Вінницький національний технічний університет
(повне найменування вищого навчального закладу)
Факультет інформаційних електронних систем
(повне найменування інституту, назва факультету (відділення))
Кафедра інформаційних радіоелектронних технологій і систем
(повна назва кафедри (предметної, циклової комісії))

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«РАДІОТЕХНІЧНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ З ІДЕНТИФІКАЦІЄЮ ОСОБИ»

Виконав: студент 2-го курсу, групи РТ-23м спеціальності 172 – Електронні комунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)
_____ Пехота Р.В.
(прізвище та ініціали)
Керівник: к.т.н., ст. викладач кафедри ІРТС
_____ Притула М. О.
(прізвище та ініціали)
«12» ____12____ 2024 р.
Опонент: к.т.н., доц. доцент каф. ІКСТ
_____ Семенова О.О.
(прізвище та ініціали)
«13» ____12____ 2024 р.

Допущено до захисту
Завідувач кафедри ІРТС
д.т.н., проф. Осадчук О.В.
(прізвище та ініціали)
«13» ____12____ 2024 р.

Вінниця ВНТУ - 2024 рік

Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інформаційних радіоелектронних технологій і систем
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань – 17 Електроніка, автоматизація та електронні комунікації
Спеціальність – 172 Електронні комунікації та радіотехніка
Освітньо-професійна програма – Радіотехніка

ЗАТВЕРДЖУЮ
Завідувач кафедри ІРТС
_____ д.т.н., проф. Осадчук О.В.
«14» вересня 2024 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Пехоті Роману Віталійовичу .
(прізвище, ім'я, по батькові)

1. Тема роботи. «Радіотехнічна система контролю доступу з ідентифікацією особи»
керівник роботи к.т.н., ст. викладач кафедри ІРТС Притула М. О.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від 17. 09.2024 р. №310.
2. Строк подання студентом роботи 13.12.2024р.
3. Вихідні дані до роботи: Напруга живлення - 3,3…12В. Струм споживання - 1…5А. Споживана потужність 20…25Вт. Двофакторна автентифікація. Діапазон температур: -10…+40^{0}С.
4. Зміст текстової частини: Вступ Аналіз систем контролю доступу з ідентифікацією особи. Дослідження методів ідентифікації особи: аналіз та порівняння. розробка системи контролю доступу з ідентифікацією особи. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу (з точним зазначенням обов'язкових креслень): Методи та способи ідентифікації особи. Модель розпізнавання обличчя. Структурна схема радіотехнічної системи контролю доступу з ідентифікацією особи. Перелік виводів Raspberry Pi5. Схема електрична принципова. Схема взаємодії між модулями. Datasheet характеристики модуля Rasberry Pi5. Фрагмент Datasheet характеристик модуля RFID&NFC PN532.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	виконання прийняв
Основна частина	ст. викладач кафедри ІРТС к.т.н., Притула М.О.		
Економічна частина	доцент каф. ЕПВМ, доцент, к.е.н., Кавецький В.В.		

7. Дата видачі завдання 16.09.2024 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Вибір, узгодження та затвердження тем МКР на випусковій кафедрі.	02.09.2024-07.09.2024	
2.	Огляд та аналіз літературних джерел.	08.09.2024-16.09.2024	
3.	Затвердження тем по ВНТУ. Розробка завдання на МКР.	17.09.2024-30.09.2024	
4.	Попередня розробка основних розділів. Аналіз вирішення поставленої задачі. Розробка структурної схеми та технічних рішень.	01.10.2024-20.10.2024	
5.	Математичне моделювання та електричні розрахунки. Експериментальне дослідження.	21.10.2024-04.11.2024	
6.	Розробка ілюстративної частини МКР.	05.11.2024-15.11.2024	
7.	Економічна частина.	16.11.2024-25.11.2024	
8.	Оформлення пояснювальної записки та ілюстративної частини.	26.11.2024-01.12.2024	
9.	Нормоконтроль.	02.12.2024-07.12.2024	
10.	Попередній захист МКР, доопрацювання, рецензування МКР.	09.12.2024-12.12.2024	
11.	Захист МКР ЕК.	14.12.2024-17.12.2024	

Студент _____ (підпис) Пехота Р.В.

Керівник роботи _____ (підпис) Притула М.О.

АНОТАЦІЯ

УДК 621.396.6

Пехота Р.В. Радіотехнічна система контролю доступу з ідентифікацією особи. Магістерська кваліфікаційна робота зі спеціальності 172 – Електронні комунікації та радіотехніка, освітня програма - радіотехніка. – Вінниця: ВНТУ, 2024. – 111с. На українській мові. Бібліогр.: 37 назв; Табл. 20; Рис. 21.

У магістерській кваліфікаційній роботі проведено дослідження та розробку радіотехнічної системи контролю доступу з ідентифікацією особи, що забезпечує двофакторну автентифікацію на основі RFID-ідентифікації та розпізнавання обличчя. У роботі виконано комплексний аналіз сучасних систем контролю доступу, їх класифікацію, визначено переваги та недоліки. Особливу увагу приділено порівнянню методів ідентифікації особи, включаючи біометричні технології, що довели свою ефективність у підвищенні рівня безпеки.

У ході виконання роботи розроблено структурну схему, апаратну частину та програмне забезпечення системи. Реалізація базується на використанні мікрокомп’ютера Raspberry Pi 5, модуля Pi Camera для розпізнавання обличчя, RFID-зчитувача PN532 та інших електронних компонентів. Алгоритми системи забезпечують інтеграцію всіх компонентів для ефективної ідентифікації осіб та надання доступу до об’єктів з обмеженим доступом.

Окрім технічної частини, у роботі виконано економічний розділ, який включає розрахунок витрат на реалізацію системи, оцінку її економічної ефективності та аналіз доцільності впровадження.

Ключові слова: система контролю доступу, двофакторна автентифікація, RFID, розпізнавання обличчя, Raspberry Pi, OpenCV.

ANOTATION

Pekhota R.V. Radio Engineering Access Control System with Person Identification. Master's Qualification Thesis in Specialty 172 – Electronic Communications and Radio Engineering, Educational Program - Radio Engineering. – Vinnytsia: VNTU, 2024. – 111 pages. In Ukrainian. Bibliography: 37 sources; Tables: 20; Figures: 21.

The master's qualification thesis presents a comprehensive study and development of a radio-technical access control system with person identification, implementing two-factor authentication based on RFID identification and facial recognition. The research includes a detailed analysis of modern access control systems, their classification, advantages, and disadvantages. Special attention is given to comparing identification methods, including biometric technologies, which have proven effective in enhancing security.

During the research, a structural diagram, hardware components, and software algorithms for the system were developed. The implementation is based on a Raspberry Pi 5 microcomputer, a Pi Camera module for facial recognition, an RFID reader PN532, and other electronic components. The algorithms ensure the integration of all components for effective identification and access control to restricted areas.

In addition to the technical part, the thesis includes an economic analysis, covering the calculation of implementation costs, evaluation of economic efficiency, and feasibility analysis. The results demonstrate that the developed system is not only a highly effective security solution but also an economically viable choice.

Keywords: access control system, two-factor authentication, RFID, facial recognition, Raspberry Pi, OpenCV, economic efficiency.

ЗМІСТ

ВСТУП

Актуальність

У сучасному світі зростає кількість об'єктів інфраструктури з обмеженим доступом, що створює нагальну потребу в забезпеченні їхньої безпеки та контролю доступу. В умовах підвищення ризиків несанкціонованого проникнення, захисту інформації та фізичних ресурсів особливо актуальним стає впровадження інноваційних систем контролю доступу. Використання двофакторної автентифікації, яка поєднує радіочастотну ідентифікацію (RFID) та розпізнавання обличчя, дозволяє досягти високого рівня надійності та функціональності системи. Такий підхід має вирішальне значення для об'єктів критичної інфраструктури, де потрібен посилений захист.

Мета роботи

Метою дослідження є розробка радіотехнічної системи контролю доступу з ідентифікацією особи, яка реалізує двофакторну автентифікацію на основі RFID-ідентифікації та технологій розпізнавання обличчя для підвищення рівня безпеки на об'єктах з обмеженим доступом.

Об'єкт дослідження

Об'єктом дослідження є радіотехнічні системи контролю доступу, призначені для забезпечення захисту об'єктів з обмеженим доступом.

Предмет дослідження

Предметом дослідження є методи двофакторної автентифікації, що включають використання RFID-ідентифікації та розпізнавання обличчя для контролю доступу.

Для досягнення поставленої мети у кваліфікаційній роботі розв'язуються наступні задачі

Для досягнення мети магістерської кваліфікаційної роботи, яка полягає у розробці радіотехнічної системи контролю доступу з ідентифікацією особи, у роботі вирішуються такі завдання.

– Проведення аналізу сучасних систем контролю доступу з ідентифікацією особи, включаючи їх класифікацію, переваги, недоліки та порівняння функціональних характеристик.

– Дослідження та порівняння методів ідентифікації особи, особливу увагу приділяючи біометричним технологіям, які забезпечують підвищений рівень безпеки.

– Розробка структурної схеми, апаратної частини та програмного забезпечення для створення ефективної системи контролю доступу.

– Виконання економічного обґрунтування розробки, включаючи розрахунок витрат, аналіз доцільності впровадження системи та її економічної ефективності.

Методи дослідження

– Для досягнення мети в роботі застосовуються такі методи.

– Аналіз та синтез — для вивчення існуючих систем контролю доступу та вибору оптимальних методів автентифікації.

– Моделювання — для розробки алгоритмів роботи радіотехнічної системи.

– Експериментальні дослідження — для перевірки ефективності розробленої системи в реальних умовах.

– Системний підхід — для комплексного оцінювання впливу запропонованих технологій на загальний рівень безпеки.

Наукова новизна

Наукова новизна роботи полягає у розробці інтегрованої радіотехнічної системи контролю доступу, яка вперше поєднує RFID-ідентифікацію та розпізнавання обличчя для забезпечення двофакторної автентифікації. Запропонована система вирізняється високою надійністю, гнучкістю та здатністю адаптуватися до різних умов експлуатації.

Практичне значення одержаних результатів

Запропонована система може бути використана для забезпечення безпеки на об'єктах різного призначення, включаючи державні установи, промислові

підприємства та інші об'єкти з обмеженим доступом. Реалізація двофакторної автентифікації дозволить:

– підвищити рівень захисту від несанкціонованого доступу;

– забезпечити точну ідентифікацію персоналу;

– спростити інтеграцію із сучасними системами моніторингу та управління;

– оперативно реагувати на надзвичайні ситуації.

Результати роботи сприятимуть вдосконаленню сучасних систем контролю доступу, що є особливо актуальним для забезпечення безпеки об'єктів із підвищеними вимогами до захисту в Україні.

Особистий внесок здобувача

Основні положення і результати магістерської кваліфікаційної роботи отримані автором практично самостійно.

Структура і обсяг роботи

Магістерська кваліфікаційна робота складається з 4 розділів, висновків, додатків та списку використаних джерел.

1 АНАЛІЗ СИСТЕМ КОНТРОЛЮ ДОСТУПУ З ІДЕНТИФІКАЦІЄЮ ОСІБ

1.1 Класифікація систем контролю доступу

Системи контролю доступу (СКД) представляють собою інноваційні технологічні рішення, спрямовані на організацію та моніторинг доступу до певних об’єктів, приміщень, ресурсів або інформаційних масивів. Їх головною метою є забезпечення захисту від несанкціонованого проникнення, зниження ризиків викрадення, втрати даних або інших порушень безпеки. Ці системи знайшли широке застосування в багатьох галузях, включаючи фізичну охорону будівель, захист комп’ютерних мереж, збереження даних, управління транспортними потоками та інші сфери, де потрібен ретельний контроль доступу до обмежених зон або ресурсів [1].

СКД, як правило, функціонують на основі поєднання апаратних засобів і програмного забезпечення. Це дозволяє створювати комплексні рішення для організації безпеки, які забезпечують контроль входу-виходу осіб або транспортних засобів через визначені точки, такі як двері, турнікети або шлагбауми. Водночас системи не тільки обмежують доступ, але й ведуть повний облік дій користувачів, що дає змогу виявляти та попереджувати можливі спроби порушення безпеки.

Сучасні СКД функціонують у двох основних форматах. Фізичний контроль доступу та логічний контроль.

1. Фізичний контроль доступу спрямований на регулювання входу до будівель, приміщень, складів або доступу до фізичних активів, наприклад, серверних кімнат чи сейфів. Цей тип контролю ефективний для запобігання проникненню неавторизованих осіб у зони з обмеженим доступом.

2. Логічний контроль доступу забезпечує захист від несанкціонованого підключення до інформаційних систем, баз даних чи комп’ютерних мереж. Він

запобігає доступу сторонніх осіб до конфіденційної інформації, використовуючи методи ідентифікації, автентифікації та авторизації.

Для підвищення ефективності СКД використовуються електронні системи, які базуються на застосуванні інформації про користувачів, таких як RFID-картки [2], біометричні дані, або PIN-коди. Вони інтегруються із сенсорними пристроями для зчитування інформації, панелями управління доступом, а також із додатковими системами сигналізації та засобами блокування. Такий підхід дозволяє створити багаторівневу інфраструктуру захисту, яка моніторить доступ, попереджає несанкціоновані спроби проникнення та веде аудити для аналізу безпеки.

Класифікація систем контролю доступу СКД поділяються на кілька основних категорій за різними параметрами.

3. Метод управління доступом.

– Біометричні системи використовують фізіологічні характеристики користувачів (відбитки пальців, райдужну оболонку ока тощо), що ускладнює їх підробку та забезпечує високий рівень безпеки.

– Мережеві системи працюють у централізованому режимі, дозволяючи керувати доступом дистанційно, інтегруватися з іншими системами (відеоспостереження, охоронна сигналізація) та гнучко налаштовувати політику доступу.

– Автономні системи не потребують підключення до мережі та працюють незалежно. Вони зручні для невеликих об'єктів, але не забезпечують функцій обліку робочого часу.

– Універсальні системи поєднують переваги автономних та мережевих рішень, працюючи як в автономному, так і в централізованому режимах.

4. Рівень ідентифікації.

– Однорівневі системи базуються на використанні одного параметра ідентифікації, наприклад, RFID-картки.

– Багаторівневі системи застосовують кілька параметрів, таких як поєднання PIN-коду та біометричних даних.

5. Кількість точок доступу.

- Малої ємності – до 80 точок.
- Середньої ємності – від 80 до 250 точок.
- Великої ємності – понад 256 точок.

Переваги СКД.

СКД не тільки забезпечують захист, але й дозволяють автоматизувати бізнес-процеси, пов’язані з управлінням доступом і обліком часу роботи. Інтеграція таких систем із бухгалтерськими програмами сприяє точному розрахунку заробітної плати, а взаємодія з системами відеоспостереження підвищує оперативність реагування на порушення.

Недоліки СКД.

Деякі СКД можуть бути складними в налаштуванні та інтеграції. Також існує необхідність у постійному оновленні програмного забезпечення та технічному обслуговуванні, що може потребувати додаткових витрат [3].

Таким чином, системи контролю доступу є багатофункціональними інструментами, які відіграють ключову роль у забезпеченні безпеки та оптимізації управління доступом. Їх вибір залежить від розміру об’єкта, кількості користувачів, специфіки діяльності та рівня безпеки, якого прагнуть досягти.

1.2 Аналіз сучасних систем контролю доступу

Системи контролю доступу виконують ключову роль у забезпеченні безпеки, виконуючи такі важливі завдання, як ідентифікація, автентифікація та авторизація користувачів або об’єктів. Їх функціонування базується на аналізі певних параметрів, наданих для отримання доступу, зокрема PIN-кодів, паролів, RFID-карток, біометричних даних чи інших маркерів безпеки. Застосування таких систем охоплює різноманітні сфери, включаючи фізичну охорону будівель, комп’ютерні мережі, громадський транспорт та інші галузі, де необхідно забезпечити обмеження доступу тільки для авторизованих користувачів.

Ідентифікація є першим і важливим етапом у процесі доступу до системи. Вона полягає у визначенні особи або об’єкта на основі заздалегідь відомої інформації, наприклад, ідентифікатора чи інших попередньо збережених даних. Цей етап слугує основою для подальшої автентифікації та авторизації. У процесі ідентифікації користувач або суб’єкт системи повідомляє свій унікальний параметр, наприклад, логін, який порівнюється з інформацією у системі. У разі успішного співпадіння система переходить до автентифікації, під час якої підтверджується, що суб’єкт є тим, за кого він себе видає, наприклад, через введення пароля або іншого секретного коду.

Одним із важливих елементів захисту в цифрових системах [4] є цифровий підпис, який представлений у вигляді послідовності бінарних даних. Цей підпис гарантує автентичність особи, яка його створила, та цілісність даних. Генерація цифрового підпису здійснюється за допомогою приватного ключа, а його перевірка – за допомогою відкритого ключа. Кожен користувач володіє унікальною парою ключів, що забезпечує високий рівень безпеки, оскільки приватний ключ залишається конфіденційним, а відкритий використовується для верифікації підпису.

Автентифікація є наступним етапом, спрямованим на підтвердження правомірності доступу до системи. Вона дозволяє переконатися, що користувач, який звертається до системи, має право на доступ. Цей процес включає перевірку введеного логіну та пароля шляхом порівняння їх із даними, збереженими в базі системи. При успішній автентифікації виконується авторизація – процес надання користувачеві доступу до певних функцій або ресурсів системи.

Існує кілька типів автентифікації.

1. Однофакторна автентифікація [5] базується на використанні одного параметра, наприклад, пароля. Цей метод є простим, але менш захищеним, оскільки паролі можуть бути втрачені або вкрадені.

2. Багатофакторна автентифікація (MFA) передбачає застосування двох або більше методів підтвердження, наприклад, пароля та фізичного токена або біометричних даних. Це забезпечує вищий рівень захисту.

3. Посилена автентифікація використовується для операцій із підвищеними вимогами до безпеки, наприклад, у фінансових системах, де необхідні різні типи факторів для підтвердження.

4. Сувора автентифікація базується на використанні асиметричної криптографії, яка передбачає створення пари ключів (приватного та відкритого) для підпису та перевірки.

Фактори автентифікації поділяються на три основні категорії.

– Фактор знання включає паролі, PIN-коди, відповіді на контрольні запитання. Вони залежать від пам’яті користувача, що робить їх вразливими до підбору чи викрадення.

– Фактор володіння передбачає використання фізичних об’єктів, таких як RFID-картки, ключі, смартфони [6]. Ці предмети забезпечують додатковий рівень захисту, оскільки їх складніше підробити.

– Фактор властивості базується на унікальних фізіологічних або поведінкових характеристиках, таких як відбитки пальців, розпізнавання обличчя чи голосу.

Авторизація – це заключний етап, під час якого визначається рівень доступу користувача до ресурсів системи. Вона встановлює, які саме функції чи операції дозволено виконувати користувачеві. Авторизація є важливим елементом забезпечення інформаційної безпеки, оскільки дозволяє контролювати дії користувачів та захищати ресурси від несанкціонованого використання.

Таким чином, системи контролю доступу є комплексним інструментом, що забезпечує багаторівневий захист через використання ідентифікації, автентифікації та авторизації. Їх ефективність залежить від використання сучасних методів перевірки доступу та інтеграції з іншими системами безпеки.

1.3 Переваги та недоліки сучасних систем контролю доступу

Принцип роботи системи контролю доступу (СКД) полягає у забезпеченні процесу перевірки та прийняття рішень щодо надання чи обмеження доступу до певних об’єктів, зон або територій. Для цього використовується спеціалізоване обладнання, яке дозволяє зчитувати дані з ідентифікатора, наприклад, пластикової картки, електронного брелока або біометричних даних користувача. Зчитана інформація передається на електронний пристрій, де вона порівнюється із записами у базі даних. Після перевірки система приймає рішення про надання доступу або його блокування. Загальна логічна схема побудови системи контролю та управління доступом подана на рисунку 1.1.

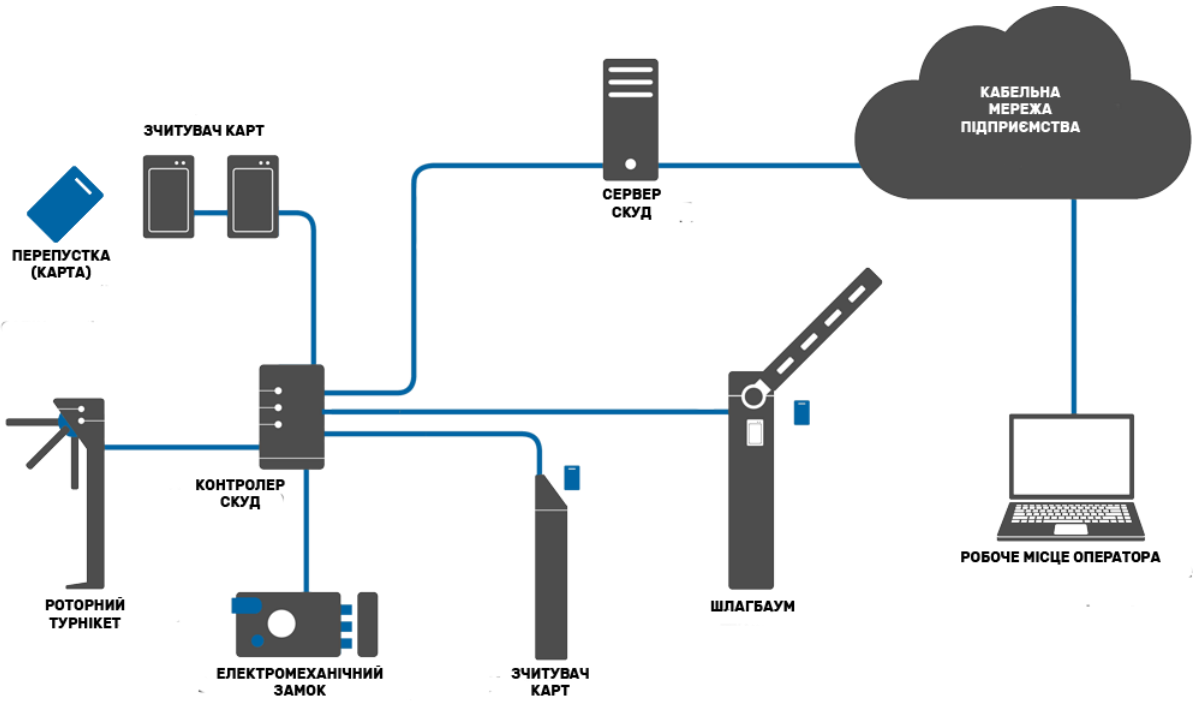

Рисунок 1.1 – Загальна схема СКУД

Для побудови та функціонування СКД необхідна інтеграція кількох ключових компонентів.

– Ідентифікатор – це основний носій інформації, що може бути представлений у вигляді пластикової картки, брелока, коду, або біометричних параметрів (відбитки пальців, розпізнавання обличчя тощо).

– Зчитувач – пристрій, призначений для отримання даних із ідентифікатора. Він забезпечує передачу зчитаної інформації на контролер.

– Контролер – головний модуль, який обробляє інформацію, отриману від зчитувача, та приймає рішення про надання доступу.

– Персональний комп’ютер та програмне забезпечення – використовується для управління всією системою, ведення баз даних користувачів, генерації звітів і налаштування політик доступу.

– Додаткові пристрої та механізми – турнікети, замки, адаптери та інше обладнання, яке фізично регулює доступ до зони.

Основна мета впровадження СКД полягає в управлінні доступом до об’єкта або території, що реалізується за допомогою таких функцій.

1. Обмеження доступу – забезпечення захисту визначеної території від проникнення неавторизованих осіб.

2. Ідентифікація користувача – перевірка прав доступу конкретного користувача, використовуючи його ідентифікатор.

