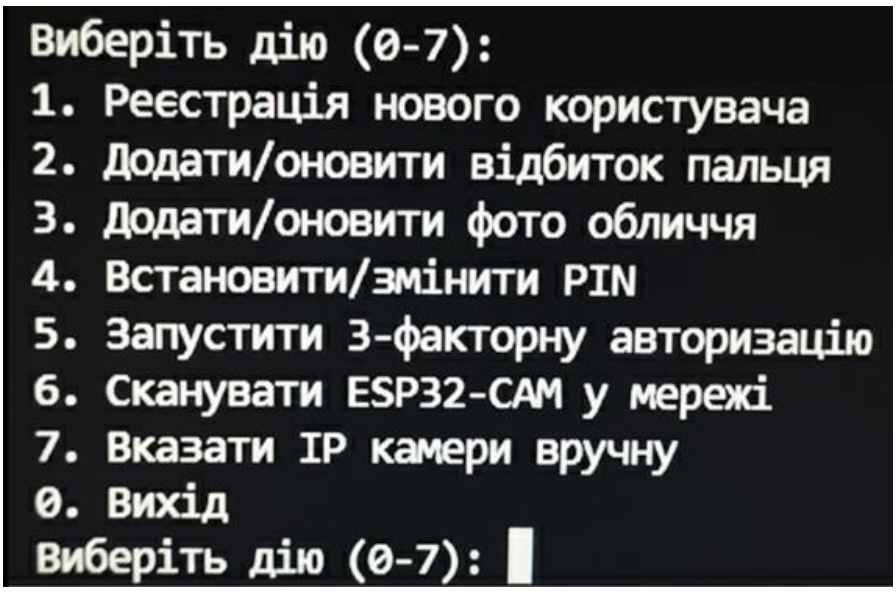


Рисунок 3.13 – Інтерфейс меню системи з усіма опціями

Особливу увагу приділено обробці помилок та повторних спроб аутентифікації. Програма контролює час аунтефікації, обмежує кількість спроб на кожному рівні та автоматично повертає користувача на початковий етап у разі невдачі. Усі дії та результати перевірок зберігаються у базі даних для подальшого аналізу та підвищення безпеки системи.

Програмна частина забезпечує стабільність, безпеку та масштабованість системи. Завдяки використанню Python реалізована можливість легко додавати нові функції, інтегрувати додаткові сенсори та покращувати алгоритми розпізнавання обличчя та відбитків пальців. Така архітектура забезпечує зручну взаємодію користувача з системою та гарантує високий рівень надійності при багаторівневій аутентифікації.

3.3 Аналіз функціонування системи та особливості багаторівневої аутентифікації

Після завершення розробки апаратної та програмної частини було проведено детальний аналіз роботи інтелектуальної системи контролю доступу з багаторівневою аутентифікацією користувачів. Основною метою цього етапу є перевірка надійності функціонування, стабільності взаємодії

компонентів та відповідності отриманих результатів поставленим вимогам. Тестування здійснювалося у реальних умовах з використанням кількох зареєстрованих користувачів, що дозволило оцінити ефективність роботи системи при різних сценаріях.

Розроблена система використовує три послідовні етапи ідентифікації: розпізнавання обличчя, перевірку відбитка пальця та введення персонального PIN-коду. Така багаторівнева структура дозволяє мінімізувати ризик несанкціонованого доступу та забезпечити достовірну перевірку користувача. Кожен рівень має свою унікальну функцію. Біометричні методи гарантують персоніфіковану ідентифікацію, а PIN-код виступає як додатковий засіб перевірки, що забезпечує ще один рівень захисту. Завдяки цьому система поєднує у собі простоту використання та високий рівень безпеки.

У ході аналізу було відзначено, що взаємодія між апаратними компонентами є стабільною та надійною. Камера ESP32-CAM забезпечує достатню якість зображення для розпізнавання навіть при зміні освітлення, а сенсор R307 демонструє високу точність визначення відбитків пальців. Затримки під час обміну даними відсутні, що свідчить про ефективну роботу інтерфейсів UART і GPIO, через які здійснюється обмін між модулями. Raspberry Pi виступає як центральний елемент керування, який координує процес аутентифікації, проводить обробку даних і відображає інформацію на екрані.

