НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

«На правах рукопису»
УДК _004.93_

До захисту допущено:
Завідувач кафедри
_____ Олександр РОЛІК
«___»_____2024 р.

Магістерська дисертація
на здобуття ступеня магістра
за освітньо– професійною програмою «Інформаційне забезпечення робототехнічних систем»
зі спеціальності 126 «Інформаційні системи та технології»
на тему: «Система контролю доступу та ідентифікації осіб на режимних об'єктах»

Виконала:
студентка 2 курсу, групи ІК– 21мп
Левченко Аліна Віталіївна _____

Керівник:
Доцент кафедри ІСТ, к.т.н., доцент
Пасько Віктор Петрович _____

Рецензент:
Доцент кафедри інформаційної безпеки,
КПІ ім. Ігоря Сікорського, к.т.н., доцент,
Коломицев Михайло Володимирович _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студентка _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки
Кафедра інформаційних систем та технологій

Рівень вищої освіти – другий (магістерський)

Спеціальність – 126 «Інформаційні системи та технології»

Освітньо– професійна програма «Інформаційне забезпечення робототехнічних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Олександр РОЛІК
«___»_____2024 р.

ЗАВДАННЯ
на магістерську дисертацію студентці
Левченко Аліні Віталіївні

1. Тема дисертації «Система контролю доступу та ідентифікації осіб на режимних об’єктах», науковий керівник дисертації Пасько Віктор Петрович, д.т.н., доцент, затверджені наказом по університету від «07» 11 2023 р. № 5168– с.

2. Термін подання студентом дисертації «08» 01 2024 р.

3. Об’єкт дослідження: Система розпізнавання облич та відбитків пальців для контролю доступу та ідентифікації осіб у режимних об'єктах за допомогою нейромереж.

4. Вихідні дані: наукова література по темі, існуючі моделі систем.

5. Перелік завдань, які потрібно розробити: загальний аналіз систем контролю доступу, аналіз методів біометричної ідентифікації, аналіз архітектур нейронних мереж, вдосконалення архітектури для, розробка системи.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу: 8

7. Дата видачі завдання 01.09.2023 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз системи контролю та управління доступом	04.09.2023 – 10.09.2023	
2	Вибір СКУД та постановка задачі	11.09.2023 – 17.09.2023	
3	Аналіз методів ідентифікації осіб	18.09.2023 – 24.10.2023	
4	Огляд сучасних методів біометричної ідентифікації	25.09.2023 – 08.10.2023	
5	Аналіз існуючих архітектур нейромереж	09.10.2023 – 15.10.2023	
6	Розробка нейронної мережі	16.10.2023 – 05.11.2023	
7	Тестування НМ та її вдосконалення	06.11.2023 – 19.11.2023	
8	Розробка додатку для контролю доступу на режимних об’єктах	20.11.2023 – 17.12.2023	
9	Тестування додатку	18.12.2023 – 24.12.2023	
10	Розробка стартап-проєкту	25.12.2023 – 31.12.2023	
11	Оформлення звіту	01.12.2023 – 07.01.2024	
12	Захист диплому	08.01.2024	

Студентка Аліна ЛЕВЧЕНКО

Науковий керівник Віктор ПАСЬКО

РЕФЕРАТ

Система контролю доступу та ідентифікації осіб на режимних об’єктах: 118 с., 34 табл., 57 рис., 10 дод., 22 джерел.

БІОМЕТРИЧНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ, БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ, НЕЙРОННА МЕРЕЖА, РОЗПІЗНАВАННЯ ОБЛИЧ, РОЗПІЗНАВАННЯ ВІДБИТКІВ ПАЛЬЦІВ

Актуальність теми. На сучасному етапі розвитку інформаційних технологій надзвичайно важливим завданням є забезпечення надійного захисту інформації. В Україні ефективна ідентифікація користувачів, які отримують доступ до об'єктів з особливим режимом, залишається актуальною і невирішеною проблемою. Таким чином, розробка такої системи має велике значення та є важливим кроком у напрямку посилення безпеки та виявлення потенційних загроз. Це особливо актуально, оскільки багато об'єктів містять конфіденційну інформацію або цінні ресурси, які необхідно якісно захищати від несанкціонованого доступу. Впровадження такої системи може помітно знизити ризик несанкціонованого доступу та виявити підозрілі особи.

Мета та задачі дослідження. Метою дослідження є оптимізація методів розпізнавання та проєктування системи контролю доступу та ідентифікації осіб на режимних об'єктах.

Об’єкт дослідження. Система розпізнавання облич та відбитків пальців для контролю доступу та ідентифікації осіб у режимних об'єктах за допомогою нейромереж.

Предмет дослідження. Засоби та методи оптимізації систем контролю та управління доступом до режимних об’єктів.