Крім основних завдань, СКД виконують низку додаткових функцій, що дозволяють значно розширити їх можливості.

– Фіксація часу перебування працівників на робочому місці для подальшого документування.

– Інтеграція з бухгалтерськими системами для автоматизації розрахунку заробітної плати.

– Ведення баз даних персоналу та відвідувачів для спрощення управління доступом.

– Співпраця із системами безпеки, такими як.

1. Система відеоспостереження – синхронізує архіви подій, відправляє команди для початку запису під час виявлення підозрілих дій та дозволяє повертати камери для документування інцидентів.

2. Охоронна сигналізація (ОС) – контролює доступ до охоронюваних об’єктів, може автоматично ставити або знімати приміщення з охорони.

3. Пожежна сигналізація (ПС) – реагує на спрацювання пожежних сповіщувачів, розблоковує евакуаційні виходи, закриває протипожежні двері для захисту людей та майна.

Загальна логічна схема побудови системи контролю та управління доступом подана на рисунку 1.1.

Таким чином, СКД [7] є не лише засобом для контролю доступу, але й потужним інструментом для автоматизації, моніторингу та інтеграції з іншими системами безпеки, що забезпечує всебічний захист об’єкта.

Процес функціонування системи контролю доступу виглядає наступним чином: поблизу входу до об'єкта з обмеженим доступом встановлюються спеціальні пристрої - зчитувачі, призначені для отримання інформації з ідентифікатора, введення пароля або кодового числа, а також для збору біометричних даних особи. Отримана інформація подається на контролери доступу, які, аналізуючи дані власника, забезпечують управління різними пристроями, такими як відкриття або блокування дверей, активація сигналізації, фіксація присутності особи на робочому місці і інші дії.

Отже, система контролю та управління доступом є необхідним елементом повноцінних рішень забезпечення високого рівня безпеки на об'єкті. Принципи функціонування СКУД надають можливість виконувати жорсткий контроль за рухом та доступом в межах визначеної зони.

1.4 Порівняння функцій системи контролю доступу

Система контролю та управління доступом (СКУД) виконує комплекс важливих функцій, які забезпечують її ефективну роботу.

– Санкціонування – надання користувачам унікального ідентифікатора, пароля або реєстрація їхніх біометричних даних. Цей процес включає введення інформації про користувача до бази даних системи для подальшого управління доступом.

– Налаштування часових інтервалів і рівнів доступу – встановлення для кожного користувача обмежень за часом і визначення рівня доступу. Це дозволяє точно регулювати, хто, куди і коли має право потрапити.

– Ідентифікація – процес розпізнавання користувача за його ідентифікатором або біометричними характеристиками, які зберігаються в системі.

– Авторизація – перевірка прав доступу користувача. Вона включає звірку наданого ідентифікатора або біометричних даних з рівнем доступу та часовими обмеженнями, визначеними в процесі санкціонування.

– Автентифікація – підтвердження автентичності користувача за його унікальними ознаками. Цей етап забезпечує впевненість у тому, що доступ намагається отримати саме зареєстрований користувач.

– Прийняття рішення – автоматичний аналіз результатів ідентифікації, авторизації та автентифікації для надання доступу або його блокування.

– Реєстрація дій – фіксація всіх дій у системі, включаючи успішні входи, відмови в доступі, спроби порушення правил. Ця інформація використовується для аналізу, звітності та виявлення потенційних загроз.

– Реагування на порушення – система автоматично виконує дії у разі виявлення несанкціонованих спроб доступу, такі як подача тривожного сигналу, активація блокування або інформування персоналу про інцидент.

Процес санкціонування [8], який визначає, хто і на яких умовах може отримати доступ, зазвичай виконується оператором або адміністратором системи. Решта функцій, таких як ідентифікація, авторизація чи реагування на порушення, можуть бути автоматизованими, що підвищує ефективність СКУД.

Важливо зазначити, що повноцінна процедура автентифікації найбільш ефективно виконується за допомогою біометричних систем, які забезпечують високий рівень захисту завдяки використанню унікальних фізіологічних або поведінкових характеристик користувача.

1.5 Висновки до розділу

У даному розділі розглянуто основні принципи та функції систем контролю та управління доступом (СКУД), а також ключові етапи, які система має виконувати для забезпечення ефективного захисту та управління доступом до об'єктів чи ресурсів.

Основною метою СКУД є забезпечення безпеки через контроль доступу до обмежених територій, приміщень або інформаційних ресурсів. Для цього використовуються різні методи ідентифікації, автентифікації та авторизації користувачів. У ході процесу санкціонування кожному користувачеві присвоюється унікальний ідентифікатор або біометричні ознаки, що дозволяє відслідковувати доступ до ресурсів і територій.

Крім основних функцій, таких як обмеження доступу та ідентифікація, СКУД виконують додаткові завдання, що сприяють інтеграції з іншими системами безпеки, такими як відеоспостереження або охоронна сигналізація. Це забезпечує більш комплексний підхід до захисту об’єкта або території, дозволяючи своєчасно реагувати на порушення.

Автентифікація, як частина системи, відіграє важливу роль у перевірці правомірності користувача, причому цей процес може включати різні рівні захисту, залежно від типу системи. Системи, що використовують біометричні методи, забезпечують високий рівень безпеки, оскільки біометричні ознаки важко підробити, що робить систему більш надійною.

Загалом, СКУД є важливим інструментом для забезпечення безпеки на об’єктах з обмеженим доступом, який дозволяє організувати ефективний контроль та моніторинг доступу до ресурсів, а також своєчасно виявляти та попереджати спроби несанкціонованого проникнення. Інтеграція з іншими системами безпеки та автоматизація процесів дозволяє значно підвищити рівень захисту, знижуючи людський фактор та оперативно реагуючи на потенційні загрози.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ІДЕНТИФІКАЦІЇ ОСОБИ. АНАЛІЗ ТА ПОРІВНЯННЯ

2.1 Аналіз сучасних методів ідентифікації осіб

Ідентифікація об'єкта являє собою процес встановлення зв’язку з конкретною особою чи об'єктом для визначення їх належності до певної категорії чи групи. У контексті інформаційних технологій термін "ідентифікація" стосується процесу визначення особи користувача в системі. Це перший і важливий етап, який дозволяє системі прийняти рішення про надання доступу до ресурсів, таких як комп'ютери, конфіденційні дані або інші обмежені зони. Ідентифікація є основою для подальших процедур безпеки та є невід'ємною частиною інформаційної безпеки в будь-яких інформаційних системах. основні методи ідентифікації зображено на рисунку 2.1.

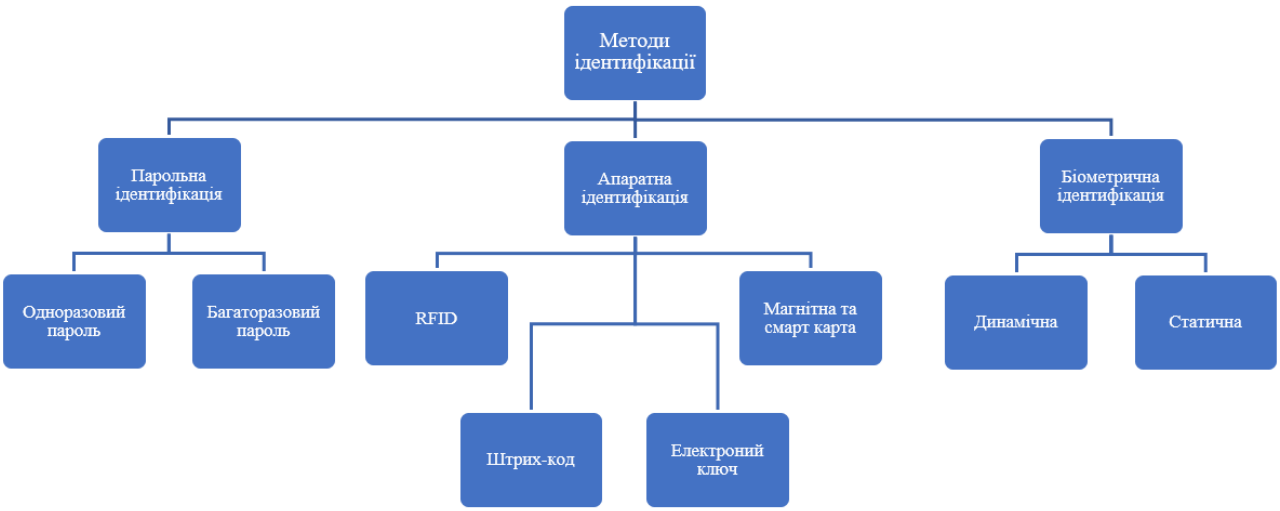

Рисунок 2.1 – класифікація методів ідентифікації

Сучасні технології пропонують кілька методів ідентифікації користувачів, кожен з яких має свої переваги та недоліки. Залежно від специфіки застосування, ці методи можуть бути більш або менш підходящими

для різних типів систем. Відзначаються три основні методи ідентифікації, кожен з яких використовується відповідно до вимог безпеки та зручності для користувача.

Парольна ідентифікація тривалий час вважалася основним методом підтвердження особистості користувача, оскільки цей метод є простим у впровадженні та використанні в повсякденному житті. Коли користувач реєструється в системі, йому надається набір особистих даних, зокрема логін і пароль. Щоразу, намагаючись увійти, користувач повинен ввести ці дані, і система, порівнюючи введені параметри з наявними в базі, визначає особистість користувача [9].

Основною перевагою парольної ідентифікації є її легкість у впровадженні та низькі витрати на використання. Цей метод активно застосовується в усіх інформаційних системах і мережах. Однак, він має й суттєві недоліки: його надійність значною мірою залежить від користувачів, адже вони повинні створювати складні паролі, що не завжди дотримується; окрім того, багато користувачів не можуть запам’ятати складні паролі, що може призвести до їх втрати або запису на ненадійних носіях, що ставить під загрозу рівень безпеки.

Апаратна ідентифікація здійснюється шляхом розпізнавання особи користувача через певний фізичний об'єкт, який знаходиться у нього в руках. Існує два основних види таких пристроїв: карткові та токени. Карткові ключі, як магнітні або смарт-карти, вважаються менш надійними для ідентифікації через їх вразливість до копіювання інформації та схильність до механічних пошкоджень. Однак їх основною перевагою є простота використання та реалізації.

Токени, що є пристроями з вбудованою пам'яттю та можливістю підключення до зовнішніх портів USB, забезпечують вищий рівень надійності, оскільки їх можна використовувати для двофакторної ідентифікації. У цьому випадку користувач спочатку надає токен, який генерує ключі (наприклад, відкритий і закритий), а потім вводить пароль або виконує іншу дію для підтвердження своєї особистості. Головною перевагою токенів є висока надійність цього методу. Однак цей підхід має й недоліки: токен можна

втратити чи вкрасти, а також його впровадження потребує додаткових витрат на обладнання та налаштування системи [10].

Види ідентифікаторів зображено на рисунку 2.2.

Рисунок 2.2 – Типи ідентифікаторів: а) –браслет б) – картка в, г) – брелок

Окрім широко використовуваних методів ідентифікації, таких як біометричні дані та паролі, існують також інші технології апаратної ідентифікації, серед яких можна виділити штрихкодову та радіочастотну ідентифікацію (RFID). Штрихкодова ідентифікація здебільшого застосовується для маркування товарів у роздрібній торгівлі, проте її можна використовувати й для ідентифікації осіб. Головною перевагою цього методу є його простота у впровадженні та використанні, проте він має низку суттєвих недоліків: зокрема, інформація в штрих-коді відкрито зберігається, що робить її вразливою до підробки.

Метод радіочастотної ідентифікації (RFID) базується на використанні двох основних пристроїв: зчитувача та RFID-мітки, яка містить необхідну інформацію для ідентифікації особи. Коли користувач наближається до зони дії зчитувача, мітка автоматично передає свої дані за допомогою радіосигналів. Одна з головних переваг цього методу полягає в тому, що він не потребує прямого контакту, є простим у використанні та забезпечує високу швидкість ідентифікації. Однак, цей метод має свої недоліки, зокрема, він чутливий до

сильних радіоінтерференцій, що може порушити роботу системи, а також він потребує значних витрат на впровадження і можливість крадіжки RFID-міток для неправомірного використання.

2.2 Біометричні методи розпізнавання особи

Біометрична ідентифікація є більш сучасним і надійним методом, що передбачає використання унікальних біологічних ознак людини, таких як відбитки пальців, райдужка ока або структура обличчя [11]. Це дозволяє забезпечити високу точність ідентифікації, оскільки біометричні ознаки є унікальними для кожної людини. Історія біометрії налічує кілька століть і розпочалась із використання відбитків пальців у криміналістиці, а з часом розвинулася в складну технологію ідентифікації особистості.

Перевагою біометричної ідентифікації є її висока надійність, оскільки біометричні параметри важко підробити, і ці ознаки неможливо забути чи втратити, як це може статися з паролем або карткою доступу [12]. Це робить біометричні системи найбільш безпечним методом підтвердження особи. Однак, такі системи мають і певні недоліки, серед яких висока вартість впровадження та необхідність в обробці великих обсягів даних. Незважаючи на ці недоліки, біометрична ідентифікація залишається одним з найбільш ефективних і надійних методів, особливо коли її використовують у поєднанні з іншими технологіями, такими як картки доступу чи паролі.

На сьогоднішній день існує кілька біометричних методів, включаючи відбитки пальців, розпізнавання обличчя, голосу, райдужки ока, а також методи, що вивчають поведінкові ознаки, такі як малюнок підпису чи динаміка набору тексту. Розвиток технологій дозволяє постійно вдосконалювати ці методи, підвищуючи точність і знижуючи вартість їх впровадження. Зображення методів та способів ідентифікації особи наведено на рисунку 2.3.

Ідентифікація особи за допомогою біометричних характеристик може здійснюватися двома основними методами.

Фізіологічна ідентифікація базується на використанні стабільних фізіологічних ознак людини, таких як відбитки пальців, форма обличчя, структура райдужки ока та інші. Ці характеристики залишаються незмінними протягом всього життя, що робить їх надійним інструментом для ідентифікації.

Поведінкова ідентифікація [13], у свою чергу, використовує біометричні ознаки, що проявляються під час виконання певних дій. Це можуть бути, наприклад, особливості ходи, підпис, голосові інтонації та інші динамічні характеристики. Однак, порівняно з фізіологічними методами, поведінкова ідентифікація має меншу надійність через можливі зміни в поведінці людини залежно від зовнішніх умов або стану здоров’я.

Рисунок 2.3 – Методи та способи ідентифікації особи

Завдяки значному прогресу в медичних та технологічних дослідженнях було виявлено ряд нових біометричних ознак, які можна ефективно використовувати для ідентифікації особи. Окрім традиційно використовуваних методів, таких як відбитки пальців і голосова ідентифікація, до сучасних методів належать.

– Розпізнавання райдужної оболонки ока. Цей метод вважається одним із найточніших завдяки унікальності райдужної оболонки кожної людини. Райдужна оболонка є стабільною і незмінною протягом життя, що робить її чудовим маркером для ідентифікації. Цей метод має високу точність, оскільки навіть двоє однояйцевих близнюків мають різні ознаки райдужки ока.

– Геометрія обличчя. Ідентифікація за допомогою тривимірної структури обличчя є ще одним прогресивним методом. Застосування 3D-технологій дозволяє точно визначити індивідуальні риси обличчя, такі як відстань між очима, форма носа, щелепи та інших ключових рис. Цей метод також є дуже надійним, оскільки обличчя не змінюється радикально протягом життя.

– Відбитки долоні. Подібно до відбитків пальців, кожна людина має унікальний малюнок ліній на долоні. Використання цього методу ідентифікації стало популярним завдяки своїй точності, оскільки структура ліній на долоні так само унікальна, як і відбитки пальців. Цей метод також часто використовується у сферах, де потрібно забезпечити високий рівень безпеки.

– ДНК. Це найбільш точний метод ідентифікації, оскільки ДНК кожної людини є абсолютно унікальним. Однак його застосування обмежене через складність процедури збору зразків та високу вартість. У практичному застосуванні цей метод найчастіше використовують у криміналістиці та в судово-медичних розслідуваннях.

Точність і надійність біометричних методів визначається цілим рядом факторів, серед яких можна виділити якість отриманих зображень або сканів, умови збору даних, а також ефективність алгоритмів розпізнавання. Найбільш точні результати зазвичай отримують методи, що працюють із статичними біометричними ознаками, такими як райдужна оболонка ока або відбитки пальців [14]. Ці ознаки є постійними та малочутливими до зовнішніх факторів. Натомість динамічні біометричні ознаки, наприклад, голос чи підпис, можуть мати більшу чутливість до змін навколишнього середовища або фізичного стану людини.

Основною перевагою біометричної ідентифікації є її здатність

використовувати унікальні характеристики, притаманні лише одній людині, що робить ймовірність збігу таких ознак між двома різними особами надзвичайно низькою. Завдяки цьому біометрія забезпечує високу надійність і точність процесу ідентифікації, що робить її найефективнішим методом забезпечення безпеки в сучасних системах.

Методи біометричної ідентифікації наведено в таблиці 2.1.

Таблиця 2.1 – Методи біометричної ідентифікації

Фізіологічні методи	Психологічні методи
за відбитками пальців	за голосом
за формою долоні	за підписом
за сітчаткою ока	за почерком
за геометрією обличчя	за клавіатурним почерком
за розташуванням вен на лицьовій стороні долоні	
за термограмою обличчя (розташування вен та судин під шкірою обличчя)	
за райдужною оболонкою ока	
за геометрією вуха	
за допомогою ДНК	

Ймовірність того, що дві особи матимуть однакові відбитки пальців на однакових пальцях руки, є надзвичайно низькою і становить лише 1 на 24 мільйони. Це свідчить про унікальність відбитків пальців у кожної людини. Основні характеристики різних методів ідентифікації наведені в таблиці 2.2.

Фізіологічні та психологічні методи ідентифікації тісно взаємопов'язані і взаємодоповнюють один одного, що дозволяє підвищити точність процесу. Статичні методи, на відміну від динамічних, не залежать від психологічного стану користувача, потребують мінімальних зусиль з його боку і тому є дуже ефективними для обробки великих обсягів даних, наприклад, для

ідентифікації великої кількості людей одночасно.

Таблиця 2.2 – Основні характеристики методів біометричної ідентифікації

Метод біометричної ідентифікації	Відмова СКУД у %	Помилка розпізнавання у %
Геометрика лодоні	менше за 4	менше 1
Відбиток пальця	2-6	мінімальна
Сітківка ока	мінімальна	до 8
Райдужка ока	менше за 2	мінімальна
Обличчя	До 7	менше 5
Звичайний почерк	до 5	5
Клавіатурний почерк	Від 3 до 10	10
Голос	до 5	5

Психологічні (динамічні) методи біометричної ідентифікації, як правило, є менш складними у впровадженні, оскільки часто не потребують використання дорогого обладнання. Для їх реалізації достатньо наявності програмного забезпечення, яке не вимагає складного технічного обслуговування або частих налаштувань.

Основні статичні біометричні характеристики та їх реалізаця наведена в таблиці 2.3.

Таблиця 2.3 – Реалізація статичних ознак

Біометричний показник	Пристрій для зчитування	Зразок біометричної характеристики	Об'єкт дослідження
Геометрична будова руки	Настінний пристрій	Графічне зображення кисті, яке включає в себе тривимірні представлення зверху та з боків.	Висота і ширина кісток і суглобів кисті і пальців

Продовження таблиці 2.3 – Реалізація статичних ознак

Відбитки пальців	Периферійний пристрій для настільного комп'ютера, PC card стандарту, миша, мікросхема або зчитувальний пристрій, інтегрований в клавіатуру.	Зображення відбитка пальця, отримане за допомогою оптичного методу, кремнієвого фотоприймача, ультразвукової технології або безконтактного способу.	Розташування та напрямок гребінчастих виступів і розгалужень на відбитку пальця, а також дрібні характеристики та особливості.
Сітківка ока	Настільний або настінний пристрій	Зображення сітківки ока	Розташування кровоносних судин
Райдужна оболонка ока	Відеокамера, здатна працювати в інфрачервоному діапазоні, камера для ПК	Чорно-біле зображення райдужної оболонки ока	Смужки і борозенки на райдужній оболонці ока
Обличчя	Відеокамера, камера для ПК, фотоапарат	Зображення особи (оптичне або теплове)	Візуальні особливості обличчя, відносне розташування і форма носа, розташування вилиць

Біометрична ідентифікація за формою кисті руки – це метод ідентифікації особи, заснований на унікальних геометричних характеристиках кисті руки. Цей підхід ґрунтується на припущенні, що форма та розміри кисті кожної людини є індивідуальними та не змінюються протягом життя.

Для ідентифікації використовуються такі основні характеристики.

Геометричні ознаки.

- Довжина і ширина пальців
- Об’єм кисті
- Відстані між суглобами
- Кути між пальцями та долонею

– Форма контуру долоні

Візуальні ознаки.

– Відбитки шкіри на з'єднаннях фаланг пальців

– Візерунки кровоносних судин

Для кращого розуміння процесу ідентифікації на рисунку 2.4 представлено зображення долоні, на якому виокремлено основні лінії, контрольні точки та геометричні ознаки, що використовуються в цьому методі.

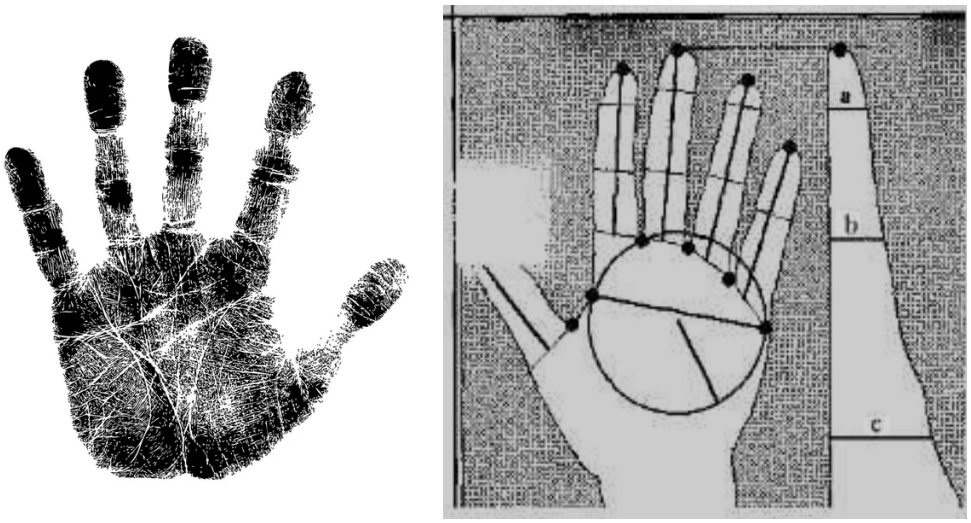

Рисунок 2.4 – Відбиток долоні та її структура

Для ідентифікації за геометричними характеристиками руки використовуються різноманітні технології, зокрема комп'ютерний зір, 3D-сканування та алгоритми машинного навчання. Ці методи дозволяють точно визначити унікальні параметри кисті руки, які використовуються для ідентифікації особи.

Розпізнавання відбитків пальців є одним з найпоширеніших та найбільш надійних способів біометричної ідентифікації. Воно ґрунтується на детальному аналізі унікальних рис папілярних ліній, які формуються на поверхні шкіри пальців. Зображення масиву відбитків пальців наведено на рисунку 2.5. Процес ідентифікації за допомогою відбитків пальців складається з кількох етапів.