Під час тестування користувач проходить усі етапи перевірки, а система реагує послідовно та передбачувано. У випадку успішного розпізнавання обличчя та відбитка пальця на дисплеї відображається повідомлення «Авторизація», після чого система переходить до введення PIN-коду. Якщо користувач вводить правильний код, на екрані з’являється повідомлення про успішний доступ, а система переходить до головного меню. У разі невірного коду або невдалого розпізнавання користувач отримує повідомлення про помилку і може повторити спробу.

Середній час повного процесу аутентифікації становить близько 10 секунд, що включає етапи зчитування обличчя, перевірки відбитка пальця, введення PIN-коду та логічної обробки даних. Такий показник є оптимальним для систем контролю доступу подібного класу, де головну роль відіграє надійність, а не максимальна швидкість. При цьому система демонструє стабільну роботу без зависань чи помилок у процесі взаємодії між апаратними модулями.

Користувацький інтерфейс системи є інтуїтивно зрозумілим та ергономічним. На головному екрані відображається поточний стан системи, повідомлення про хід аутентифікації та результати перевірки. Після входу у головне меню користувач має можливість переглядати список зареєстрованих користувачів, додавати нові облікові записи або оновлювати свої біометричні дані. Завдяки такому підходу система є зручною для адміністрування і може бути масштабована для більшої кількості користувачів без втрати продуктивності.

Проведене тестування підтвердило, що розроблена система має високий рівень точності, стабільності та узгодженості роботи. Всі апаратні модулі функціонують синхронно, а програмна частина ефективно реалізує задану логіку багаторівневої аутентифікації. Отримані результати дозволяють стверджувати, що система здатна успішно виконувати свої функції в умовах реальної експлуатації зокрема, у приміщеннях із контрольованим доступом, навчальних лабораторіях або невеликих офісах, де важливо забезпечити персоніфікований контроль входу.

Таким чином, аналіз показав, що створена система на базі Raspberry Pi повністю відповідає поставленим вимогам і може бути використана як ефективне рішення для побудови сучасних інтелектуальних систем контролю доступу. Поєднання біометричних технологій та класичних методів ідентифікації робить її надійною, зручною у використанні та придатною для подальшого розвитку.

ВИСНОВКИ

У ході виконання роботи проведено комплексне дослідження сучасних технологій контролю доступу та методів аутентифікації користувачів. Аналіз існуючих систем показав, що традиційні однофакторні рішення вже не забезпечують належного рівня безпеки, а впровадження біометричних та комбінованих підходів є ключовою тенденцією розвитку інтелектуальних систем захисту. Це підтвердило актуальність обраної теми та необхідність розробки багаторівневої системи контролю доступу з використанням доступного апаратного забезпечення.

У рамках дослідження проведено аналіз методів аутентифікації, обрано апаратну платформу Raspberry Pi та додаткові модулі у вигляді камери ESP32-CAM, сенсора відбитків пальців R307 і сенсорний інтерфейс для введення PIN-коду. Це забезпечило створення гнучкої апаратної основи для побудови системи.

На етапі програмної реалізації розроблено алгоритм багаторівневої аутентифікації, який поєднує розпізнавання обличчя, ідентифікацію за відбитком пальця та перевірку PIN-коду. Забезпечено узгоджену взаємодію всіх компонентів, включаючи обробку зображення, роботу з шаблонами відбитків та логіку послідовної перевірки користувача. Створено інтерфейс, який дозволяє виконувати авторизацію, переглядати список користувачів та керувати параметрами доступу.

Проведене тестування системи підтвердило її працездатність, стабільність та відповідність поставленим вимогам. Середній час повної аутентифікації користувача становив близько 10 секунд, що є прийнятним показником для систем безпеки на базі мікрокомп’ютерів. Усі модулі продемонстрували коректну роботу, а інтегрований алгоритм забезпечив послідовну та надійну перевірку особи.

На основі отриманих результатів можна зробити висновок, що створена багаторівнева система контролю доступу є ефективним, практичним та

безпечним рішенням, яке може бути адаптоване для використання у навчальних, офісних та лабораторних приміщеннях. Завдяки модульності та відкритості програмної частини система має потенціал для подальшого розширення впровадження мережевих можливостей, віддаленого адміністрування та використання додаткових методів аутентифікації.

Отримані результати підтверджують доцільність використання Raspberry Pi та недорогих біометричних модулів для створення сучасних систем безпеки, а також демонструють перспективність подальшого розвитку таких рішень.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Будко Д., Боровик О., Костючко С. Система моніторингу ресурсів мережі на базі Raspberry PI. Технічні вісті 2025/1(61), 2(62). С. 66-68.

2. Сєдов А. В. Системи контролю доступу: навчальний посібник. К.: Ліра-К, 2020. 256 с.

3. Дьяков В. А. Технології біометричної ідентифікації. Харків: ХНУРЕ, 2021. 184 с.

4. OWASP Cheat Sheet Series. *Multifactor Authentication*. URL: https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html (дата звернення: 06.10.2025).

5. R. Alrawili, A. A. S. AlQahtani, M. K. Khan. Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion, ArXiv, 2023. URL: https://arxiv.org/abs/2311.13416 (дата звернення: 06.10.2025).

6. Михайленко В. І. Інформаційна безпека: захист даних у мережах. К.: Кондор, 2020. 312 с.

7. Biometric Update. Trends in Facial Recognition and Fingerprint Authentication. URL: https://www.biometricupdate.com (дата звернення: 07.10.2025).

8. J W. Jolles et al. Broad-scale Applications of the Raspberry Pi. Wiley, Methods in Ecology and Evolution, 2021. URL: https://besjournals.onlinelibrary.wiley.com/doi/10.1111/2041-210X.13652 (дата звернення: 07.10.2025).

9. OpenCV Documentation. Face Recognition Module. URL: https://docs.opencv.org (дата звернення: 08.10.2025).

10. Raspberry Pi Documentation. Security and Camera Integration. URL: https://www.raspberrypi.com/documentation/ (дата звернення: 09.10.2025).

11. Python.org. Python 3 Documentation. URL: https://docs.python.org (дата звернення: 09.10.2025).

12. Flask Documentation. Flask Web Framework. URL: https://flask.palletsprojects.com (дата звернення: 10.10.2025).

13. TensorFlow Documentation. TensorFlow for Image Processing. URL: https://www.tensorflow.org (дата звернення: 10.10.2025).

14. Keras Documentation. Deep Learning Models. URL: https://keras.io (дата звернення: 11.10.2025).

15. ESP32-CAM Module Facial Recognition Door Lock Security System (Journal of Engineering Technology and Innovation, 2024). URL: https://www.researchgate.net/publication/389894228_ESP32-CAM_Module_Facial_Recognition_Door_Lock_Security_System (дата звернення: 12.10.2025).

16. Microsoft Azure Documentation. Face API Overview. URL: https://learn.microsoft.com/azure/cognitive-services/face (дата звернення: 12.10.2025).

17. AWS Rekognition Documentation. Image and Face Analysis. URL: https://aws.amazon.com/rekognition/ (дата звернення: 12.10.2025).

18. Гнатюк С. О. Захист інформації в інформаційно-комунікаційних системах. К.: НАУ, 2020. 276 с.

19. NIST Special Publication 800-63B. Digital Identity Guidelines Authentication and Lifecycle Management. URL: https://pages.nist.gov/800-63-3/sp800-63b.html (дата звернення: 13.10.2025).

20. OpenAI Documentation. Face Recognition AI Ethics and Privacy. URL: https://openai.com/research (дата звернення: 14.10.2025).

21. Coursera. Introduction to Computer Vision with Python. URL: https://www.coursera.org/learn/computer-vision-basics (дата звернення: 15.10.2025).

22. Towards Data Science. Building a Facial Recognition System with OpenCV and Flask. URL: https://towardsdatascience.com (дата звернення: 16.10.2025).