Рисунок 2.5 – Масив відбитків пальців

1. Збір даних [15]. Спочатку використовується спеціалізоване обладнання, яке створює високоякісне зображення відбитка пальця. Сучасні сканери застосовують різні технології для отримання зображення, серед яких:

– Оптична технологія, що використовує світло для зняття зображення;

– Капацитивна технологія, яка вимірює електричні зміни на поверхні шкіри;

– Акустична технологія, що використовує ультразвукові хвилі для зчитування відбитка;

– Ультразвукова технологія, яка забезпечує високу точність, оскільки дозволяє детально фіксувати структуру шкіри.

Кожна з цих технологій має свої переваги, але всі вони дозволяють створити високоякісне, чітке зображення відбитка пальця, що є основою для подальшої обробки.

2. Обробка зображення. Після отримання зображення відбитка пальця, воно піддається обробці для виділення характерних ознак. Зокрема, ідентифікуються такі особливості, як:

– кінцеві точки ліній, які є важливими маркерами;

– точки розгалуження, де лінії змінюють свій напрямок;

– загальний візерунок папілярних ліній, який унікальний для кожної особи.

Ці біометричні ознаки залишаються незмінними протягом усього життя людини, що робить розпізнавання відбитків пальців надзвичайно точним і надійним методом ідентифікації.

На основі виявлених характеристик відбитка пальця створюється математична модель або шаблон, що відображає унікальні особливості цього відбитка. Цей шаблон зберігається в електронній базі даних для подальшого використання.

Для процесу ідентифікації під час перевірки отриманий відбиток пальця порівнюється з шаблонами, які вже є в базі даних. Спеціалізовані алгоритми обчислюють рівень схожості між новим відбитком і вже збереженими шаблонами. Якщо ступінь схожості перевищує встановлений поріг, система приймає рішення щодо автентифікації особи. Це дозволяє забезпечити точність і надійність процесу біометричної ідентифікації.

Розпізнавання за сітківкою ока є високоточним методом біометричної ідентифікації, який базується на аналізі унікального судинного малюнка сітківки ока. Сітківка — це світлочутлива оболонка ока, яка відповідає за перетворення світлових сигналів на нервові імпульси, що передаються в мозок. Завдяки своїй стабільності і унікальності, цей метод забезпечує надзвичайно високий рівень точності.

Процес ідентифікації за сітківкою ока починається зі сканування ока за допомогою спеціалізованого обладнання. Для цього зазвичай використовуються інфрачервоні або світлодіодні джерела світла, що дозволяють отримати високо детальоване зображення судинної сітки.

Отримане зображення піддається ретельній обробці, що дозволяє виділити ключові характеристики сітківки. До основних рис належать відстань між судинами, розташування нервового диска, а також топографія розгалужень судин. Ці ознаки є унікальними для кожної людини і не змінюються протягом її життя, що робить розпізнавання за сітківкою ока

одним з найбільш надійних методів біометричної ідентифікації.

На основі виявлених характеристик формуються біометричний шаблон — унікальний цифровий код, що відображає судинний малюнок сітківки ока. Цей шаблон зберігається в базі даних і використовується для подальшої ідентифікації особи під час перевірки. Приклад сканування та обробки сітківки наведено на рисунку 2.6

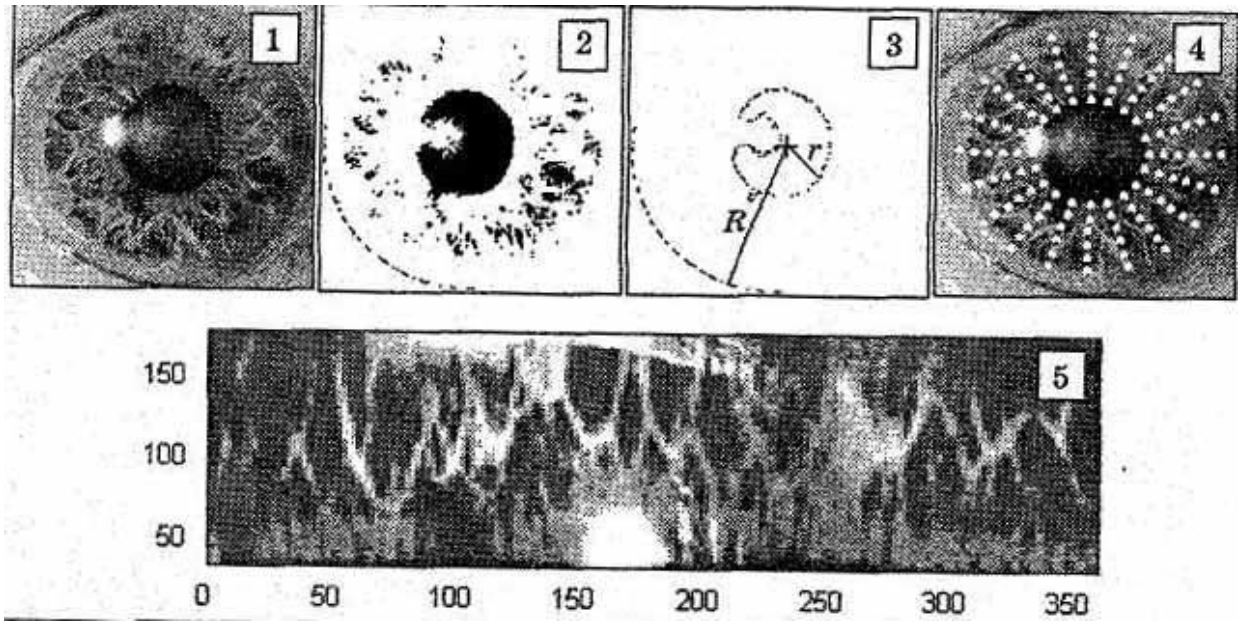

Рисунок 2.6 – Приклад сканування та обробки сітківки

Розпізнавання обличчя — це передовий метод біометричної ідентифікації, що ґрунтується на аналізі унікальних геометричних характеристик людського обличчя. Процес розпізнавання починається з отримання зображень обличчя за допомогою різноманітних пристроїв: від висококласних відеокамер до вбудованих веб-камер на мобільних пристроях. Отримані зображення піддаються попередній обробці, яка включає корекцію масштабу, обертання та освітлення, що забезпечує оптимальні умови для подальшого аналізу.

Наступним етапом є виявлення та вимірювання ключових геометричних ознак обличчя, таких як відстань між очима, форма носа, контури підборіддя та інші характеристики. Ці ознаки формують індивідуальний геометричний шаблон, що є унікальним для кожної людини. Після цього створений шаблон

порівнюється з шаблонами, що зберігаються в базі даних, для перевірки наявності збігу, що дозволяє точно ідентифікувати особу.

2.3 Переваги й недоліки біометричних методів ідентифікації

Ідеальна ідентичність в біометричних характеристиках користувачів, збіг яких складає 100% з даними в електронно-аналітичному пристрої, є малоймовірною. Навіть для двох показників характеристики біометрії це непрактично, оскільки на пальцях та долонях можуть з'явитися порізи, рани, тим самим змінюючі тілесні дані. При великій кількості користувачів, інформація про яких зберігається в електронно-аналітичному пристрої, можливі помилки при розпізнаванні [16].

Біометричні системи автентифікації здійснюють два типи помилок.

– Хибне відхилення доступу (FR). Це відмова в доступі особі, яка має право користування ресурсом. Може виникнути через неправильне використання ідентифікатора або помилкове введення біометричних характеристик;

– Хибне надання доступу (FA). Це надання доступу до ресурсу особі, яка взагалі не має права доступу. Тут скоріше за все є помилка в реєстрації або не оновлена БД. Порівнення переваг та недоліків біометричних систем наведено в таблиці 2.4.

Отже розглянемо головні переваги та недоліки біометричних систем автентифікації осіб [17].

Таблиця 2.4 – Переваги та недоліки біометричної системи

№	Переваги	Недоліки
1	Висока унікальність: базується на унікальних фізичних або поведінкових характеристиках людини, що забезпечує високий рівень безпеки.	Вразливість до змін: зміни в біометричних характеристиках (внаслідок травм, старіння тощо) можуть знизити точність ідентифікації.

Продовження таблиці 2.4 – Переваги та недоліки біометричної системи

2	Стійкість до втрати або забування: біометричні дані неможливо втратити або забути, на відміну від паролів, що забезпечує надійність і безпеку доступу.	Можливі помилки розпізнавання: технічні збої, низька якість зображення або зовнішні фактори можуть призвести до помилкового розпізнавання, що знижує точність системи.
3	Зручність використання: біометрична аутентифікація є швидким і простим процесом, що підвищує зручність для користувача.	Висока вартість обладнання та інфраструктури: для зчитування біометричних даних та створення відповідної інфраструктури потрібне спеціалізоване обладнання, що значно збільшує початкові витрати.
4	Стійкість до підбору: біометричні дані неможливо підібрати, на відміну від паролів або PIN-кодів, що ускладнює несанкціонований доступ.	Ризик порушення приватності: збір, зберігання та обробка біометричних даних вимагають високого рівня безпеки для захисту особистої інформації, що створює потенційні загрози для конфіденційності..
5	Економічна ефективність: після початкових інвестицій у необхідне обладнання, подальше використання системи є відносно недорогим.	Відсутність єдиних стандартів: відсутність загальноприйнятих стандартів для зберігання і обміну біометричними даними ускладнює їх інтеграцію між різними системами та платформами.

Отже, біометрична ідентифікація [18] має значні переваги, такі як висока стійкість до втрати, зручність використання, і неможливість підбору біометричних даних. Однак цей метод також має ряд недоліків, серед яких технічні проблеми, висока вартість обладнання, ризики для приватності та відсутність єдиних стандартів.

Наступним методом біометричної ідентифікації є розпізнавання за відбитками пальців, яке має свої особливості, переваги та обмеження. Переваги та недоліки розпізнавання за відбитком пальців наведено у таблиці 2.5.

Таблиця 2.5 – Переваги та недоліки розпізнавання за відбитком пальців

№	Переваги	Недоліки
1	Висока унікальність: відбитки пальців є абсолютно унікальними для кожної людини, що забезпечує високий рівень безпеки.	Вразливість до змін: пошкодження пальців або захворювання шкіри можуть впливати на точність розпізнавання.
2	Швидкість розпізнавання: процес сканування та порівняння відбитків пальців зазвичай займає мінімум часу, що робить систему швидкою та ефективною.	Можливі помилки розпізнавання: технічні збої, низька якість зображення або зовнішні фактори (наприклад, бруд чи вологість) можуть призвести до помилок.
3	Стійкість до підробок: підробити відбиток пальця дуже складно, що робить цей метод одним з найбільш надійних для ідентифікації.	Висока вартість обладнання: для зчитування відбитків пальців необхідні спеціалізовані сканери, що підвищує вартість системи.
4	Зручність використання: відбитки пальців є природним і звичним способом ідентифікації для людини, що робить процес інтуїтивно зрозумілим.	Ризик порушення приватності: несанкціонований збір або використання відбитків пальців може призвести до порушення конфіденційності та приватності особи.
5	Широкий спектр застосування: цей метод широко використовується в різних сферах — від особистого використання на смартфонах до корпоративної та державної безпеки.	Юридичні та етичні питання: використання біометрії порушує низку юридичних та етичних питань, пов'язаних із захистом персональних даних.

Цей метод має багато переваг [19], проте його застосування потребує ретельного врахування технічних і юридичних аспектів, що стосуються безпеки та приватності користувачів. Переваги та недоліки розпізнавання за обличчям наведено в таблиці 2.6.

Таблиця 2.6 – Переваги та недоліки розпізнавання за обличчям

1	Безконтактний метод: цей метод не вимагає фізичного контакту, що робить його зручним та гігієнічним для користувачів.	Вразливість до умов освітлення: якість зображення обличчя може залежати від рівня освітлення, що може негативно вплинути на точність розпізнавання, особливо в умовах поганого освітлення.
2	Широке застосування: розпізнавання обличчя можна впровадити з використанням вже існуючих камер та програмного забезпечення, що значно полегшує інтеграцію в існуючі системи.	Вплив зовнішніх змін: зміни у зовнішності (зачіска, макіяж, окуляри) можуть ускладнити процес ідентифікації та знизити точність розпізнавання.
3	Висока унікальність: риси обличчя є індивідуальними для кожної людини, що ускладнює підробку і підвищує точність ідентифікації.	Ризик омани: є можливість обдурити систему, використовуючи фотографії або маски, що може призвести до помилкової ідентифікації.
4	Віддалена ідентифікація: цей метод дозволяє здійснювати ідентифікацію на відстані, що особливо зручно для використання в умовах відеоконференцій та інших віддалених комунікацій.	Висока вартість: для ефективного розпізнавання обличчя потрібне спеціалізоване обладнання та програмне забезпечення, що може значно збільшити вартість впровадження системи.

Цей метод є дуже зручним та ефективним, але для його впровадження потрібно враховувати певні технічні обмеження та витрати. Переваги та недоліки розпізнавання за райдужною оболонкою ока наведено в таблиці 2.7.

Перейдемо до розгляду виявлених переваг та недоліків способу розпізнавання особи за райдужною оболонкою ока.

Таблиця 2.7 – Переваги та недоліки розпізнавання за райдужною оболонкою ока

№	Переваги	Недоліки
1	Висока унікальність: кожна райдужна оболонка є унікальною, що забезпечує високий рівень безпеки та точності ідентифікації.	Висока вартість впровадження: розробка та встановлення систем для розпізнавання за райдужною оболонкою можуть бути досить дорогими, що обмежує їхнє широке використання.
2	Стабільність характеристик: візерунок райдужної оболонки не змінюється протягом всього життя людини, що робить цей метод надійним для довгострокової ідентифікації.	Вплив зовнішніх факторів: якість зображення райдужної оболонки може залежати від умов освітлення, стану ока (наприклад, катаракта або запалення) або носіння контактних лінз, що може вплинути на точність ідентифікації.
3	Висока точність: системи розпізнавання за райдужною оболонкою характеризуються високою точністю, що робить їх одним з найбільш ефективних методів біометричної ідентифікації.	-
4	Безконтактний метод: розпізнавання не вимагає фізичного контакту з користувачем, що забезпечує зручність і гігієнічність використання.	-
5	Можливість віддаленої ідентифікації: цей метод можна використовувати для ідентифікації на відстані, що робить його зручним для різних застосувань, зокрема в системах безпеки.	-
6	Швидкість розпізнавання: процес сканування та порівняння даних займає дуже мало часу, що дозволяє швидко здійснювати ідентифікацію.	-
7	Висока стійкість до підробок: підробити райдужну оболонку ока практично неможливо, що робить цей метод дуже надійним для забезпечення безпеки.	-

Цей метод має багато переваг, зокрема високу точність і стійкість до підробок, але потребує значних інвестицій у технічне обладнання та може бути чутливим до певних зовнішніх факторів. Переваги та недоліки розпізнавання за голосом наведено в таблиці 2.8.

Таблиця 2.8 – Переваги та недоліки розпізнавання за голосом

№	Переваги	Недоліки
1	Висока унікальність: голос кожної людини є унікальним завдяки фізіологічним особливостям голосового апарату, що забезпечує високу точність ідентифікації.	Вразливість до змін голосу: захворювання, зміни в емоційному стані або фоновий шум можуть вплинути на точність розпізнавання.
2	Безконтактний метод: розпізнавання за допомогою голосу не вимагає фізичного контакту з пристроєм, що робить цей метод зручним і гігієнічним..	Ризик підробок: можливість використання записів голосу або синтезованих голосових команд може призвести до обману системи.
3	Зручність використання: голосова ідентифікація є інтуїтивно зрозумілим способом взаємодії, що робить процес легким для користувача.	Вплив якості запису: якість мікрофона та умови запису можуть суттєво вплинути на точність розпізнавання голосу.
4	Високий рівень зручності: не потрібно запам'ятовувати додаткові дані, такі як паролі чи PIN-коди, що підвищує комфорт користування.	Вплив психологічного стану: стрес, втома або інші емоційні стани можуть змінити голос і знизити точність ідентифікації.
5	Широкий спектр застосування: голосова біометрія використовується в різних сферах, таких як банківська справа, телекомунікації та системи безпеки, що забезпечує її універсальність.	-

Розпізнавання за голосом має чимало переваг, таких як зручність використання та відсутність потреби в фізичному контакті, але воно також має свої обмеження, пов'язані з чутливістю до змін в голосі та зовнішніх умовах.

Методи розпізнавання обличчя та відбитків пальців

Розпізнавання обличчя – це високотехнологічний процес ідентифікації особи, що базується на аналізі фізичних рис обличчя. Зазвичай цей метод включає кілька етапів.

1. Захоплення зображень обличчя. Для отримання зображення обличчя використовуються різноманітні джерела, такі як камери відеоспостереження, веб-камери, смартфони тощо. Після цього система перевіряє наявність обличчя на зображенні і передає його на попередню обробку.

2. Попередня обробка зображення. Для стандартизації зображення проводиться корекція масштабу, освітлення та кольорової палітри, а також видалення шумів.

3. Визначення ключових точок обличчя. Ідентифікуються важливі точки, такі як очі, ніс, рот, для подальшого аналізу.

4. Виділення унікальних рис обличчя. Такі риси, як форма обличчя та розташування ключових точок, використовуються для створення шаблону обличчя.

5. Створення шаблону обличчя. Використовуючи виділені особливості, створюється унікальний шаблон, який зберігається в базі даних.

6. Порівняння з шаблонами в базі даних. Нове зображення обличчя порівнюється з існуючими шаблонами для ідентифікації.

7. Прийняття рішення. Система визначає, чи зображення обличчя відповідає існуючому шаблону, та приймає рішення про ідентифікацію.

8. Оновлення шаблонів. Система може оновлювати шаблони з часом для покращення точності ідентифікації.

9. Захист даних. Розробляються механізми для захисту особистих даних і запобігання незаконному використанню технології.

10. Застосування в різних сферах. Розпізнавання обличчя використовується у таких галузях, як безпека, контроль доступу, реклама та автоматизована ідентифікація.

Існують різні методи для розпізнавання обличчя, кожен з яких має свої особливості, точність та швидкість. Найпоширенішими є.

1. Метод знаходження ключових точок (Feature-based methods).

Визначення ключових точок обличчя (очі, ніс, рот) для аналізу та розпізнавання.

2. Метод використання геометричних особливостей (Geometry-based methods). Аналіз геометрії обличчя, таких як відстані між очима та пропорції обличчя.

3. Методи на основі текстурних ознак (Texture-based methods). Аналіз текстури обличчя для розпізнавання, за допомогою методів текстурного аналізу або штучних нейронних мереж.

4. Методи засновані на виокремленні ознак (Feature-based methods). Визначення конкретних особливостей обличчя, таких як контури та кольорові характеристики.

5. Методи глибокого навчання (Deep Learning methods). Використання нейронних мереж, таких як згорткові (CNN) або рекурентні (RNN), для вивчення та визначення шаблонів обличчя.

6. Методи 3D-моделювання обличчя (3D Face Modeling methods). Використання тривимірних моделей обличчя для розпізнавання.

7. Методи на основі контурів (Contour-based methods). Визначення контурів обличчя для ідентифікації за допомогою алгоритмів знаходження контурів.

8. Гібридні методи (Hybrid methods). Комбінація різних підходів для покращення точності та ефективності ідентифікації.

Сучасні системи розпізнавання обличчя часто використовують комбінацію цих методів, особливо з інтеграцією глибокого навчання для покращення ефективності та точності ідентифікації. Переваги й недоліки кожного з методів наведено в таблиці 2.9.

Таблиця 2.9 – Переваги та недоліки методів і підходів до розпізнавання обличчя

Метод	Переваги	Недоліки
Геометричні особливості	Оцінює відстані між основними точками обличчя, дозволяючи визначати його положення.	Потребує точних геометричних моделей, чутливий до змін у формі обличчя.

Продовження таблиці 2.9 – Переваги та недоліки методів і підходів до розпізнавання обличчя

Текстурні ознаки	Може працювати в різних умовах освітлення, забезпечуючи більшу універсальність.	Чутливий до змін текстури шкіри, а також має обмеження у реалізації на великих базах даних у реальному часі.
Виокремлення ознак	Дозволяє виділяти унікальні риси обличчя та використовувати їх для розпізнавання емоцій.	Вразливий до змін зовнішності та умов освітлення, що може вплинути на точність.
Глибоке навчання	Автоматично адаптується до великих обсягів даних, демонструючи високу точність у різних умовах.	Потребує значних обсягів даних для навчання, що може призвести до упереджень у результатах.
3D-моделі	Враховує тривимірні характеристики обличчя, що робить систему стійкішою до змін пози або освітлення.	Вимагає спеціалізованого обладнання для створення 3D-моделей, складний у впровадженні..
Контури обличчя	Ефективно визначає контури, що дозволяє точно розпізнавати обличчя.	Чутливий до змін форми обличчя та навколишнього фону, а також не працює з частково прихованими обличчями.
Гібридні методи	Об’єднує переваги кількох методів, що підвищує точність ідентифікації.	Складний у впровадженні, потребує додаткових оптимізацій для досягнення найкращих результатів.

Розпізнавання відбитка пальця є процесом ідентифікації або верифікації особи через аналіз унікальних фізичних характеристик відбитка пальця, таких як відстані між лініями, дугами, форма та розташування вихідних точок. Процес розпізнавання включає кілька ключових етапів [20].

1. Захоплення зображення. Спочатку отримують образ відбитка пальця за допомогою спеціальних сканерів.

2. Попередня обробка. Проводиться очищення зображення, стандартизація розмірів і корекція освітлення для підготовки до подальшого аналізу.

3. Визначення характеристик. Аналізують основні ознаки, такі як форма ліній, розташування дуг і вихідних точок.

4. Створення шаблону. Визначені характеристики перетворюються на математичне представлення відбитка пальця, яке використовується для порівняння.

5. Зберігання шаблонів. Унікальні шаблони зберігаються в базі даних для подальшого порівняння з новими відбитками.

6. Порівняння з шаблонами. Новий відбиток порівнюється з наявними шаблонами для ідентифікації.

7. Прийняття рішення. Система оцінює, чи відповідає новий відбиток існуючому шаблону і надає відповідний результат.

8. Оновлення шаблонів. Система може коригувати шаблони з часом для підвищення точності.

9. Безпека даних. Вживаються заходи для захисту персональних даних і запобігання несанкціонованому використанню технології.

10. Застосування в різних галузях. Технологія використовується у безпеці, контролі доступу, мобільних пристроях, банківських послугах та інших сферах.

Методи розпізнавання відбитків пальців включають різноманітні підходи, як традиційні, так і сучасні методи машинного навчання.

– Метод знаходження особливостей (Minutiae-based methods). Використовує характеристики відбитка, такі як кількість, розташування і тип папілярних ліній, щоб створити унікальний шаблон.

– Метод знаходження глобальних особливостей (Ridge-based methods). Оцінює глобальні властивості відбитка пальця, такі як форма, густота і орієнтація папілярних ліній.

– Метод глибокого навчання (Deep Learning methods). Застосовує нейронні мережі для автоматичного виявлення та аналізу характеристик відбитка пальця, що дозволяє покращити точність і швидкість.

– Методи кореляції (Correlation-based methods). Порівнюють два відбитки пальців за допомогою кореляційних алгоритмів для вимірювання схожості між ними.

– Методи на основі структурних ознак (Structural Feature-based methods). Використовують структуру папілярних ліній, таких як арки, петлі, відгалуження, для ідентифікації відбитка.

– Методи на основі геометричних параметрів (Geometric-based methods). Оцінюють геометричні параметри, такі як довжина, ширина та форма папілярних ліній, для створення унікальних шаблонів.

– Методи на основі термальних зображень (Thermal-based methods). Використовують теплові зображення пальця для визначення унікальних характеристик, стійких до змін зовнішніх умов.

– Методи на основі 3D-відбитків (3D Fingerprint methods). Залучають тривимірні моделі для точнішого представлення відбитка пальця.

– Методи анти-хибного розпізнавання (Anti-Spoofing methods). Включають технології для запобігання підробці відбитків, використовуючи термальні або спектральні характеристики для розпізнавання живих тканин.

– Ці методи та підходи дозволяють забезпечити високу точність і надійність у процесі біометричної ідентифікації, зокрема при використанні сучасних алгоритмів, таких як глибоке навчання, для підвищення ефективності. Переваги й недоліки кожного з методів наведено в таблиці 2.10.

Таблиця 2.10 – Переваги та недоліки методів і підходів до розпізнавання відбитків пальця.

Метод	Переваги	Недоліки
На основі методу ключових точок	Висока точність, унікальність методу, простота алгоритмів, підходить для великих систем	Чутливість до якості та орієнтації зображення, потребує високоякісних сканерів
На основі глобальних структур	Швидкість, менша чутливість до шуму, підходить для великих систем	Менша точність порівняно з методами на основі ключових точок, менш унікальні глобальні характеристики

Продовження таблиці 2.10 – Переваги та недоліки методів і підходів до розпізнавання відбитків пальця.

Глибоке навчання	Висока точність, автоматичне навчання, можливість розпізнавання в реальному часі	Вимагає великої кількості даних для навчання, складність розробки та впровадження, чутливість до змін умов зйомки
Кореляційні методи	Висока швидкість, простота реалізації	Чутливість до змін розміру та позиції пальця, низька точність при високому рівні шуму
Структурні ознаки	Вищий рівень унікальності	Менш ефективний у великих системах або для завдань у реальному часі
Геометричні параметри	Менша чутливість до змін у формі та розмірі пальця	Потрібні якісні відбитки пальців
Термальні зображення	Стійкість до змін у сенсорних умовах	Висока вартість обладнання, складність обслуговування
3D-відбитки	Стійкість до підробок, висока точність	Висока вартість обладнання, складність обслуговування
Анти фальшиві методи	Висока вартість обладнання, складність обслуговування	Можливі помилкові відмови при розпізнаванні живих пальців

2.4 Висновки до розділу

У ході дослідження проведено аналіз сучасних методів ідентифікації особи, які використовуються в системах контролю доступу, включаючи парольний, апаратний та біометричний підходи. Серед них біометрична ідентифікація визнана найбільш перспективною завдяки її унікальності, високій точності та стійкості до підробки. Зокрема, метод розпізнавання обличчя виділено як найзручніший для інтеграції в сучасні системи через розвиток технологій обробки зображень і алгоритмів машинного навчання. Попри високий потенціал, біометричні методи мають певні недоліки, такі як висока вартість впровадження, вимоги до обробки великих обсягів даних та ризики для конфіденційності персональної інформації. Отримані результати дослідження створюють основу для розробки ефективних і надійних систем контролю доступу з використанням біометричних технологій.

3 РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ З ІДЕНТИФІКАЦІЄЮ ОСОБИ

3.1 Розробка структурної схеми радіотехнічної системи

Система контролю доступу з ідентифікацією особи, що розробляється є інтегрованим рішенням [21], що поєднує в собі передові технології розпізнавання обличчя та ідентифікації за допомогою RFID-карт. Серцем системи є мікрокомп'ютер Raspberry Pi 5, потужний і гнучкий пристрій, який керує всіма компонентами та виконує інтенсивні обчислювальні завдання. Структурна схема зображена на рисунку 3.1.

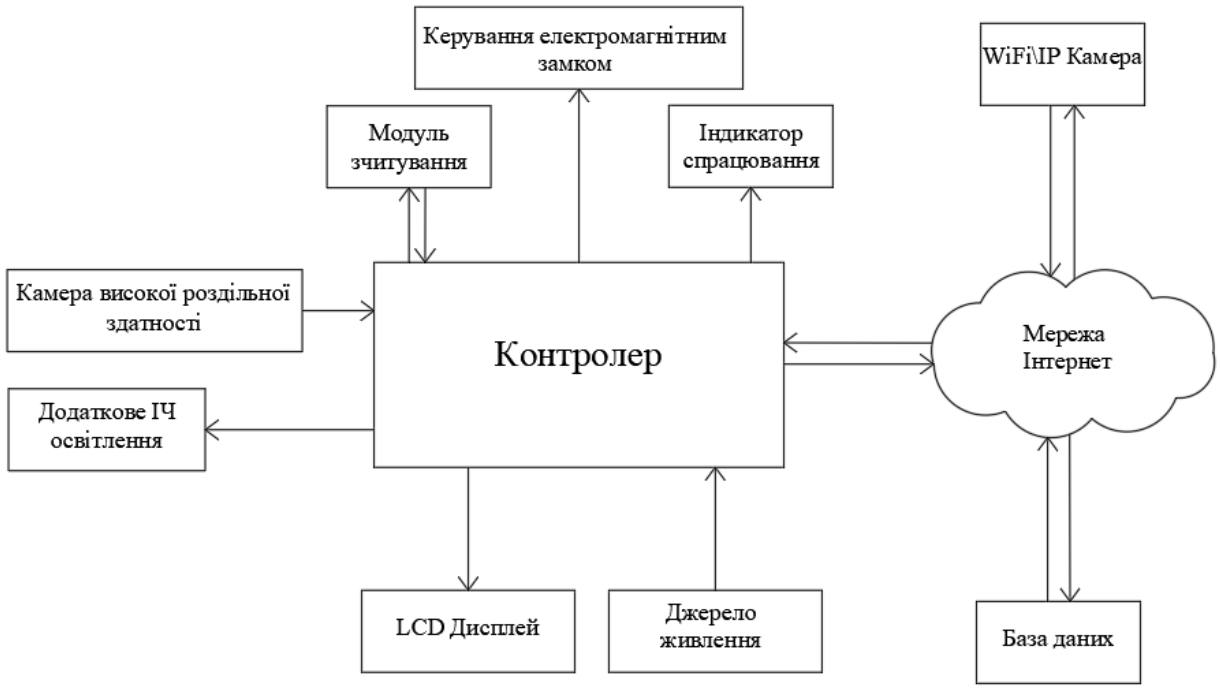

Рисунок 3.1 – Структурна схема радіотехнічної системи контролю доступу з ідентифікацією особи

Структурна схема системи відображає взаємозв'язки між усіма компонентами. Контролер є центральним вузлом, який з'єднаний з камерою,

модулем RFID, звуковим сигналом, реле та базою даних. Кожен компонент виконує свою специфічну функцію і взаємодіє з іншими через відповідні інтерфейси.

Вибір та обґрунтування модулів та складових системи що розробляється.

Ядром системи було обрано мікрокомп'ютер Raspberry Pi5, модуль зображено на рисунку 3.2.

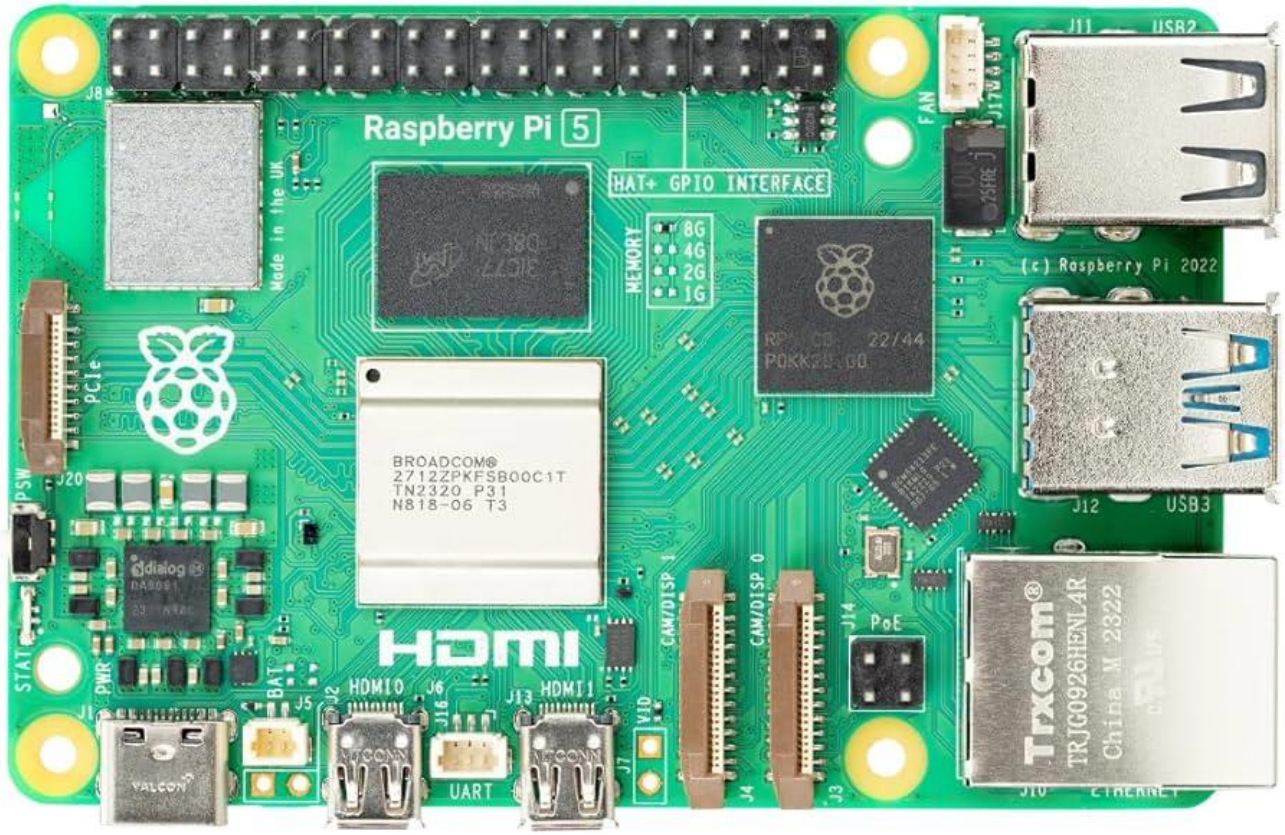

Рисунок 3.2 – Вигляд мікрокомп'ютера Raspberry Pi5

Raspberry Pi 5 - це п'яте покоління популярних одноплатних комп'ютерів, яке пропонує значне підвищення продуктивності та розширені можливості порівняно зі своїми попередниками. Цей компактний пристрій, розміром з кредитну картку, відкриває широкі перспективи для різноманітних проектів, від навчання програмування до створення IoT-пристроїв та індустріальних застосувань [22].

Переваги даного модулю.

– Потужний процесор. Raspberry Pi 5 обладнаний більш швидким і енергоефективним процесором, що забезпечує значне збільшення швидкодії в

порівнянні з попередніми моделями. Це дозволяє виконувати більш складні обчислення та запускати вимогливіші програми.

– Збільшений об'єм оперативної пам'яті. Наявність більшої кількості оперативної пам'яті дозволяє запускати більше додатків одночасно і працювати з більш об'ємними даними.

– Розширені можливості підключення. Raspberry Pi 5 пропонує більшу кількість портів USB, що дозволяє підключати більше периферійних пристроїв. Крім того, він підтримує новіші стандарти бездротової комунікації [23]. Перелік та опис виводів Raspberry Pi5 наведено на рисунку 3.3.

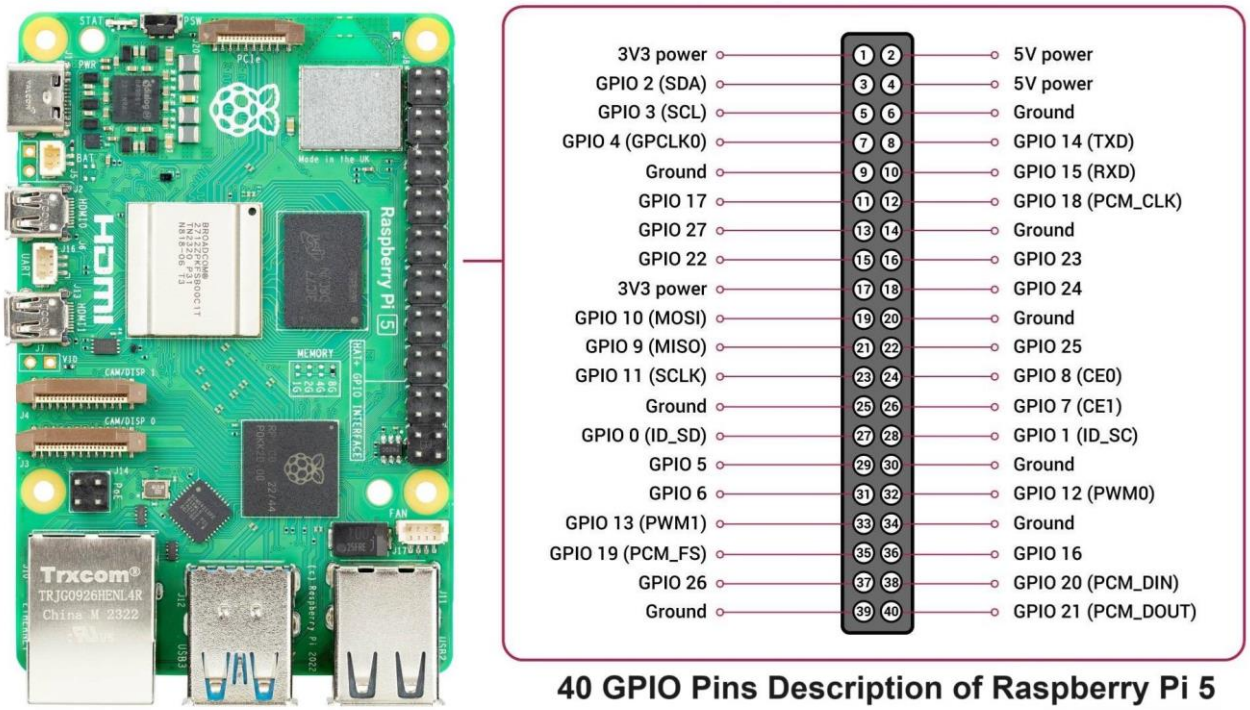

Рисунок 3.3 – Перелік виводів Raspberry Pi5

– Підтримка операційних систем. Raspberry Pi 5 сумісний з різними операційними системами, включаючи Raspberry Pi OS, Ubuntu, Debian та інші. Це дозволяє вибрати найбільш підходящу ОС для ваших потреб.

– Спільнота розробників. Велика і активна спільнота розробників забезпечує постійну підтримку, велику кількість навчальних матеріалів та готових рішень.

Актуальність. швидкість та продуктивність, значне підвищення швидкодії процесора та збільшення об'єму оперативної пам'яті дозволяє Raspberry Pi 5 виконувати більш складні завдання, такі як машинне навчання, обробка зображень у реальному часі та виконання вимогливих ігор.

Розширені можливості: нові інтерфейси та підтримка сучасних стандартів роблять Raspberry Pi 5 більш універсальним пристроєм, що дозволяє підключати різноманітні периферійні пристрої та створювати складні системи.

Енергоефективність: незважаючи на підвищену продуктивність, Raspberry Pi 5 залишається енергоефективним, що дозволяє використовувати його в автономних системах та проектах з обмеженим енергоспоживанням.

Спільнота та підтримка: велика та активна спільнота розробників Raspberry Pi забезпечує постійну підтримку, велику кількість навчальних матеріалів та готових рішень. Це значно полегшує процес навчання та розробки.

Доступність: Raspberry Pi 5 є відносно недорогим пристроєм, що робить його доступним для широкого кола користувачів.

Raspberry Pi 5 є оптимальним вибором для створення систем контролю доступу завдяки своїй високій обчислювальній потужності, гнучкості, підтримці широкого спектру програмного забезпечення та активній спільноті розробників. Хоча Arduino та ESP можуть бути більш привабливими за ціною для простих проектів, Raspberry Pi 5 забезпечує значно більші можливості для реалізації складних і масштабних систем безпеки.

Технічні характеристики мікрокомп'ютера Raspberry Pi5 (Фрагмент даташиту Raspberry Pi5 наведено на рисунку 7 Додатку А).

– CPU: чотириядерний 64-бітний процесор Arm Cortex-A76 з частотою 2.4 ГГц.
– GPU: VideoCore VII GPU з підтримкою OpenGL ES 3.1, Vulkan 1.2.
– RAM: 8 ГБ.

Підключення.

– Ethernet: гігабітний Ethernet.
– Wi-Fi: дводіапазонний Wi-Fi 802.11ac.

– Bluetooth: Bluetooth 5.0 з підтримкою BLE (Bluetooth Low Energy).

– USB: 2 x USB 3.0, 2 x USB 2.0.

– Відео виходи: подвійний вихід дисплея HDMI 4kp60 із підтримкою HDR

– Камера: два 4-канальні трансивери MIPI CSI/DSI, підтримка 2x дисплеїв або 2x камер; або 1x дисплей + 1x камера.

– GPIO: 40-контактний роз'єм GPIO Raspberry Pi.

– PCIe: роз'єм Raspberry Pi для PCIe (1 порт 2.0, потрібна додаткова плата розширення).

– Додаткові характеристики.

– Декодер: 4kp60 HEVC.

– Процесор датчика зображення: Raspberry Pi ISP.

– Годинник реального часу: RTC.

Для забезпечення отримання зображення достатньої якості, щоб відповідати потребам системи, було обрано модуль Raspberry Pi Camera Module 3 - це високоякісна камера, спеціально розроблена для використання з одноплатними комп'ютерами Raspberry Pi. Її компактні розміри та легкість підключення роблять її ідеальним вибором для різних проєктів, включаючи системи відеоспостереження, роботизовані системи та, зокрема, системи контролю доступу з ідентифікацією особи. Зовнішній вигляд Camera Module 3 наведено на рисунку 3.4.

Чому саме Camera Module 3?

– Висока роздільна здатність та чіткість зображення: 12-мегапіксельний сенсор Sony IMX708 забезпечує деталізовані зображення, що дозволяє точно розпізнавати обличчя навіть за складних умов освітлення.

– Автофокус: ця функція дозволяє камері автоматично налаштовувати фокус, забезпечуючи чітке зображення об'єкта, незалежно від відстані.

– Режим HDR: завдяки режиму HDR камера здатна знімати зображення з високим динамічним діапазоном, що дозволяє отримувати деталізовані зображення як у світлих, так і в темних областях.

– Компактність та легкість встановлення: камера має невеликі розміри і легко встановлюється на плату Raspberry Pi за допомогою спеціального роз'єму CSI.

– Програмна підтримка: модуль повністю підтримується бібліотекою libcamera, що значно спрощує його використання в різних проектах.

– Сумісність: камера ідеально поєднується з Raspberry Pi, забезпечуючи безпроблемну інтеграцію в систему.

Рисунок 3.4 – Зовнішній вигляд Pi Camera Module 3

Як Camera Module 3 працює в системі контролю доступу?

1. Зйомка зображення: камера здійснює зйомку обличчя людини, яка намагається отримати доступ.

2. Обробка зображення: отримане зображення передається на процесор Raspberry Pi, де воно обробляється за допомогою спеціального програмного забезпечення.

3. Порівняння з базою даних: оброблене зображення порівнюється з зображеннями, що зберігаються в базі даних системи.

4. Ідентифікація: якщо зображення збігається з одним із зображень в базі даних, система ідентифікує користувача і надає йому доступ.

5. Відмова в доступі: якщо збігу не знайдено, система відмовляє в доступі.

Переваги використання Pi Camera Module 3 в системах контролю доступу:

– Висока точність ідентифікації: завдяки високій роздільній здатності та функції автофокусу, камера забезпечує точне розпізнавання облич навіть за складних умов.

– Безпека: система контролю доступу на основі розпізнавання облич є більш надійною, ніж традиційні системи, що використовують картки або коди доступу.

– Зручність використання: користувачеві не потрібно носити з собою додаткові пристрої для ідентифікації.

– Можливість інтеграції: камера може бути легко інтегрована в інші системи безпеки, такі як системи відеоспостереження або системи контролю доступу на основі відбитків пальців.

Технічні характеристики камери:

- Діапазон фокусування: 10cm → ∞
- Фокусна відстань: 4,74 мм
- Діагональне поле зору: 75 градусів
- Горизонтальне поле зору: 66 градусів
- Вертикальне поле зору: 41 градус
- Фокусне співвідношення (діафрагма): F1,8
- ІЧ-фільтр: інтегрований

Сенсор: Sony IMX708

- Роздільна здатність: 11,9 мегапікселів
- Розмір сенсора: діагональ датчика 7,4 мм
- Розмір пікселя: 1,4 мкм × 1,4 мкм
- По горизонталі/вертикалі: 4608 × 2592 пікселів
- Загальні режими відео: 1080p50, 720p100, 480p120
- Вихід: RAW10
- Система автофокусування: автофокусування з визначенням фази

- Довжина стрічкового кабелю: 200 мм
- Роз'єм кабелю: 15 × 1 мм FPC
- Робоча температура: від 0°C до 50°C

Дисплей Raspberry Pi 5.0inch LCD 800x480 обрано з огляду на наступні характеристики та переваги Зображення дисплею наведено на рисунку 3.5-3.6:

Рисунок 3.5 – Дисплей Raspberry Pi 5.0inch LCD 800x480

1. Оптимальний розмір. Дисплей із діагоналлю 5 дюймів достатньо компактний, щоб інтегруватися в систему доступу, зберігаючи зручність використання. Цей розмір ідеально підходить для відображення основної інформації, такої як статус доступу, текстові повідомлення або інструкції для користувачів.

2. Роздільна здатність 800x480. Висока роздільна здатність забезпечує чітке та деталізоване зображення, що важливо для відображення текстової та графічної інформації, зокрема логотипів, ідентифікаційних номерів або QR-кодів.

3. Сенсорна функціональність (опціонально). Обрана модель дисплея підтримує сенсорний екран, це дозволяє інтегрувати інтерфейс для введення PIN-коду, вибору режимів доступу або налаштувань системи, що значно підвищує функціональність.

4. Сумісність з Raspberry Pi. Дисплей легко підключається до Raspberry Pi через інтерфейс HDMI або GPIO, що спрощує інтеграцію без потреби у додаткових адаптерах або драйверах. Його компонування наведено на рисунку 3.6.

Рисунок 3.6 – Компонування дисплею Raspberry Pi 5.0inch LCD 800x480

5. Енергозбереження. Дисплей споживає мінімальну кількість енергії, що важливо для систем, які працюють у режимі постійного доступу.

6. Міцність і компактність. Дисплей має міцну конструкцію, що дозволяє використовувати його в умовах підвищеного зносу, наприклад, у громадських місцях чи на виробничих об’єктах.

7. Додаткові можливості налаштування інтерфейсу. На дисплеї можуть відображатися.

– Поточний статус системи (доступ дозволено чи заборонено).
– Ідентифікаційна інформація (ім’я користувача, фото).
– Інструкції для користувачів щодо користування RFID-сканером.

Таким чином, використання Raspberry Pi 5.0inch LCD 800x480 дозволяє створити доступну, функціональну та зручну систему контролю доступу, яка відповідає сучасним вимогам до інтерактивності та ергономічності.

Для ідентифікації та зчитування первинної інформації було обрано модуль PN532 було обрано для реалізації системи контролю доступу, що працюють з безконтактними носіями, такими як RFID та NFC. Його універсальність, легкість використання та широкий спектр підтримуваних стандартів роблять його ідеальним рішенням для інтеграції в систему контролю доступу. Зовнішній вигляд модулю PN532 наведено на рисунку 3.7.

PN532 - це інтегрована схема, яка підтримує безліч стандартів безконтактної комунікації, включаючи.

– 13.56 МГц RFID: найбільш поширений стандарт для безконтактних карток.

– NFC: технологія ближньої безконтактної комунікації, що використовується в смартфонах та інших пристроях.

– ISO/IEC 14443 A/B [24]: міжнародні стандарти для безконтактних смарт-карт.

– FeliCa: японський стандарт безконтактної смарт-карти.

Переваги використання PN532:

– Універсальність: підтримка широкого спектру стандартів дозволяє працювати з різними типами безконтактних карток.

– Простота використання: модуль має простий інтерфейс (I2C або SPI) і добре документовану бібліотеку, що полегшує інтеграцію в різні проекти.

– Низьке енергоспоживання: PN532 є енергоефективним пристроєм, що дозволяє використовувати його в портативних та батарейних пристроях.

– Малі розміри: компактні розміри модуля дозволяють легко вбудовувати його в різні пристрої.

– Доступність: модуль PN532 широко доступний і має низьку вартість.

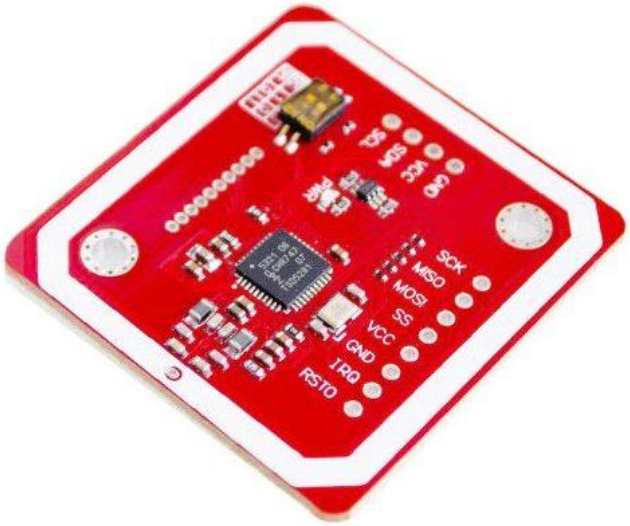

Рисунок 3.7 – Зовнішній вигляд RFID\NFC модулю PN532

Як PN532 працює в системі контролю доступу? (Фрагмент даташиту модуля PN532 наведено на рисунку 8 Додатку А):

1. Зчитування даних з носія: коли користувач підносить безконтактний носій до зчитувача, PN532 зчитує унікальний ідентифікатор, записаний на носії.

2. Передача даних на мікроконтролер: зчитаний ідентифікатор передається на мікроконтролер Raspberry Pi.

3. Порівняння з базою даних: мікроконтролер порівнює отриманий ідентифікатор з даними, що зберігаються в базі даних системи контролю доступу.

4. Прийняття рішення: якщо ідентифікатор знайдено в базі даних і відповідає дозволеним користувачам, система відкриває доступ. В іншому випадку доступ відмовляється.

Інтеграція PN532 з Raspberry Pi Camera Module 3.

Комбінація модуля PN532 і Raspberry Pi Camera Module 3 дозволяє створити більш безпечну систему контролю доступу, яка використовує як

біометричні дані (розпізнавання облич), так і безконтактні картки. Наприклад, для отримання доступу користувач може спочатку прикласти картку до зчитувача, а потім підтвердити свою особистість за допомогою розпізнавання обличчя.

ІЧ світлодіод TSAL6100 було обрано для підсвічування об'єкта в системі контролю доступу з використанням камери Raspberry Pi Camera Module 3 . зовнішній вигляд обраного ІЧ світлодіоду наведено на зображені 3.8.

Рисунок 3.8 – Обраний ІЧ світлодіод TSAL6100

Оптимальна довжина хвилі (850 нм): ця довжина хвилі забезпечує хороший баланс між невидимістю для людського ока та чутливістю сенсора камери. Світло з такою довжиною хвилі ефективно відбивається від шкіри обличчя, забезпечуючи чітке зображення навіть в умовах низької освітленості.

Потужність 50 мВт: цього достатньо для проєктованої системи контролю доступу, де відстань до об'єкта невелика. Така потужність забезпечує яскраве підсвічування, не викликаючи перегріву світлодіода.

Кут розсіювання 30 градусів: цей кут дозволяє сфокусувати світловий потік на об'єкті, забезпечуючи рівномірне підсвічування і мінімізуючи відблиски.

Компактний корпус TO-92: легко встановлюється на плату і не займає багато місця.

Широка доступність: цей світлодіод є одним з найпопулярніших на ринку, що гарантує його доступність і низьку вартість.

Переваги використання TSAL6100 в системі контролю доступу.

– Покращення якості зображення. Завдяки ІЧ підсвічуванню камера зможе знімати чіткі зображення навіть в умовах повного затемнення, що підвищить точність розпізнавання обличь.

– Збільшення дальності дії. ІЧ підсвічування дозволить збільшити відстань, на якій камера зможе розпізнавати обличчя.

– Збільшення швидкості розпізнавання. Яскраве і рівномірне підсвічування дозволить алгоритму розпізнавання швидше обробляти зображення.

– Збільшення надійності системи. ІЧ підсвічування дозволить системі працювати в більш широкому діапазоні умов освітлення, що підвищить її надійність.

Для забезпечення живлення системи було обрано офіційний блок живлення Raspberry Pi 5 27W USB-C PD PSU EU.

Переваги обраного блоку живлення.

– Оптимальна сумісність. він створений спеціально для Raspberry Pi 5, що гарантує безпроблемну роботу.

– Стабільність. технологія Power Delivery забезпечує плавне та стабільне живлення, незалежно від навантаження.

– Потужність. 27 Вт – це достатньо для живлення як самого Raspberry Pi 5, так і підключених периферійних пристроїв.

– Компактність та зручність. компактний розмір і стандартний USB-C роз'єм роблять його зручним у використанні.

– Безпека. вбудовані захисти оберігають пристрій від пошкоджень.

– Довговічність. високоякісні компоненти гарантують тривалий термін служби.

Зображення обраного блоку живлення наведено на рисунку 3.9.

Рисунок 3.9 – Обраний блок живлення 27W USB-C PD PSU EU

Обраний блок живлення відповідає всім необхідним вимогам та забезпечує оптимальні умови роботи Raspberry Pi 5.

Принцип роботи системи полягає в наступному: користувач підносить до зчитувача RFID-карту або смартфон з NFC-модулем. Модуль PN532 зчитує унікальний ідентифікатор з носія та передає його на Raspberry Pi. Одночасно камера Raspberry Pi Camera Module 3 здійснює зйомку обличчя користувача. Отримане зображення обробляється програмним забезпеченням, яке порівнює його з даними, що зберігаються в базі даних. Якщо зображення обличчя відповідає збереженим даним і ідентифікатор з RFID-карти підтверджує особу, система видає команду на відкриття замку. Вся інформація про події фіксується в журналі для подальшого аналізу.

3.2 Розробка апаратної частини системи контролю доступу

Наступним етапом розробки є переведення структурної схеми в конкретну електричну схему за допомогою програми EasyEDA. Цей крок дозволив нам візуалізувати всі елементи системи та їх взаємодію.

Для реалізації електрично-принципової схеми було обрано середовище EasyEDA, оскільки воно є безкоштовним онлайн-інструментом, який дозволяє проектувати електронні схеми, створювати друковані плати (PCB) та проводити симуляцію електричних схем. Це середовище стало популярним серед інженерів, студентів і хобістів, оскільки надає всі необхідні інструменти для проектування електронних пристроїв будь-якої складності. EasyEDA доступна не лише у веб-версії, але й у вигляді десктопних додатків для Windows, macOS та Linux, що дає змогу працювати як в онлайн, так і в офлайн-режимах.

Переваги EasyEDA.

– Вільний доступ: доступність для всіх користувачів без фінансових обмежень.

– Простота використання: інтуїтивно зрозумілий інтерфейс для швидкого освоєння.

– Доступність в онлайн та офлайн режимах: можливість працювати через браузер або за допомогою десктопного додатку.

– Інтеграція з JLCPCB: зручне замовлення друкованих плат безпосередньо з середовища.

– Багатий набір інструментів: наявність бібліотек компонентів і симуляцій для точного тестування проектів.

Головний екран середовища з частиною схеми наведено на риснуку 3.10.

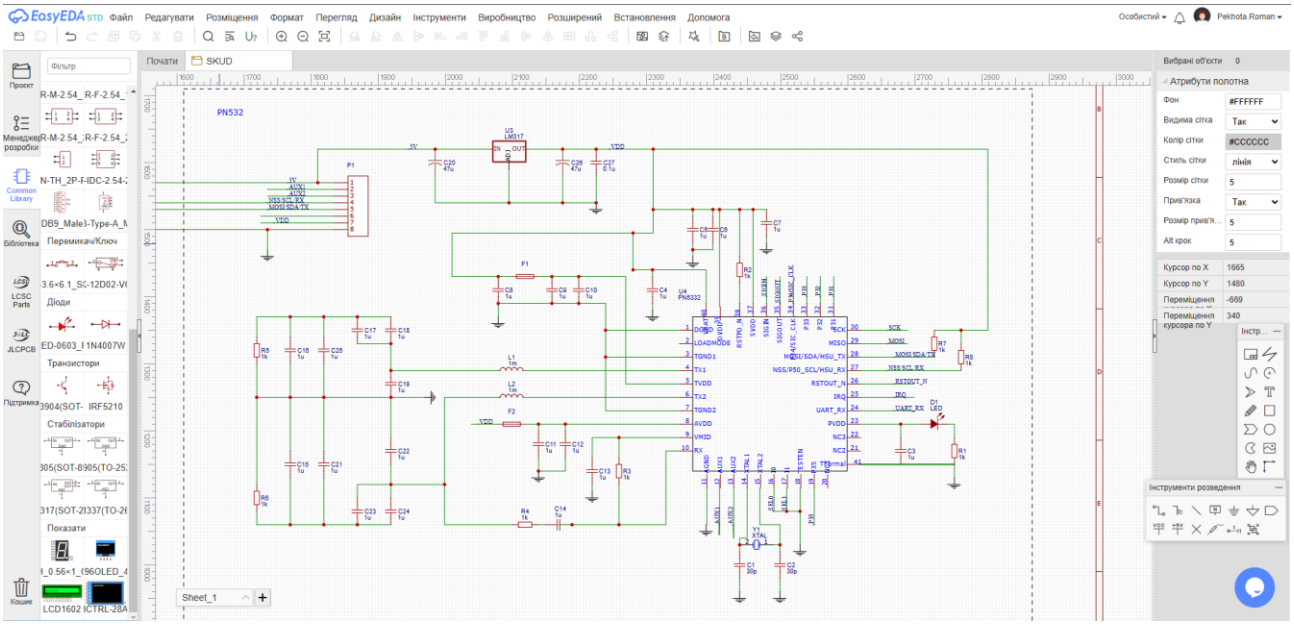

Рисунок 3.10 – Головний екран середовища в процесі розробки схеми

Основні можливості EasyEDA.

1. Редактор схем. Інтерфейс редактора схеми дозволяє зручно створювати електронні схеми з багатим набором компонентів, серед яких транзистори, мікросхеми, резистори, конденсатори, діоди та інші. Компоненти можна розміщувати на схемі, з'єднувати між собою і редагувати. Деякі ключові функції редактора.

– Бібліотека компонентів: доступ до компонентів від таких виробників, як Texas Instruments, Analog Devices, NXP та інших.

– Налаштування параметрів компонентів: можливість змінювати характеристики компонентів, такі як опір, ємність, індуктивність тощо.

– Перевірка підключень (ERC): функція перевірки правильності підключень для мінімізації помилок.

– Можливість спільної роботи: можливість працювати з іншими користувачами над спільними проектами і доступ до загальних бібліотек.

2. Редактор друкованих плат. EasyEDA має потужний інструмент для проектування друкованих плат, який включає.

– Інструменти трасування: для прокладання з’єднань між компонентами.

– Підтримка багатошарових плат: дозволяє створювати складні плати з кількома шарами з’єднань.

– Перевірка правил проектування (DRC): автоматична перевірка на відповідність мінімальним вимогам для ширини доріжок, відстані між ними та інших параметрів.

– Автоматичне трасування: функція для автоматичного прокладання трас, що полегшує роботу для початківців.

3. Бібліотека компонентів. В EasyEDA доступна велика бібліотека компонентів, яку можна шукати за назвою, категорією або параметрами. До її складу входять.

– Компоненти з SPICE-моделями для симуляції.

– Частини від великих виробників, таких як Microchip, Texas Instruments, STMicroelectronics.

– Можливість завантажувати і використовувати бібліотеки, створені іншими користувачами.

4. Симуляція схем. EasyEDA дозволяє проводити симуляцію схеми, що дає змогу перевіряти її функціональність перед виготовленням плати. Симуляція включає.

– DC і AC аналіз: дозволяє оцінити роботу схеми при постійному та змінному струмі.

– Транзактний аналіз: перевірка змін у часі для більш детального аналізу поведінки схеми.

– Підтримка SPICE-моделей для тестування параметрів компонентів.

– Інтеграція з JLCPCB. EasyEDA має інтеграцію з JLCPCB, одним із найбільших виробників друкованих плат, що дає змогу. Замовляти виготовлення плат безпосередньо після завершення проектування.

– Швидко отримувати плати завдяки ефективній доставці від JLCPCB.

– Переглядати проект у 3D до виготовлення плати для перевірки її зовнішнього вигляду та компонування.

5. Формати файлів та імпорт/експорт. EasyEDA підтримує імпорт та експорт різних форматів файлів, що дозволяє без проблем працювати з іншими CAD-системами. Серед можливостей.

– Імпорт файлів з Altium, Eagle, Kicad.

– Експорт у Gerber-формат для виготовлення плат.

– Імпорт та експорт бібліотек компонентів для зручного використання вже наявних розробок.

6. Спільнота та ресурси. EasyEDA має велику спільноту користувачів, які діляться своїми проектами, бібліотеками та навчальними матеріалами. На офіційному сайті доступні численні приклади, відеоуроки та інструкції для користувачів усіх рівнів.

Схему електричну принципову наведено на рисунку 3.11.

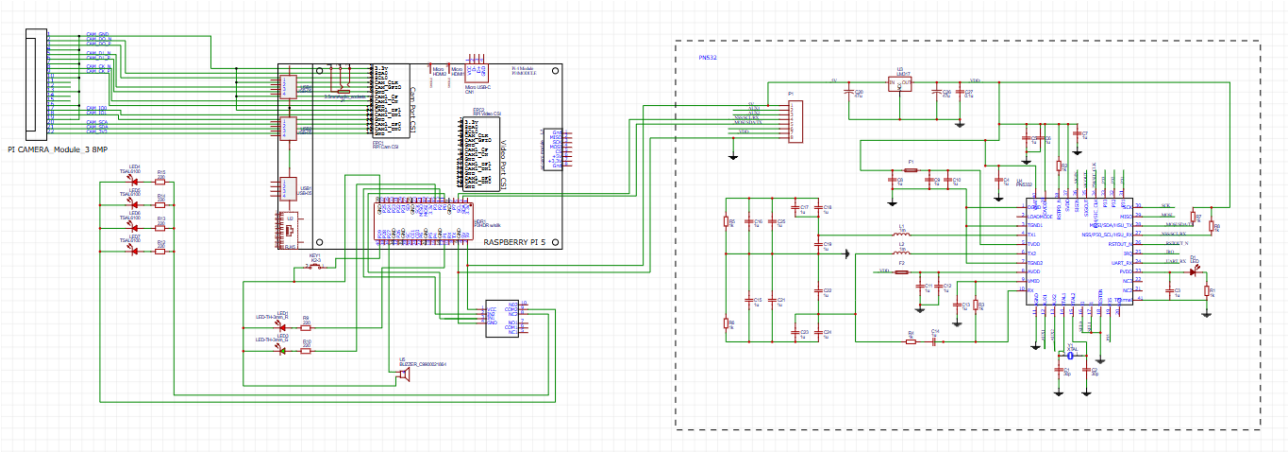

Рисунок 3.11 – Схема електрична принципова системи контролю доступу

Для реалізації керування електромагнітом з модуля Raspberry Pi5 [25], з'явилась необхідність розробити шилд для підтримки двох реле та забезпення їх роботи на 12в, оскільки дану напругу не підтримує модуль Raspberry Pi5, на рисунку 3.12 наведено вигляд компоненту на схемі електричній принциповій та його друкована плата.

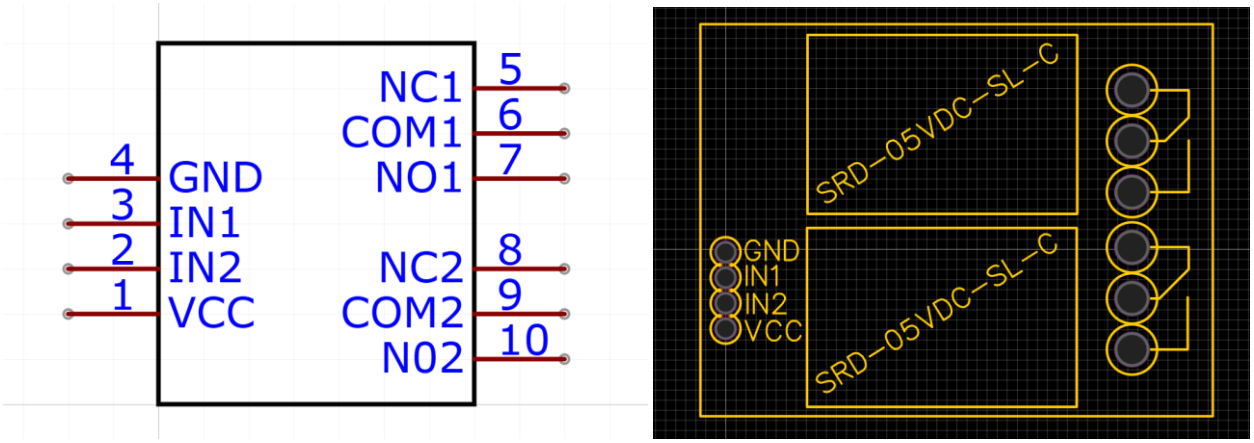

Рисунок 3.12 – Схема електрична принципова та друкована плата шилд модулю на дві реле для керування електромагнітом

Опис компонентів схеми.

1. Raspberry Pi 5. [26]

– Центральний мікрокомп'ютер, який виконує роль контролера для всієї системи.

– Має порти для підключення камери (CSI), GPIO для управління реле, а також I²C для обміну даними з RFID-модулем PN532.

– Живиться від блоку живлення через роз'єм USB Type-C з підтримкою Power Delivery.

2. Pi Camera Module 3.

– Камера, підключена до спеціального CSI-порту Raspberry Pi 5 через шлейф.

– Використовується для фото- або відеофіксації під час розпізнавання користувача або відкриття дверей.

– RFID NFC модуль PN532

– Дозволяє розпізнавати RFID/NFC мітки.

– Підключений до Raspberry Pi через шину I²C.

3. Шилд на 2 реле.

– Використовується для керування електромагнітним замком та додатковим освітленням.

– Отримує сигнали управління від GPIO Raspberry Pi.

4. Інфрачервоні світлодіоди (4 шт.).

– Забезпечують додаткове освітлення для камери в умовах низької освітленості.

– Підключені до одного з реле.

5. Індикація спрацювання.

– Зелений світлодіод сигналізує про успішну ідентифікацію.

– Червоний світлодіод сигналізує про помилку ідентифікації.

– Динамік відтворює звуковий сигнал для підтвердження дій (наприклад, відкриття замка або помилки).

– Підключення світлодіодів і динаміка реалізується через GPIO Raspberry Pi із використанням обмежувальних резисторів.

6. Блок живлення (5В, 5А).

– Живить Raspberry Pi, модулі та периферійні пристрої.

– Забезпечує стабільну роботу системи навіть при значному споживанні струму.

3.3 Розробка програмних алгоритмів системи

У цьому підрозділі детально описується процес розробки програмних алгоритмів, що лежать в основі функціонування системи контролю доступу на основі розпізнавання обличчя та RFID-ідентифікації. Розроблені алгоритми забезпечують зчитування та обробку даних з RFID-карток та смартфонів, розпізнавання обличчя, порівняння отриманих даних з базою даних та управління виконавчими механізмами наприклад, електромагнітним замком. Структурна схема взаємодії між модулями зображена на рисунку 3.13.

Архітектура системи включає модулі зчитування даних з RFID, обробки зображень, розпізнавання облич, взаємодії з базою даних [27], управління виконавчими механізмами та ведення журналу подій. Кожен модуль виконує чітко визначену функцію та взаємодіє з іншими модулями за допомогою визначених інтерфейсів.

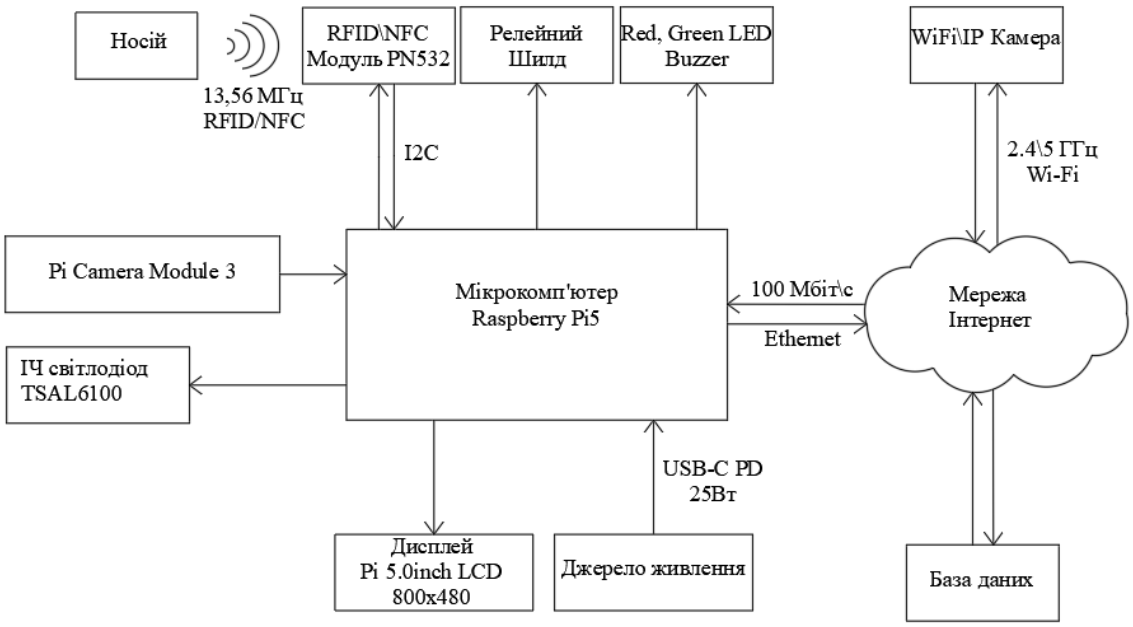

Рисунок 3.13 – Структурна схема взаємодії між модулями

Модуль зчитування даних з RFID-карток та смартфонів взаємодіє з модулем PN532, зчитуючи унікальні ідентифікатори та передаючи їх на наступний етап обробки.

Модуль обробки зображень здійснює зйомку, попередню обробку (нормалізацію, детектування обличчя) та екстракцію ознак з отриманого зображення.

Модуль розпізнавання обличчя порівнює екстраговані ознаки з шаблонами в базі даних та приймає рішення про відповідність [28].

Модуль взаємодії з базою даних зберігає та шукає необхідну інформацію в базі даних (ідентифікатори, шаблони облич, журнали подій).

Модуль управління виконавчими механізмами передає команди на відкриття/закриття замку на основі результатів перевірки.

Модуль ведення журналу подій фіксує всі події в системі.

Алгоритми обробки зображень та розпізнавання обличь включають перед обробку зображення (нормалізацію, виділення області обличчя), екстракцію ознак (наприклад, за допомогою Local Binary Patterns Histogram) та порівняння з базою даних (наприклад, за допомогою евклідової відстані).

Взаємодія з базою даних здійснюється за допомогою SQL-запитів для збереження нової інформації, пошуку шаблонів облич та запису журнальних записів.

Реалізація системи передбачає вибір мови програмування, бібліотек та інструментів розробки.

Тестування системи проводиться для перевірки працездатності всіх функціональних можливостей та точності розпізнавання.

Аналіз результатів дозволяє оцінити ефективність системи, виявити слабкі місця та внести необхідні зміни.

Вибір мови програмування та бібліотек [29].

Для розробки системи контролю доступу на основі розпізнавання обличчя та RFID-ідентифікації було обрано мову програмування Python та бібліотеку OpenCV. Цей вибір обумовлений низкою факторів.

Python як мова програмування вирізняється простотою синтаксису, що значно спрощує процес розробки та робить код більш читабельним[30]. Велика кількість готових бібліотек та фреймворків, таких як NumPy, SciPy, TensorFlow, дозволяє ефективно вирішувати різноманітні завдання машинного навчання та обробки даних. Крім того, Python має активну спільноту розробників, що забезпечує доступність великої кількості навчальних матеріалів та підтримки.

OpenCV (Open Source Computer Vision Library) є однією з найпопулярніших бібліотек для обробки зображень та комп'ютерного зору[31]. Вона пропонує широкий спектр функцій для детектування облич, розпізнавання ознак, порівняння зображень та інших завдань, необхідних для реалізації системи розпізнавання облич. OpenCV легко інтегрується з Python, що дозволяє швидко створювати прототипи та розробляти повноцінні системи[32].

Додаткові бібліотеки.

– NumPy. Для ефективної роботи з масивами та матрицями, що широко використовуються в обробці зображень.

– SciPy. Для наукових обчислень та оптимізації.

– Pandas. Для роботи з даними, зокрема для управління базою даних системи.

– Pillow (PIL Fork). Для базової обробки зображень.

– RPi.GPIO. Для взаємодії з GPIO-портами Raspberry Pi для управління зовнішніми пристроями (наприклад, замком).

– mfrc522-python. Для роботи з модулем RFID RC522. Хоча ми використовуємо PN532, ця бібліотека може бути адаптована або використана як основа для створення власного драйвера для PN532.

Переваги такого вибору.

– Швидкість розробки. Python та OpenCV [33] дозволяють швидко створювати прототипи та втілювати нові ідеї.

– Гнучкість. Широкий спектр бібліотек дозволяє адаптувати систему до різних завдань та вимог.

– Спільнота. Активна спільнота розробників забезпечує постійний розвиток та підтримку.

– Відкритість. OpenCV є бібліотекою з відкритим кодом, що дозволяє вивчати її внутрішню роботу та вносити власні зміни.

– Ефективність. Оптимізовані алгоритми OpenCV забезпечують високу швидкість обробки зображень.

– Розроблений лістинг програмного забезпечення наведено нижче.

Лістинг коду.

```
import cv2
import numpy as np
import time
import sqlite3
import pickle
from tensorflow.keras.applications.resnet50 import ResNet50,
preprocess_input
from imutils.video import VideoStream
from sklearn.neighbors import KNeighborsClassifier
from mfrc522 import SimpleMFRC522  # Бібліотека для RFID
import RPi.GPIO as GPIO
import Adafruit_CharLCD as LCD  # Бібліотека для роботи з LCD-
дисплеєм
```

На початку програми виконується імпорт усіх необхідних бібліотек, які забезпечують роботу різних модулів системи.

Ці бібліотеки виконують такі функції:

OpenCV (cv2): забезпечує обробку зображень та відеопотоку, включно з функціями для роботи з камерами, обробкою кадрів, розпізнаванням облич і загальною передобробкою даних.

NumPy (np): використовується для роботи з багатовимірними масивами та виконання різноманітних математичних операцій, які потрібні для аналізу даних.

Time: забезпечує виконання часових затримок і вимірювання тривалості виконання завдань.

SQLite3: використовується для роботи з локальною базою даних, яка містить інформацію про користувачів системи.

Pickle: забезпечує збереження та завантаження моделей машинного навчання (наприклад, KNN) у двійковому форматі.

TensorFlow та Keras: модуль tensorflow.keras.applications включає модель ResNet50 і функцію preprocess_input для передобробки зображень перед аналізом.

Imutils: бібліотека для роботи з відео, спрощує використання камер і обробку відеопотоків.

Scikit-learn (sklearn): використовується для класифікації даних за допомогою KNN-моделі.

MFRC522: модуль для взаємодії з RFID-зчитувачем через Raspberry Pi.

RPi.GPIO: забезпечує керування GPIO-пінами Raspberry Pi, необхідними для підключення зовнішніх пристроїв, таких як реле замка чи кнопка аварійного відкриття.

Adafruit_CharLCD: бібліотека для роботи з LCD-дисплеєм, який використовується для виведення повідомлень користувачу.

Таким чином, підключення бібліотек забезпечує роботу всіх ключових модулів системи — від аналізу відеопотоку до взаємодії з апаратними компонентами.

```
# === Ініціалізація модулів ===
print("[INFO] Ініціалізація системи...")
# Ініціалізація RFID/NFC модуля
```

```
reader = SimpleMFRC522()
# Завантаження моделі ResNet50
model = ResNet50(weights='imagenet', include_top=False,
input_shape=(224, 224, 3))
# Підключення до локальної бази даних
conn = sqlite3.connect('users.db')
cursor = conn.cursor()
# Підключення до камери
cap = VideoStream(src=0).start()
time.sleep(2.0)  # Затримка для запуску камери
# Налаштування GPIO
RELAY_LOCK = 17  # Пін для реле замка
EMERGENCY_BUTTON = 27  # Пін для кнопки аварійного відкриття
GPIO.setmode(GPIO.BCM)
GPIO.setup(RELAY_LOCK, GPIO.OUT, initial=GPIO.LOW)
GPIO.setup(EMERGENCY_BUTTON, GPIO.IN, pull_up_down=GPIO.PUD_UP)

# Ініціалізація LCD-дисплея
lcd = LCD.Adafruit_CharLCDPlate()
lcd.clear()
```

На етапі ініціалізації модулів виконується підготовка всіх компонентів системи для забезпечення її функціональності. Система ініціалізує модуль для роботи з RFID/NFC-зчитувачем, який зчитує мітки користувачів. Завантажується попередньо навчена модель ResNet50 для аналізу зображень облич та вилучення їхніх глибинних ознак. Підключення до локальної бази даних SQLite забезпечує зберігання інформації про користувачів, включно з їхніми RFID-ідентифікаторами та характеристиками облич.

Додатково, ініціалізується камера для захоплення відеопотоку, що є основою для розпізнавання облич. Налаштовуються GPIO-піни для взаємодії із зовнішніми пристроями, зокрема реле замка та кнопкою аварійного відкриття, а також LCD-дисплей для виведення повідомлень користувачу. Завершення процесу підготовки підтверджується повідомленням на дисплеї, що сигналізує про готовність системи до роботи.

```
# === Функції ===
def preprocess_image(image):
    """Передобробка зображення для моделі ResNet."""
    img = cv2.resize(image, (224, 224))
    img = preprocess_input(img)
    return np.expand_dims(img, axis=0)
def recognize_face(image, model, knn_model):
    """Розпізнає обличчя на основі зображення."""
    processed_img = preprocess_image(image)
```

```
    features = model.predict(processed_img).flatten()
    user_id = knn_model.predict([features])[0]
    return user_id
def read_rfid():
    """Зчитує RFID/NFC мітку."""
    try:
        rfid_id, text = reader.read()
        return text.strip()
    except Exception as e:
        lcd.clear()
        lcd.message("Помилка RFID!")
        print(f"[ERROR] Помилка зчитування RFID: {e}")
        return None
def check_access(rfid, face_id):
    """Перевіряє відповідність даних з бази та повертає статус
доступу."""
    cursor.execute("SELECT * FROM users WHERE rfid_id = ?",
(rfid,))
    user = cursor.fetchone()
    if user and str(user[0]) == str(face_id):
        lcd.clear()
        lcd.message(f"Доступ надано\n{user[1]}")
        print(f"[ACCESS GRANTED] Користувач: {user[1]}")
        return True
    lcd.clear()
    lcd.message("Доступ заборонено")
    print("[ACCESS DENIED] Невідповідність даних.")
    return False
def open_door():
    """Відкриває двері на кілька секунд."""
    lcd.clear()
    lcd.message("Двері відкриті")
    print("[INFO] Двері відкриті.")
    GPIO.output(RELAY_LOCK, GPIO.HIGH)
    time.sleep(3)  # Тримати двері відкритими 3 секунди
    GPIO.output(RELAY_LOCK, GPIO.LOW)
    lcd.clear()
    lcd.message("Двері зачинені")
    print("[INFO] Двері зачинені.")
def emergency_open(channel):
    """Відкриває двері при натисканні кнопки аварійного
відкриття."""
    lcd.clear()
    lcd.message("Аварійне\nвідкриття")
    print("[EMERGENCY] Аварійне відкриття дверей.")
    open_door()
# Налаштування переривання для кнопки аварійного відкриття
GPIO.add_event_detect(EMERGENCY_BUTTON, GPIO.FALLING,
callback=emergency_open, bouncetime=300)
```

Система включає кілька ключових функцій, які забезпечують виконання основних завдань.

preprocess_image(image) функція здійснює передобробку зображень для роботи з моделлю ResNet50. Зображення масштабується до розміру 224x224 пікселів і нормалізується, щоб відповідати вхідним вимогам нейронної мережі.

recognize_face(image, model, knn_model) ця функція використовується для розпізнавання облич. Вона отримує ознаки обличчя за допомогою ResNet50, а потім передає ці дані в KNN-модель для визначення користувача [34].

read_rfid() функція виконує зчитування RFID/NFC-міток. У разі успішного зчитування повертається ідентифікатор мітки. Якщо виникають помилки, вони фіксуються, а на дисплей виводиться відповідне повідомлення.

check_access(rfid, face_id) ця функція відповідає за перевірку відповідності даних з RFID-мітки і розпізнаного обличчя з інформацією в базі даних. Якщо дані збігаються, користувачу надається доступ, і на дисплей виводиться підтвердження. Якщо відповідності немає, доступ блокується.

open_door() функція відповідає за управління реле замка для відкриття дверей. Вона відкриває двері на визначений час (3 секунди), після чого замок автоматично зачиняється. Про стан дверей повідомляється через LCD-дисплей.

emergency_open(channel) функція активується натисканням кнопки аварійного відкриття. Вона негайно відкриває двері, незалежно від результатів ідентифікації, що є важливим для забезпечення безпеки в надзвичайних ситуаціях.

Ці функції працюють у тісній взаємодії, забезпечуючи зчитування даних, перевірку ідентифікації, контроль доступу і керування апаратними елементами системи.

```
# === Основний цикл роботи ===
print("[INFO] Система запущена. Очікування користувача...")
lcd.message("Система готова")
# Завантаження KNN моделі
with open('knn_model.sav', 'rb') as f:
    knn_model = pickle.load(f)
try:
    while True:
        # Зчитування RFID/NFC
        rfid = read_rfid()
        if not rfid:
            continue
        print(f"[INFO] Зчитано RFID: {rfid}")
        lcd.clear()
```

```
        lcd.message(f"RFID: {rfid}")
        # Розпізнавання обличчя
        frame = cap.read()
        gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
        face_cascade = cv2.CascadeClassifier(cv2.data.haarcascades
+ "haarcascade_frontalface_default.xml")
        faces = face_cascade.detectMultiScale(gray,
scaleFactor=1.1, minNeighbors=5, minSize=(30, 30))
        if len(faces) > 0:
            (x, y, w, h) = faces[0]  # Перший знайдений об'єкт
            face_roi = frame[y:y+h, x:x+w]
            try:
                face_id = recognize_face(face_roi, model,
knn_model)
                print(f"[INFO] Розпізнано обличчя: {face_id}")
                lcd.clear()
                lcd.message(f"Обличчя: {face_id}")
                # Перевірка доступу
                if check_access(rfid, face_id):
                    open_door()
                else:
                    print("[INFO] Доступ заборонено.")
            except Exception as e:
                lcd.clear()
                lcd.message("Помилка обличчя!")
                print(f"[ERROR] Помилка розпізнавання обличчя:
{e}")
        else:
            lcd.clear()
            lcd.message("Обличчя не знайдено")
            print("[INFO] Обличчя не знайдено.")
        time.sleep(1)
except KeyboardInterrupt:
    print("[INFO] Завершення роботи...")
finally:
    GPIO.cleanup()
    cap.stop()
    conn.close()
```

Ця програма забезпечує дворівневу систему ідентифікації користувачів для контролю доступу до приміщення. Вона поєднує RFID/NFC зчитування (перший рівень ідентифікації) із розпізнаванням обличчя за допомогою нейронної мережі ResNet50 та класифікації через метод KNN (другий рівень). Розглянемо детально, як працює кожен компонент системи 1. RFID/NFC-зчитування. Модуль MFRC522 зчитує UID (унікальний ідентифікатор) RFID/NFC мітки.

Логіка.

– Функція read_rfid() отримує UID мітки або NFC-з'єднання з мобільного пристрою.

– UID порівнюється із записами в базі даних SQLite.

– Умови.

– Якщо мітка знайдена в базі, система переходить до наступного етапу — розпізнавання обличчя.

– Якщо UID невідомий, доступ заборонено, і програма повідомляє про це.

2. Розпізнавання обличчя. Розпізнавання обличчя реалізовано за допомогою.

– OpenCV — для захоплення кадру з камери та виявлення облич на зображенні.

– ResNet50 — для отримання векторного представлення обличчя.

– KNN (k-найближчих сусідів) — для порівняння векторів облич користувачів із векторами у базі даних.

Логіка.

1) Захоплення обличчя.

– Камера захоплює поточне зображення, а OpenCV виділяє область із виявленим обличчям.

– Якщо обличчя знайдено, вирізана область передається в модель ResNet50.

2) Розрахунок векторів.

– Модель ResNet50 генерує векторні представлення (embedding) для зображення обличчя.

3) Порівняння.

– Генерований вектор порівнюється із збереженими векторами у базі даних через класифікатор KNN.

– Якщо обличчя знайдено в базі, повертається ID користувача.

– Результат.

– Якщо обличчя співпадає з RFID-записом у базі, доступ дозволяється.

– Якщо обличчя не співпадає або не знайдено, доступ забороняється.

3. База даних SQLite. Система використовує локальну базу даних users.db, яка містить інформацію про користувачів.

Структура таблиці users.

– id — унікальний ID користувача.

– name — ім'я користувача.

– rfid_id — UID RFID/NFC мітки.

– face_vector — векторне представлення обличчя.

– role — роль користувача (наприклад, "admin" або "user").

– status — статус доступу (активний або заблокований).

Функціонал бази даних.

– Функція check_access() перевіряє відповідність UID мітки та ID обличчя.

– Доступ дозволяється лише, якщо знайдено обидва збіги.

4. Керування дверним замком. Для керування електромагнітним замком використовується GPIO-порт Raspberry Pi.

Логіка.

– Якщо доступ дозволено, функція open_door() активує реле замка, що відкриває двері на кілька секунд.

– Замок автоматично блокується після закінчення часу.

5. Обробка виключень. Система враховує можливі помилки.

– Помилка зчитування RFID: повідомлення про неможливість отримати UID.

– Відсутність обличчя в кадрі: перехід до наступної ітерації.

– Невідомий користувач: сповіщення про відмову у доступі.

6. Навчання KNN-моделі. Для розпізнавання облич використовується класифікатор KNN. Попередньо його потрібно навчити [35] на векторах облич зареєстрованих користувачів. Модель розпізнавання обличчя наведена на риснку 3.14.

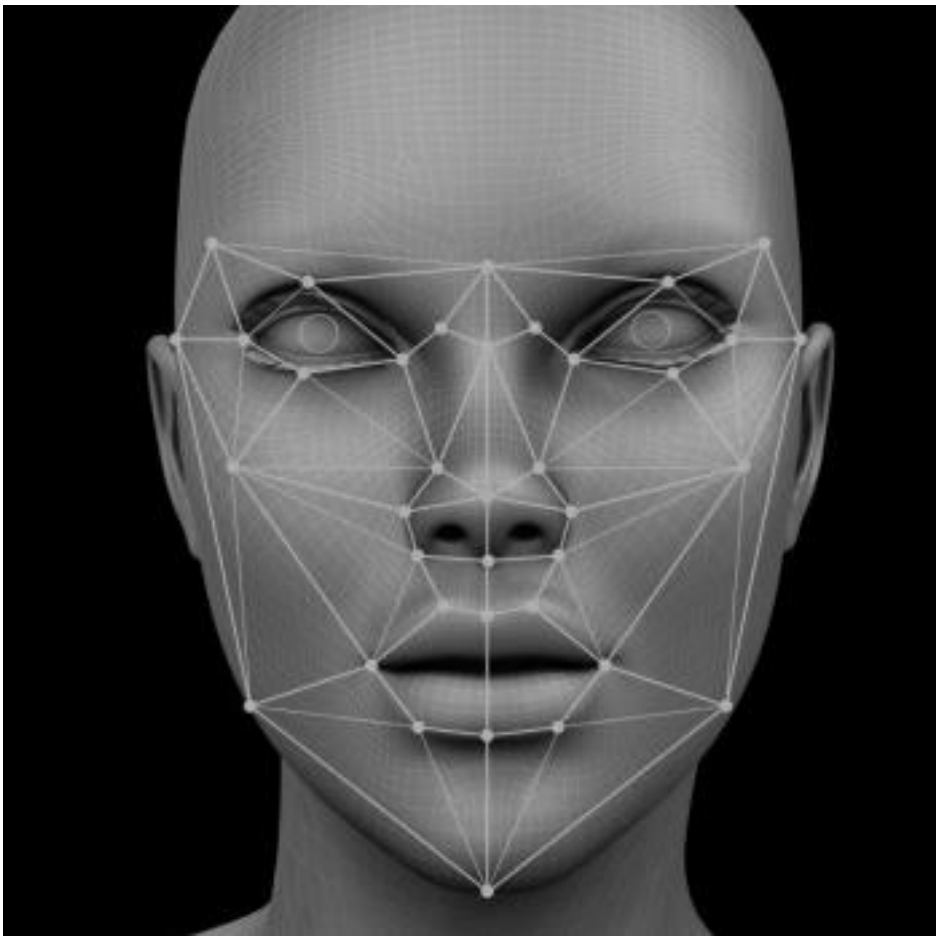

Рисунок 3.14 – Модель розпізнавання обличчя.

Принцип навчання KNN.

```
from sklearn.neighbors import KNeighborsClassifier
import pickle

# Завантаження векторів облич та відповідних ID
data = np.load('face_vectors.npy')  # Вектори облич
labels = np.load('user_ids.npy')    # Відповідні ID

# Створення та навчання моделі
knn = KNeighborsClassifier(n_neighbors=3, metric='euclidean')
knn.fit(data, labels)

# Збереження моделі
with open('knn_model.sav', 'wb') as f:
    pickle.dump(knn, f)
```

7. Основний цикл роботи. Програма безперервно.

1) Очікує зчитування RFID/NFC.
2) Захоплює кадри з камери та аналізує обличчя.
3) Порівнює отримані дані з базою користувачів.

4) Виконує дії (відкриття дверей або відмову в доступі) залежно від результатів перевірки.

8. Можливе розширення функціоналу.

– Хмарна база даних: для централізованого керування доступом.

– Журнал подій: запис усіх успішних і невдалих спроб доступу.

– Інтеграція з іншими системами: надсилання повідомлень адміністратору.

3.4 Висновки до розділу

У процесі розробки системи контролю доступу створено інтегровану апаратно-програмну платформу, яка реалізує двофакторну автентифікацію на основі RFID-ідентифікації та розпізнавання обличчя. Розроблено структурну схему, апаратну частину та алгоритми, що забезпечують взаємодію між компонентами системи в реальному часі. Використання сучасного обладнання, зокрема Raspberry Pi 5, модуля Pi Camera та RFID-зчитувача PN532, дозволило досягти високої точності та надійності роботи системи. Окрім цього, визначено можливості масштабування, включаючи інтеграцію з хмарними сервісами для централізованого управління доступом. Запропонована система демонструє високу ефективність, гнучкість і потенціал для застосування на об’єктах із підвищеними вимогами до безпеки.

4 ЕКОНОМІЧНА ЧАСТИНА

Науково-технічна розробка має право на існування та впровадження, якщо вона відповідає вимогам часу, як в напрямку науково-технічного прогресу та і в плані економіки. Тому для науково-дослідної роботи необхідно оцінювати економічну ефективність результатів виконаної роботи.

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Метою проведення комерційного і технологічного аудиту дослідження за темою «Радіотехнічна система контролю доступу з ідентифікацією особи» є оцінювання науково-технічного рівня та рівня комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності.

Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-ти бальної системи оцінювання за 12-ма критеріями [37].

Таблиця 4.1 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Експерт (ПІБ, посада)		
	1	2	3
	Бали:		
1. Технічна здійсненність концепції	4	4	4
2. Ринкові переваги (наявність аналогів)	3	4	3
3. Ринкові переваги (ціна продукту)	3	2	3
4. Ринкові переваги (технічні властивості)	4	3	4
5. Ринкові переваги (експлуатаційні витрати)	3	2	3
6. Ринкові перспективи (розмір ринку)	3	3	3
7. Ринкові перспективи (конкуренція)	2	2	2
8. Практична здійсненність (наявність фахівців)	4	4	4
9. Практична здійсненність (наявність фінансів)	2	3	2
10. Практична здійсненність (необхідність нових матеріалів)	3	4	4

11. Практична здійсненність (термін реалізації)	2	2	2
12. Практична здійсненність (розробка документів)	3	3	3

Продовження таблиці 4.1 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Сума балів	36	36	37
Середньоарифметична сума балів $СБ_c$	36,3		

За результатами розрахунків, наведених в таблиці 4.1, зробимо висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки. При цьому використаємо рекомендації, наведені в [37].

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Радіотехнічна система контролю доступу з ідентифікацією особи» становить 36,3 бала, що, відповідно до [37], свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вище середнього).

4.2 Розрахунок узагальненого коефіцієнта якості розробки

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення розрахуємо за формулою 4.1 [36].

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i , \qquad (4.1)$$

де k – кількість найбільш важливих технічних показників, які впливають на якість нового технічного рішення;

α_i – коефіцієнт, який враховує питому вагу *і-го* технічного показника в загальній якості розробки. Коефіцієнт α_i визначається експертним шляхом і при цьому має виконуватись умова $\sum_{i=1}^{k} \alpha_i = 1$;

β_i – відносне значення *і-го* технічного показника якості нової розробки.

Результати порівняння зведемо до таблиці 4.2.

Таблиця 4.2 – Порівняння основних параметрів розробки та аналога

Показники (параметри)	Одиниця вимірю-вання	Аналог	Проектований продукт	Відношення параметрів нової розробки до аналога	Питома вага показника
Напруга живлення	В	12	5	2,1	0,3
Споживана потужність	Вт	36	25	1,44	0,15
Зчитування RFID	МГц	-	13,56	3	0,2
Роздільна здатність камери	Мп	8	12	1,5	0,25
Підтримуваний формат зображення	р	720	1080	1,44	0,1

Узагальнений коефіцієнт якості ($B_н$) для нового технічного рішення складе

$$B_н = \sum_{i=1}^{k} \alpha_i \cdot \beta_i = 2{,}1 \cdot 0{,}3 + 1{,}44 \cdot 0{,}15 + 3 \cdot 0{,}2 + 1{,}5 \cdot 0{,}25 + 1{,}44 \cdot 0{,}1 = 1{,}97.$$

Отже за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,97 рази.

4.3 Розрахунок витрат на проведення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Радіотехнічна система контролю доступу з ідентифікацією особи», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.3.1 Витрати на оплату праці

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою 4.2 [37].

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (4.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, (грн.);

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$$З_о = 17210{,}00 \cdot 7 / 21 = 5409{,}11 \ (грн.).$$

Проведені розрахунки зведемо до таблиці 4.3.

Таблиця 4.3 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, (грн.)	Оплата за робочий день, (грн.)	Число днів роботи	Витрати на заробітну плату, (грн.)
Керівник проекту	17210,00	772,73	7	5409,11
Інженер-розробник програмного забезпечення	16670,00	750,00	21	15750,00
Провідний фахівець дослідження біометричних характеристик людини	8230,00	681,82	12	8181,84
Інженер-конструктор радіоелектронної апаратури	16000,00	761,90	32	24380,95
Всього				53721,90

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Радіотехнічна система контролю доступу з ідентифікацією особи» розраховуємо за формулою 4.3.

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i, \quad (4.3)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, (грн/год.);

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою 4.4.

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \quad (4.4)$$

де M_M – розмір мінімальної місячної заробітної плати, приймемо $Мм$=8000,00 (грн.);

K_i – коефіцієнт міжкваліфікаційного співвідношення (табл. Б.2, додаток Б) [14];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок;

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$$C_1 = 8000{,}00 \cdot 1{,}10 \cdot 1{,}15 / (21 \cdot 8) = 60{,}24 \text{ (грн.)}.$$

$$З_{р1} = 60{,}24 \cdot 7{,}30 = 439{,}74 \text{ (грн.)}.$$

Таблиця 4.4 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, (грн.)	Величина оплати на робітника (грн.)
Установка обладнання для розробки радіотехнічної системи контролю	7,30	2	1,10	60,24	439,74
Підготовка робочого місця розробника радіотехнічної системи	6,10	3	1,35	73,93	450,96
Інсталяція програмного забезпечення для розпізнавання зображення	5,65	5	1,70	93,10	525,99

Продовження таблиці 4.4 – Величина витрат на основну заробітну плату робітників

Компіляція програмних блоків	4,00	4	1,50	82,14	328,57
Налагодження програмних блоків	4,30	5	1,70	93,10	400,31
Формування бази даних результатів дослідження	12,00	4	1,50	82,14	985,71
Налаштування обладнання системи контролю доступу з ідентифікацією особи	5,40	5	1,70	93,10	502,71
Всього					3634,00

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$$З_{дод} = (53721{,}90 + 3634{,}00) \cdot 11 / 100\% = 6309{,}15 \text{ (грн.)}.$$

4.3.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.6)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

$$Зн = (53721{,}90 + 3634{,}00 + 6309{,}15) \cdot 22 / 100\% = 14006{,}31 \text{ (грн.)}.$$

4.3.3 Сировина та матеріали

Витрати на матеріали (*М*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}\ , \qquad (4.7)$$

де H_j – норма витрат матеріалу *j*-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу *j*-го найменування, (грн./кг);

K_j – коефіцієнт транспортних витрат, (K_j = *1,1 … 1,15*);

B_j – маса відходів *j*-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, (грн/кг.).

$$M_1 = 4{,}0 \cdot 206{,}00 \cdot 1{,}12 - 0 \cdot 0 = 922{,}88\ (грн.).$$

Проведені розрахунки зведемо до таблиці 4.5.

Таблиця 4.5 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, (грн.)	Норма витрат, кг	Величина відходів, кг	Ціна відходів, (грн/кг.)	Вартість витраченого матеріалу, (грн.)
Папір канцелярський офісний (А4)	206,00	4,0	0	0	922,88
Папір для заміток (А5)	120,00	3,0	0	0	403,20
Начиння канцелярське	178,00	3,0	0	0	598,08
Органайзер офісний	199,00	4,0	0	0	891,52

Продовження таблиці 4.5 – Витрати на матеріали

Картридж для принтера	2018,00	1,0	0	0	2260,16
Патч-корд RJ-45 1м	24,00	1,0	0	0	26,88
Припой ПОС-61	564,00	0,001	0	0	0,63
Флюс-гель ВК-223	354,00	0,001	0	0	0,40
Всього					5103,75

4.3.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Радіотехнічна система контролю доступу з ідентифікацією особи», розраховуємо, згідно з їхньою номенклатурою, за формулою 4.8.

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \qquad (4.8)$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, (грн.);

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ *= 1,1 … 1,15*).

$$К_в = 1 \cdot 4931{,}00 \cdot 1{,}12 = 5522{,}72 \text{ (грн.)}.$$

Проведені розрахунки зведемо до таблиці 4.6.

Таблиця 4.6 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, (грн.)	Сума, (грн.)
Мікрокомп'ютер Raspberry Pi5 – 1шт.	1	4931,00	5522,72
Пристрій для візуального розпізнавання Pi Camera – 1шт.	1	852,00	954,24
Дисплей Raspberry Pi 5.0inch LCD 800x480.	1	1799,00	2014,88

Продовження таблиці 4.6 – Витрати на комплектуючі

Зчитувач фізичних носіїв RFID\NFC – PN532 v3 – 1шт.	1	255,00	285,60
ІЧ світлодіод TSAL6100 – 4шт.	4	25,00	112,00
Червоний світлодіод – 1шт.	1	7,95	8,90
Зелений світлодіод – 1шт.	1	6,50	7,28
Резистор 220 Ом – 6шт.	6	5,40	36,29
Активний зумер – 1шт.	1	33,00	36,96
SRD-12VDC-SL-C - Реле електромеханічне 12В (10A/250VAC) – 2шт.	2	64,00	143,36
Корпус пристрою	1	248,00	277,76
Всього			9399,99

4.3.5 Спецустаткування для наукових (експериментальних) робіт

Балансову вартість спецустаткування розраховуємо за формулою 4.9.

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \ , \qquad (4.9)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, (грн.);

$C_{пр.i}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань устаткування.

$$B_{спец} = 6300,00 \cdot 1 \cdot 1,12 = 7056,00 \ (грн.).$$

Отримані результати зведемо до таблиці 4.7.

Таблиця 4.7 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, (грн.)	Вартість, (грн.)
Блок інтерфейсний	1	6300,00	7056,00
Мультиметр Uni-t UT61D	1	6200,00	6944,00
Осцилограф FNIRSI-2C23T	1	4300,00	4816,00
Всього			18816,00

4.3.6 Програмне забезпечення для наукових (експериментальних) робіт

Балансову вартість програмного забезпечення розраховуємо за формулою 4.10.

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \ , \qquad (4.10)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, (грн.);

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$$B_{прг} = 4520,00 \cdot 1 \cdot 1,05 = 4746,00 \text{ (грн.)}.$$

Отримані результати зведемо до таблиці 4.8.

Таблиця 4.8 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, (грн.)	Вартість, (грн.)
Пакет Visual System Simulator	1	4520,00	4746,00
Пакет Microwave Office	1	3710,00	3895,50
EASY EDA – для проектування електричних схем та друкованих плат	1	5480,00	5754,00

Продовження таблиці 4.8 – Витрати на придбання програмних засобів по кожному виду

Програмне забезпечення MATLAB 7.0	1	7770,00	8158,50
Всього			22554,00

4.3.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою 4.11.

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, (грн.);

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$$A_{обл} = (27799{,}00 \cdot 2) / (3 \cdot 12) = 1544{,}39 \text{ (грн.)}.$$

Проведені розрахунки зведемо до таблиці 4.9.

Таблиця 4.9 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, (грн.)	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, (грн.)
Персональний комп'ютер розробника програмного забезпечення	27799,00	3	2	1544,39
Робоче місце інженера-програміста	7250,00	5	2	241,67

Продовження таблиці 4.9 – Амортизаційні відрахування по кожному виду обладнання

Пристрої передачі даних	6510,00	5	2	217,00
Офісна оргтехніка	7960,00	5	2	265,33
Приміщення лабораторії розробки	405000,00	25	2	2700,00
Електронно-обчислювальний комплекс	48500,00	2	2	4041,67
ОС Windows 11	6600,00	3	2	366,67
Прикладний пакет Microsoft Office 2019	6700,00	3	2	372,22
Робоче місце інженера-конструктора РЕА	7800,00	5	2	260,00
Всього				10008,94

4.3.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою 4.12.

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, (грн.); приймемо $Ц_e$ = 10,98 (грн.);

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$$B_e = 0,24 \cdot 200,0 \cdot 10,98 \cdot 0,95 / 0,97 = 527,04 \text{ (грн.)}.$$

Проведені розрахунки зведемо до таблиці 4.10.

Таблиця 4.10 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, (грн.)
Персональний комп'ютер розробника програмного забезпечення	0,24	200,0	527,04
Робоче місце інженера-програміста	0,10	200,0	219,60
Пристрої передачі даних	0,03	200,0	65,88
Офісна оргтехніка	0,65	1,5	10,71
Електронно-обчислювальний комплекс	0,40	200,0	878,40
Мультиметр Uni-t UT61D	0,02	50,0	10,98
Осцилограф FNIRSI-2C23T	0,01	50,0	5,49
Робоче місце інженера-конструктора РЕА	0,10	200,0	219,60
Всього			1937,70

4.3.9 Службові відрядження

Витрати за статтею «Службові відрядження» відсутні.

4.3.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою 4.13.

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.13)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$$B_{сп} = (53721,90 + 3634,00) \cdot 30 / 100\% = 17206,77 \text{ (грн.)}.$$

4.3.11 Інші витрати

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою 4.14.

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.14)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 50%.

$$I_в = (53721,90 + 3634,00) \cdot 50 / 100\% = 28677,95 \text{ (грн.)}.$$

4.3.12 Накладні (загальновиробничі) витрати

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою 4.15.

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.15)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$$В_{нзв} = (53721,90 + 3634,00) \cdot 100 / 100\% = 57355,90 \text{ (грн.)}.$$

Витрати на проведення науково-дослідної роботи на тему «Радіотехнічна система контролю доступу з ідентифікацією особи» розраховуємо як суму всіх попередніх статей витрат за формулою 4.16.

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + I_в + В_{нзв}. \quad (4.16)$$

$$B_{заг} = 53721,90 + 3634,00 + 6309,15 + 14006,31 + 5103,75 + 9399,99 + 18816,00 + 22554,00 + 10008,94 + 1937,70 + 0,00 + 17206,77 + 28677,95 + 57355,90 = 248732,37 \text{ (грн.)}.$$

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою 4.17.

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.17)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,95.

$$ЗВ = 248732,37 / 0,95 = 261823,54 \text{ (грн.)}.$$

4.4 Розрахунок економічної ефективності науково-технічної розробки при її можливій комерціалізації потенційним інвестором

Результати дослідження проведені за темою «Радіотехнічна система контролю доступу з ідентифікацією особи» передбачають комерціалізацію протягом 4-х років реалізації на ринку.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних.

ΔN – збільшення кількості споживачів пристрою, у періоди часу, що аналізуються, від покращення його певних характеристик;

Показник	1-й рік	2-й рік	3-й рік	4-й рік
Збільшення кількості споживачів, осіб	50	75	90	75

N – кількість споживачів які використовували аналогічний пристрій у році до впровадження результатів нової науково-технічної розробки, приймемо 5000 осіб;

$Ц_б$ – вартість пристрою у році до впровадження результатів розробки, приймемо 15000,00 (грн.);

$\pm\Delta Ц_о$ – зміна вартості пристрою від впровадження результатів науково-технічної розробки, приймемо 475,00 (грн.).

Можливе збільшення чистого прибутку у потенційного інвестора $\Delta П_i$ для кожного із 4-х років, протягом яких очікується отримання позитивних результатів від можливого впровадження та комерціалізації науково-технічної розробки, розраховуємо за формулою 4.18 [37].

$$\Delta П_i = (\pm\Delta Ц_о \cdot N + Ц_о \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (4.18)$$

де λ – коефіцієнт, який враховує сплату потенційним інвестором податку на додану вартість. У 2024 році ставка податку на додану вартість складає 20%, а коефіцієнт $\lambda = 0,8333$;

ρ – коефіцієнт, який враховує рентабельність інноваційного продукту). Приймемо ρ =38%;

ϑ – ставка податку на прибуток, який має сплачувати потенційний інвестор, у 2024 році $\vartheta = 18\%$;

Збільшення чистого прибутку 1-го року.

$\Delta П_1$ =(475,00·5000,00+15475,00·50)·0,83·0,38·(1-0,18/100%)=814354,92 (грн.).

Збільшення чистого прибутку 2-го року.

$\Delta П_2$ =(475,00·5000,00+15475,00·125)·0,83·0,38·(1-0,18/100%)=1114525,04 (грн.).

Збільшення чистого прибутку 3-го року.

$\Delta П_3$ =(475,00·5000,00+15475,00·215)·0,83·0,38·(1-0,18/100%)=1474729,18 (грн.).

Збільшення чистого прибутку 4-го року.

$\Delta П_4$ =(475,00·5000,00+15475,00·290)·0,83·0,38·(1-0,18/100%)=1774899,31 (грн.).

Приведена вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки за формулою 4.19.

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.19)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, (грн.);

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження та комерціалізації науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, τ =0,11;

t – період часу (в роках) від моменту початку впровадження науково-технічної розробки до моменту отримання потенційним інвестором додаткових чистих прибутків у цьому році.

$$ПП = 814354,92/(1+0,11)^1+1114525,04/(1+0,11)^2+1474729,18/(1+0,11)^3+$$
$$+1774899,31/(1+0,11)^4=733653,08+904573,52+1078309,27+1169181,15=$$
$$= 3885717,02 \text{ (грн.)}.$$

Величина початкових інвестицій PV, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки за формулою 4.20.

$$PV = k_{інв} \cdot ЗВ, \quad (4.20)$$

де $k_{інв}$ – коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію, приймаємо $k_{інв}$ =2;

$ЗВ$ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, приймаємо 261823,54 (грн.).

$$PV = k_{інв} \cdot ЗВ = 2 \cdot 261823{,}54 = 523647{,}09 \text{ (грн.)}.$$

Абсолютний економічний ефект $E_{абс}$ для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки розраховується за формулою 4.21.

$$E_{абс} = ПП - PV \tag{4.21}$$

де $ПП$ – приведена вартість зростання всіх чистих прибутків від можливого впровадження та комерціалізації науково-технічної розробки, 3885717,02 (грн.);

PV – теперішня вартість початкових інвестицій, 523647,09 (грн.).

$$E_{абс} = ПП - PV = 3885717{,}02 - 523647{,}09 = 3362069{,}93 \text{ (грн.)}.$$

Внутрішня економічна дохідність інвестицій $E_в$, які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки розраховується за формулою 4.22.

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{4.22}$$

де $E_{абс}$ – абсолютний економічний ефект вкладених інвестицій, 3362069,93 (грн.);

PV – теперішня вартість початкових інвестицій, 523647,09 (грн.);

$T_ж$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, 4 роки.

$$E_в = \sqrt[Tж]{1 + \frac{E_{абс}}{PV}} - 1 = (1+3362069{,}93/523647{,}09)^{1/4} = 0{,}65.$$

Мінімальна внутрішня економічна дохідність вкладених інвестицій $\tau_{мін}$ розраховується за формулою 4.23.

$$\tau_{мін} = d + f, \quad (4.23)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2024 році в Україні d =0,11;

f – показник, що характеризує ризикованість вкладення інвестицій, приймемо 0,3.

$\tau_{мін}$ = 0,11+0,3 = 0,41 < 0,65 свідчить про те, що внутрішня економічна дохідність інвестицій $E_в$, вища мінімальної внутрішньої дохідності. Тобто інвестувати в науково-дослідну роботу за темою «Радіотехнічна система контролю доступу з ідентифікацією особи» доцільно.

Період окупності інвестицій $T_{ок}$ які можуть бути вкладені потенційним інвестором у впровадження та комерціалізацію науково-технічної розробки розраховується за формулою 4.24.

$$T_{ок} = \frac{1}{E_в}, \quad (4.24)$$

де $E_в$ – внутрішня економічна дохідність вкладених інвестицій.

$T_{ок}$ = 1 / 0,65 = 1,54 р.

$T_{ок}$ < 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

4.5 Висновки до розділу

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Радіотехнічна система контролю доступу з ідентифікацією особи»

становить 36,3 бала, що, свідчить про комерційну важливість проведення даних досліджень (рівень комерційного потенціалу розробки вище середнього).

При оцінюванні за технічними параметрами, згідно узагальненого коефіцієнту якості розробки, науково-технічна розробка переважає існуючі аналоги приблизно в 1,97 рази.

Також термін окупності становить 1,54 р., що менше 3-х років, що свідчить про комерційну привабливість науково-технічної розробки і може спонукати потенційного інвестора профінансувати впровадження даної розробки та виведення її на ринок.

Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Радіотехнічна система контролю доступу з ідентифікацією особи».

ВИСНОВКИ

У ході виконання магістерської кваліфікаційної роботи було розроблено радіотехнічну систему контролю доступу з ідентифікацією особи, яка забезпечує двофакторну автентифікацію, поєднуючи RFID-ідентифікацію та технології розпізнавання обличчя. Такий підхід дозволяє значно підвищити рівень безпеки, надійності та точності ідентифікації осіб у зоні з обмеженим доступом.

Під час виконання роботи проведено аналіз сучасних систем контролю доступу, їхніх функцій, переваг і недоліків, а також порівняння різних методів ідентифікації особи. Особливу увагу приділено біометричним методам, які виявилися найбільш перспективними завдяки високій точності та надійності. На основі отриманих даних було розроблено структуру, апаратну частину та програмне забезпечення запропонованої системи.

Структурна схема і принципова електрична схема системи були створені за допомогою САПР EASYEDA. Система реалізована на основі мікрокомп'ютера Raspberry Pi 5, оснащеного модулем Pi Camera для візуального розпізнавання, RFID-зчитувачем PN532 v3 для ідентифікації фізичних носіїв, а також іншими компонентами для забезпечення функціональності, включаючи дисплей, світлодіоди, реле та зумер. Розроблено алгоритм роботи системи, що забезпечує інтеграцію всіх компонентів у єдину функціональну структуру.

Розроблена система має значний практичний потенціал для використання в різних сферах, включаючи підприємства, установи та об'єкти з підвищеними вимогами до безпеки. Вона забезпечує не лише високий рівень захисту, але й зручність використання, гнучкість та можливість адаптації до різних умов експлуатації. Запропонована система може стати основою для впровадження нових підходів до управління доступом, спрямованих на підвищення ефективності захисту територій і приміщень та зменшення ризиків несанкціонованого проникнення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Технології контролю доступу для корпоративних систем [Електронний ресурс]. – Режим доступу: https://corporatescud-tech.com.

2. Dobkin, D. M. The RF in RFID: Passive UHF RFID in Practice. – Newnes, 2012.

3. Finkenzeller, K. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication. – Wiley, 2010.

4. Коваль, О. М. Радіотехнічні системи в системах безпеки. – Одеса, 2020.

5. Принципи функціонування сучасних RFID-систем [Електронний ресурс]. – Режим доступу: https://rfid-system-tech.com.

6. Формування ефективності використання RFID [Електронний ресурс]. – Режим доступу: https://rfidworld.com/articles.

7. Притула, М. О. Основи розробки систем контролю доступу. – Вінниця, 2023.

8. Наукова електронна бібліотека періодичних видань НАН України [Електронний ресурс]. – Режим доступу: http://dspace.nbuv.gov.ua/.

9. ResearchGate [Електронний ресурс]. – Режим доступу: https://www.researchgate.net.

10. Daugman, J. How Iris Recognition Works. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 21-30, 2009.

11. Jain, A., Ross, A., & Prabhakar, A. An Introduction to Biometric Recognition. – Springer, 2007.

12. Особливості використання біометрії в умовах критичної інфраструктури [Електронний ресурс]. – Режим доступу: https://biometricsecurity.com/articles.

13. Психологічні та технічні аспекти розпізнавання обличчя [Електронний ресурс]. – Режим доступу: https://facerecognition-psychtech.com.

14. Удосконалення методів ідентифікації в СКУД [Електронний ресурс]. – Режим доступу: https://scud-dev.com/articles.

15. IEEE Transactions on Information Forensics and Security [Електронний ресурс]. – Режим доступу: https://ieeexplore.ieee.org/Xplore/home.jsp.

16. ISO/IEC 19795 [Електронний ресурс]. – Режим доступу: https://www.nist.gov/system/files/documents/2020/12/15/340_1_mansfield_panel_ibpc.pdf.

17. Жайн, А., Росс, А., Прабхакар, А. Методи біометричної автентифікації. – Київ, 2017.

18. Критерії оцінки ефективності біометричних систем [Електронний ресурс]. – Режим доступу: https://biometricsefficiency.com/articles.

19. Переваги й недоліки біометричного захисту [Електронний ресурс]. – Режим доступу: https://worldvision.com.ua/preimushchestva-i-nedostatki-biometricheskoy-sistemy-autentifikatsii.

20. Форми біометричної автентифікації [Електронний ресурс]. – Режим доступу: https://worldvision.com.ua/articles/formi–biometricheskoy–autentifikatsii.

21. Мельник, В. В. Автоматизація процесів ідентифікації у СКУД. – Львів, 2019.

22. Szeliski, R. Computer Vision: Algorithms and Applications. – Springer, 2010.

23. Szeliski, R. Computer Vision: Algorithms and Applications. – Springer, 2021.

24. ISO/IEC 14443 A/B [Електронний ресурс]. – Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=52942

25. Удосконалення методів використання Raspberry Pi [Електронний ресурс]. – Режим доступу: https://raspberrypidevelopment.com.

26. Raspberry Pi Official Documentation [Електронний ресурс]. – Режим доступу: https://www.raspberrypi.org/documentation.

27. Monk, S. Programming the Raspberry Pi: Getting Started with Python. – McGraw-Hill Education, 2019.

28. Зеліскі, Р. Алгоритми обробки зображень у комп’ютерному баченні. – Харків, 2018.

29. Halfacree, G., & Upton, E. Raspberry Pi User Guide. – Wiley, 2022.

30. Python Software Foundation [Електронний ресурс]. – Режим доступу: https://www.python.org.

31. Rosebrock, A. Practical Python and OpenCV. – PyImageSearch, 2018.

32. Bradski, G., & Kaehler, A. Learning OpenCV: Computer Vision with the OpenCV Library. – O'Reilly Media, 2008.

33. OpenCV Documentation [Електронний ресурс]. – Режим доступу: https://docs.opencv.org.

34. O’Reilly, K. Deep Learning for Computer Vision with Python. – PyImageSearch, 2019.

35. Розробка ефективних алгоритмів для OpenCV [Електронний ресурс]. – Режим доступу: https://opencv-algorithms.com.

36. Кавецький В. В., Козловський В. О., Причепа І. В. Економічне обґрунтування інноваційних рішень: практикум. – Вінниця : ВНТУ, 2016. – 113 с.

37. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

Додаток А

(обов`язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

РАДІОТЕХНІЧНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ З ІДЕНТИФІКАЦІЄЮ ОСОБИ

Виконав: студент 2-го курсу, групи РТ-23м
спеціальності 172 – Електронні комунікації та радіотехніка
(шифр і назва напряму підготовки, спеціальності)
Пехота Р.В.
(прізвище та ініціали)
Керівник: к.т.н., ст. викладач кафедри ІРТС
12.12.2024р Притула М. О.
(прізвище та ініціали)

Вінниця ВНТУ - 2024 рік

Рисунок 1 – Методи та способи ідентифікації особи

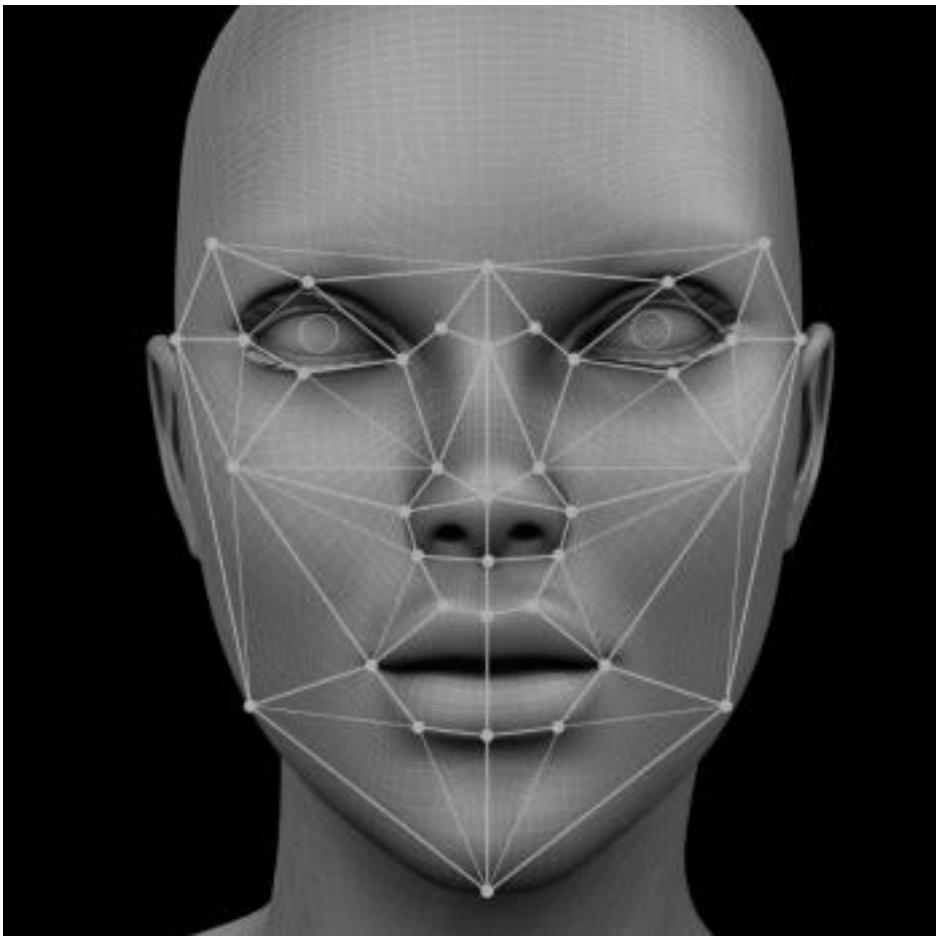

Рисунок 2 – Модель розпізнавання обличчя

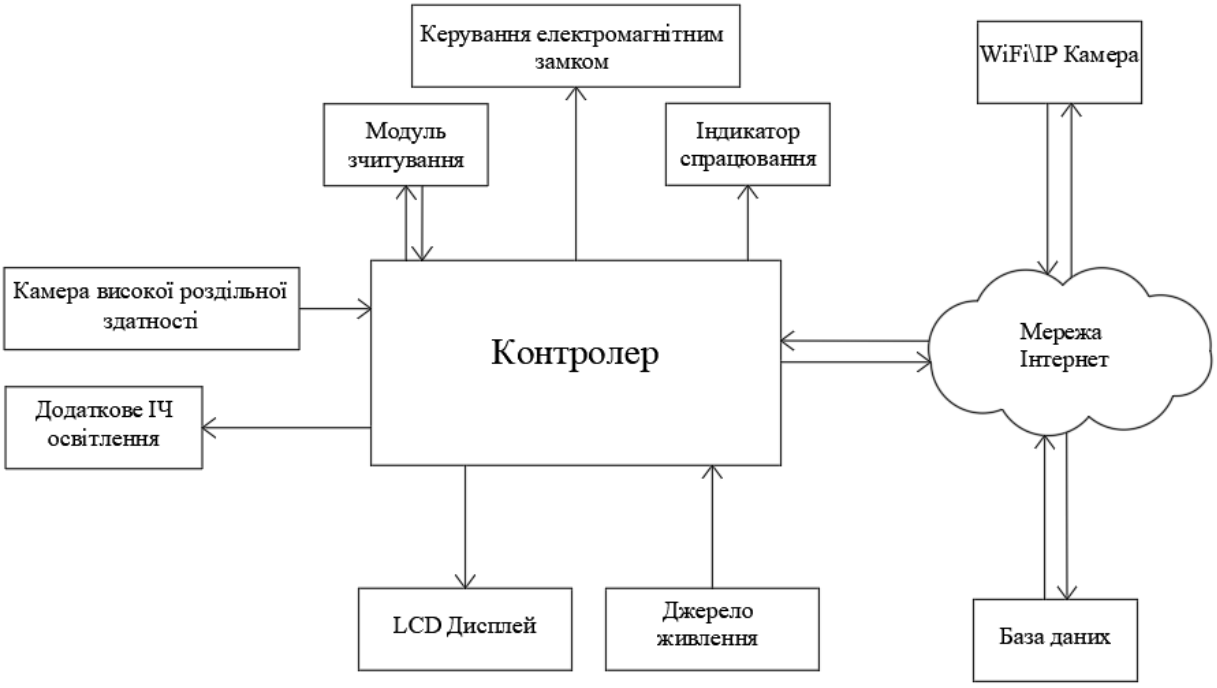

Рисунок 3 – Структурна схема радіотехнічної системи контролю доступу з ідентифікацією особи.

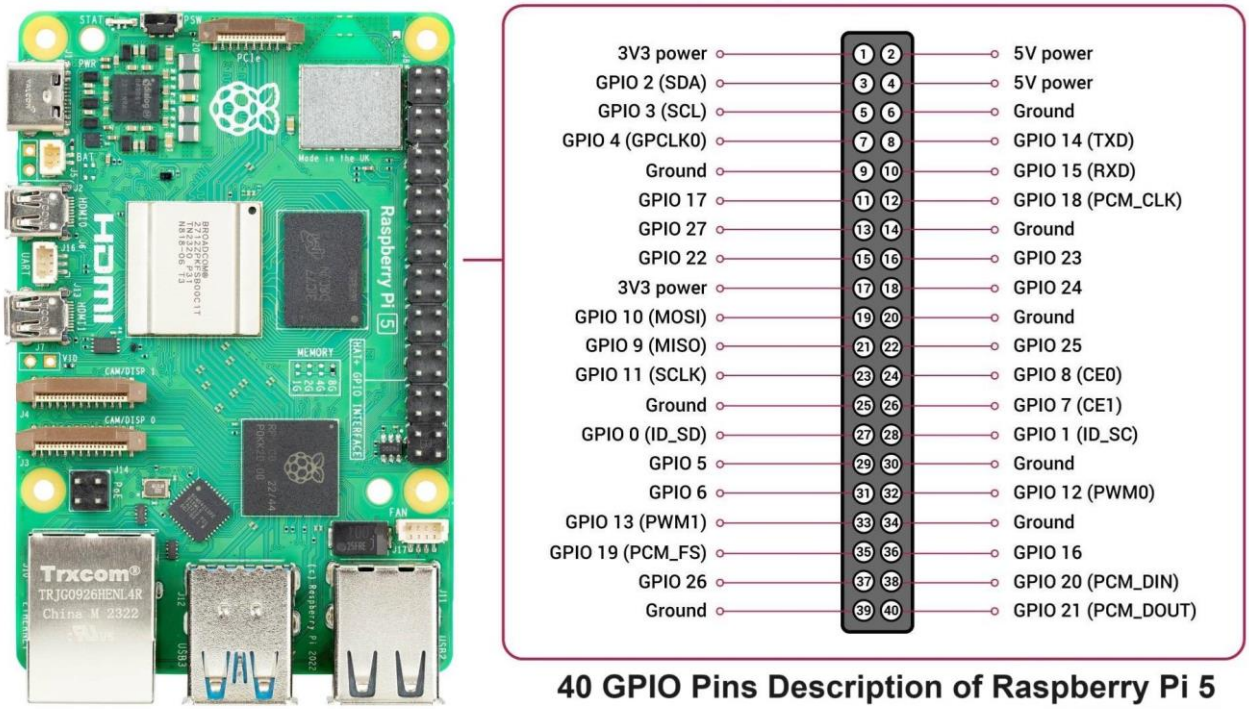

Рисунок 4 – Перелік виводів Raspberry Pi5

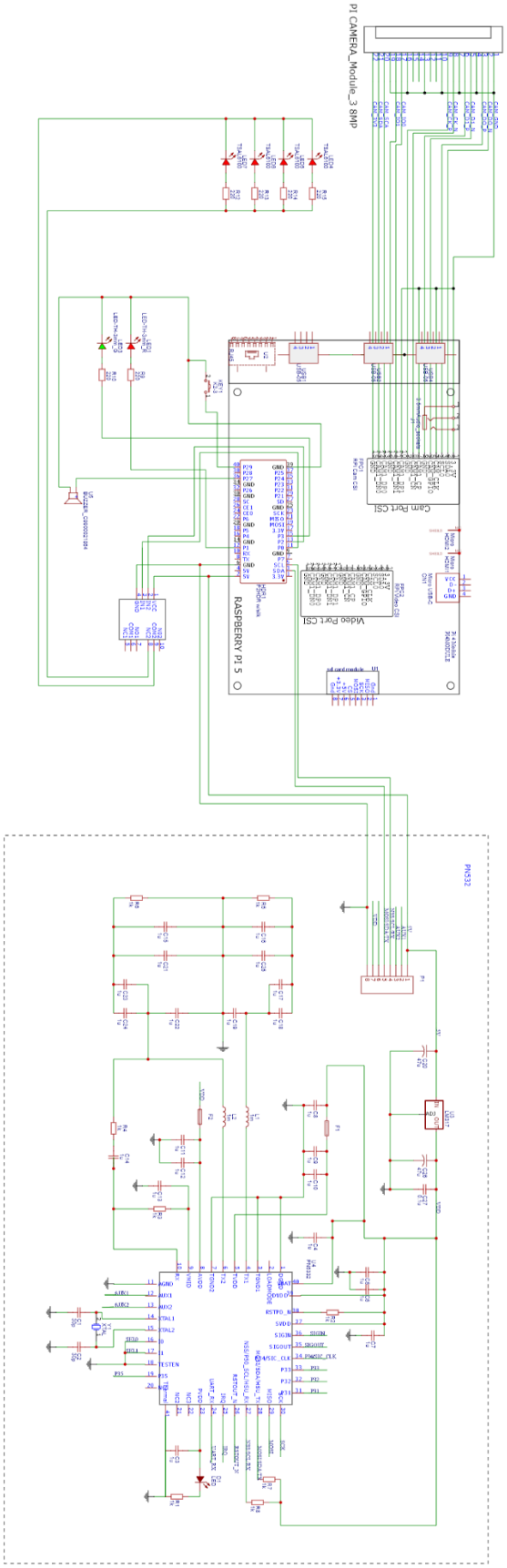

Рисунок 5 – Схема електрична принципова

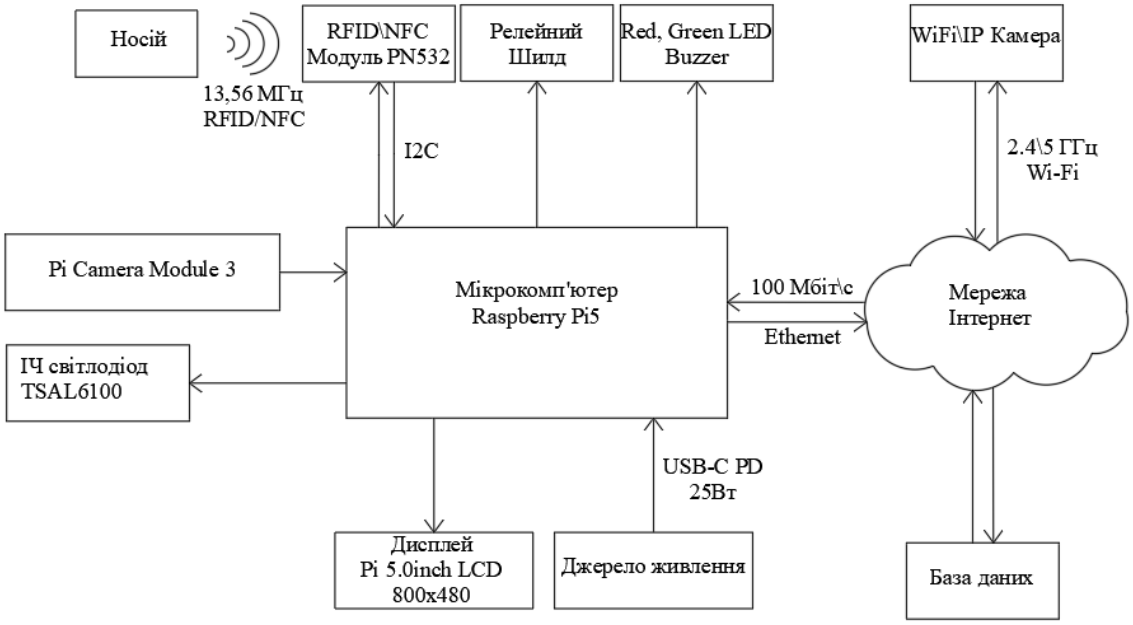

Рисунок 6 – Схема взаємодії між модулями.

Specification

Processor	Broadcom BCM2712 2.4GHz quad-core 64-bit Arm Cortex-A76 CPU, with Cryptographic Extension, 512KB per-core L2 caches, and a 2MB shared L3 cache
Features:	• VideoCore VII GPU, supporting OpenGL ES 3.1, Vulkan 1.2 • Dual 4Kp60 HDMI® display output with HDR support • 4Kp60 HEVC decoder • LPDDR4X-4267 SDRAM (options for 2GB, 4GB and 8GB) • Dual-band 802.11ac Wi-Fi® • Bluetooth 5.0 / Bluetooth Low Energy (BLE) • microSD card slot, with support for high-speed SDR104 mode • 2 × USB 3.0 ports, supporting simultaneous 5Gbps operation • 2 × USB 2.0 ports • Gigabit Ethernet, with PoE+ support (requires separate PoE+ HAT) • 2 × 4-lane MIPI camera/display transceivers • PCIe 2.0 x1 interface for fast peripherals (requires separate M.2 HAT or other adapter) • 5V/5A DC power via USB-C, with Power Delivery support • Raspberry Pi standard 40-pin header • Real-time clock (RTC), powered from external battery • Power button
Production lifetime:	Raspberry Pi 5 will remain in production until at least January 2036
Compliance:	For a full list of local and regional product approvals, please visit pip.raspberrypi.com

Рисунок 7 – Datasheet характеристики модуля Rasberry Pi5.

8.6.3.2 FeliCa Reader/Writer

The following diagram describes the communication at the physical level. Table 146 describes the physical parameters.

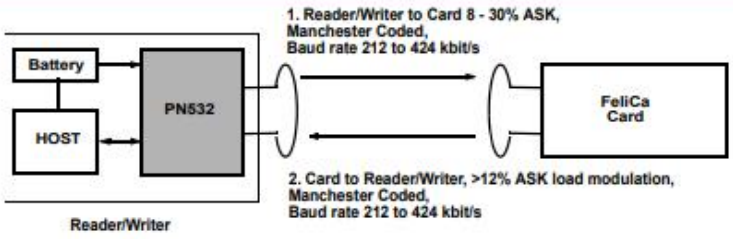

Fig 29. FeliCa Reader/Writer communication diagram

Table 146. Communication overview for FeliCa Reader/Writer

Communication scheme		FeliCa	FeliCa higher baud rate
Baud rate		**212 kbit/s**	**424 kbit/s**
Bit length		$\frac{64}{13{,}56MHz} \approx 4{,}72\mu s$	$\frac{32}{13{,}56MHz} \approx 2{,}36\mu s$
PN532 to PICC/Card	Modulation	8 - 30% ASK	8 - 30% ASK
	Bit coding	Manchester coding	Manchester coding
PICC/Card to PN532	Modulation	>12% ASK	>12% ASK
	Bit coding	Manchester coding	Manchester coding

With appropriate firmware, the PN532 can handle the FeliCa protocol.

The FeliCa Framing and coding must comply with the following table:

Table 147. FeliCa Framing and Coding

Preamble						SYNC		LEN	n-Data				CRC	
00h	00h	00h	00h	00h	00h	B2h	4Dh							

To enable the FeliCa communication a 6-byte preamble (00h, 00h, 00h, 00h, 00h, 00h) and 2-byte SYNC bytes (B2h, 4Dh) are sent to synchronize the receiver.

The following LEN byte indicates the length of the sent data bytes plus the LEN byte itself. The CRC calculation is done according to the FeliCa definitions with the MSB first.

To transmit data on the RF interface, the 80C51 has to send the LEN and data bytes to the CIU. The Preamble and SYNC bytes are generated by the CIU automatically and must not be written to the FIFO. The CIU performs internally the CRC calculation and adds the result to the frame.

The starting value for the CRC Polynomial is 2 null bytes: (00h), (00h)

Example of frame:

Table 148. FeliCa framing and coding

Preamble						SYNC		LEN	2 Data Bytes		CRC	
00	00	00	00	00	00	B2	4D	03	AB	CD	90	35

Рисунок 8 – Фрагмент Datasheet характеристик модуля RFID&NFC PN532.

Додаток Б

(обов`язковий)

ПРОТОКОЛ ПЕРЕВІРКИ РОБОТИ

РАДІОТЕХНІЧНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ З ІДЕНТИФІКАЦІЄЮ ОСОБИ

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: **«Радіотехнічна система контролю доступу з ідентифікацією особи»**

Тип роботи: МКР
(БДР, МКР)

Підрозділ IPTC, IEC
(кафедра, факультет)

Показники звіту подібності Turnitin

Оригінальність 95,0% Схожість 5,0%

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку  Андрій СЕМЕНОВ
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Turnitin щодо роботи.

Автор роботи  Роман ПЕХОТА
(підпис) (прізвище, ініціали)

Керівник роботи  Максим ПРИТУЛА
(підпис) (прізвище, ініціали)

Додаток В

(довідниковий)

Лістинг коду для системи контролю доступу з ідентифікацією особи.

```
import cv2
import numpy as np
import time
import sqlite3
import pickle
from tensorflow.keras.applications.resnet50 import ResNet50,
preprocess_input
from imutils.video import VideoStream
from sklearn.neighbors import KNeighborsClassifier
from mfrc522 import SimpleMFRC522  # Бібліотека для RFID
import RPi.GPIO as GPIO
import Adafruit_CharLCD as LCD  # Бібліотека для роботи з LCD-
дисплеєм
# === Ініціалізація модулів ===
print("[INFO] Ініціалізація системи...")
# Ініціалізація RFID/NFC модуля
reader = SimpleMFRC522()
# Завантаження моделі ResNet50
model = ResNet50(weights='imagenet', include_top=False,
input_shape=(224, 224, 3))
# Підключення до локальної бази даних
conn = sqlite3.connect('users.db')
cursor = conn.cursor()
# Підключення до камери
cap = VideoStream(src=0).start()
time.sleep(2.0)  # Затримка для запуску камери
# Налаштування GPIO
RELAY_LOCK = 17  # Пін для реле замка
EMERGENCY_BUTTON = 27  # Пін для кнопки аварійного відкриття
GPIO.setmode(GPIO.BCM)
GPIO.setup(RELAY_LOCK, GPIO.OUT, initial=GPIO.LOW)
GPIO.setup(EMERGENCY_BUTTON, GPIO.IN, pull_up_down=GPIO.PUD_UP)

# Ініціалізація LCD-дисплея
lcd = LCD.Adafruit_CharLCDPlate()
lcd.clear()
# === Функції ===
def preprocess_image(image):
    """Передобробка зображення для моделі ResNet."""
    img = cv2.resize(image, (224, 224))
    img = preprocess_input(img)
    return np.expand_dims(img, axis=0)
def recognize_face(image, model, knn_model):
    """Розпізнає обличчя на основі зображення."""
```

```
    processed_img = preprocess_image(image)
    features = model.predict(processed_img).flatten()
    user_id = knn_model.predict([features])[0]
    return user_id
def read_rfid():
    """Зчитує RFID/NFC мітку."""
    try:
        rfid_id, text = reader.read()
        return text.strip()
    except Exception as e:
        lcd.clear()
        lcd.message("Помилка RFID!")
        print(f"[ERROR] Помилка зчитування RFID: {e}")
        return None
def check_access(rfid, face_id):
    """Перевіряє відповідність даних з бази та повертає статус
доступу."""
    cursor.execute("SELECT * FROM users WHERE rfid_id = ?",
(rfid,))
    user = cursor.fetchone()
    if user and str(user[0]) == str(face_id):
        lcd.clear()
        lcd.message(f"Доступ надано\n{user[1]}")
        print(f"[ACCESS GRANTED] Користувач: {user[1]}")
        return True
    lcd.clear()
    lcd.message("Доступ заборонено")
    print("[ACCESS DENIED] Невідповідність даних.")
    return False
def open_door():
    """Відкриває двері на кілька секунд."""
    lcd.clear()
    lcd.message("Двері відкриті")
    print("[INFO] Двері відкриті.")
    GPIO.output(RELAY_LOCK, GPIO.HIGH)
    time.sleep(3)  # Тримати двері відкритими 3 секунди
    GPIO.output(RELAY_LOCK, GPIO.LOW)
    lcd.clear()
    lcd.message("Двері зачинені")
    print("[INFO] Двері зачинені.")
def emergency_open(channel):
    """Відкриває двері при натисканні кнопки аварійного
відкриття."""
    lcd.clear()
    lcd.message("Аварійне\nвідкриття")
    print("[EMERGENCY] Аварійне відкриття дверей.")
    open_door()
# Налаштування переривання для кнопки аварійного відкриття
GPIO.add_event_detect(EMERGENCY_BUTTON, GPIO.FALLING,
callback=emergency_open, bouncetime=300)

# === Основний цикл роботи ===
print("[INFO] Система запущена. Очікування користувача...")
lcd.message("Система готова")
# Завантаження KNN моделі
```

```
with open('knn_model.sav', 'rb') as f:
    knn_model = pickle.load(f)
try:
    while True:
        # Зчитування RFID/NFC
        rfid = read_rfid()
        if not rfid:
            continue
        print(f"[INFO] Зчитано RFID: {rfid}")
        lcd.clear()
        lcd.message(f"RFID: {rfid}")
        # Розпізнавання обличчя
        frame = cap.read()
        gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
        face_cascade = cv2.CascadeClassifier(cv2.data.haarcascades
+ "haarcascade_frontalface_default.xml")
        faces = face_cascade.detectMultiScale(gray,
scaleFactor=1.1, minNeighbors=5, minSize=(30, 30))
        if len(faces) > 0:
            (x, y, w, h) = faces[0]  # Перший знайдений об'єкт
            face_roi = frame[y:y+h, x:x+w]
            try:
                face_id = recognize_face(face_roi, model,
knn_model)
                print(f"[INFO] Розпізнано обличчя: {face_id}")
                lcd.clear()
                lcd.message(f"Обличчя: {face_id}")
                # Перевірка доступу
                if check_access(rfid, face_id):
                    open_door()
                else:
                    print("[INFO] Доступ заборонено.")
            except Exception as e:
                lcd.clear()
                lcd.message("Помилка обличчя!")
                print(f"[ERROR] Помилка розпізнавання обличчя:
{e}")
        else:
            lcd.clear()
            lcd.message("Обличчя не знайдено")
            print("[INFO] Обличчя не знайдено.")
        time.sleep(1)
except KeyboardInterrupt:
    print("[INFO] Завершення роботи...")
finally:
    GPIO.cleanup()
    cap.stop()
    conn.close()
```