Пояснювальна записка складається з п’яти розділів. В першому розділі проведено аналіз систем, їх складові та принципи функціонування. Визначено перелік завдань, які необхідно розробити для досягнення мети. У другому розділі проведений аналіз методів біометричної ідентифікації та методів розпізнавання. В третьому розділі спроєктовано систему. В четвертому проведено тестування й покращення. В останньому розроблений стартап-проєкт.

SUMMERY

System of access control and identification of persons at regime facilitie: 118p., 34 tab., 57 draw., 10 app., 22 sources.

BIOMETRIC ACCESS CONTROL SYSTEM, BIOMETRIC IDENTIFICATION AND AUTHENTICATION, NEURAL NETWORK, FACIAL RECOGNITION, FINGERPRINT RECOGNITION

Actuality of theme. At the current stage of information technology development, ensuring reliable information protection is an extremely important task. In Ukraine, the effective identification of users who gain access to objects with a special regime remains an actual and unresolved problem. Thus, the development of such a system is of great importance and is an important step in the direction of strengthening security and identifying potential threats. This is especially relevant, since many objects contain confidential information or valuable resources that must be properly protected from unauthorized access. Implementation of such a system can significantly reduce the risk of unauthorized access and identify suspicious persons.

The purpose and objectives of the research. The purpose of the study is to optimize the methods of recognition and design of the access control system and identification of persons at regime facilities.

Object of study. Face and fingerprint recognition system for access control and identification of persons in regime facilities using neural networks.

Subject of study. Means and methods of optimization of systems of control and management of access to regime objects.

The explanatory note consists of five sections. In the first section, an analysis of the systems, their components and principles of operation was carried out. A list of tasks that must be developed to achieve the goal is defined. In the second chapter, an analysis of biometric identification methods and recognition methods is carried out. In the third section, the system is designed. In the fourth, testing and improvement was carried out. In the latter, a startup project was developed.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ ТА ПОЗНАЧЕНЬ

КД – контроль доступу

ЗІ – захист інформації

СЗІ – система захисту інформації

СКД (Access Control Systems) – система контролю доступу

СКУД – система контролю та управління доступом

MFA– багатофакторна аутентифікація

БД – база даних

НМ – нейронна мережа

ВСТУП

У наш час спостерігається збільшення кількості об'єктів інфраструктури з обмеженим доступом, які річно наростають в кількості. Проблема забезпечення безпеки цих об'єктів та контролю доступу до них стає все більш актуальною. Сучасні системи контролю доступу та ідентифікації осіб визначаються як важлива складова управління безпекою, гарантуючи високий рівень захисту інформації, ресурсів та персоналу.

Варто відзначити, що сучасні технології систем контролю доступу та ідентифікації осіб дозволяють розробляти гнучкі та інтегровані рішення. Ці системи ефективно управляють рухом осіб на території об'єкта, гарантуючи високий рівень безпеки та контролю доступу до різних зон. Розглядаються різні методи ідентифікації, такі як фізичні картки, біометричні дані, PIN-коди, електронні замки, карткові чи біометричні ключі, а також системи відеоспостереження та аналізу поведінки.

Крім того, системи контролю доступу можуть бути впроваджені в різних сферах, включаючи корпоративний сектор, державні установи, банківські установи, енергетичні об'єкти та інші об'єкти критичної інфраструктури. Вони надають можливість не лише для фізичного доступу, а й для електронного доступу до інформаційних ресурсів, що робить їх важливим елементом в галузі кібербезпеки. Використання цих систем дозволяє ефективно розв’язувати проблеми, пов'язані з втратою даних, крадіжками, терористичними атаками та іншими загрозами.

Забезпечення безпеки на об'єктах через системи контролю доступу — це не лише захист від зовнішніх атак, але й підвищення ефективності управління об'єктом, організації робочого процесу та ресурсів. Загалом, системи контролю доступу та ідентифікації осіб на об'єктах з обмеженим доступом встановлюють нові стандарти безпеки та ефективного управління, відповідаючи сучасним викликам і гарантуючи високий рівень захисту, конфіденційності та доступності.

Однією з ключових складових цих систем є ідентифікація осіб. Використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя або голосу, дозволяє створювати надійні механізми визначення осіб та уникнення можливого несанкціонованого доступу. Впровадження систем контролю доступу та ідентифікації на об'єктах з обмеженим доступом не лише запобігає потенційним загрозам безпеці, але також ефективно веде облік робочого часу, контролює вхід та вихід персоналу, а також реагує на надзвичайні ситуації.

Загалом, такі системи є необхідним елементом сучасної системи безпеки, спрямованої на мінімізацію ризиків та захист цінних ресурсів та інформації.

Актуальність роботи визначається переважно тим, що системи контролю доступу на об'єктах з обмеженим доступом включають комплекс технічних та програмних засобів безпеки, які регулюють вхід/вихід та переміщення людей на територіях під охороною, що сприяє адміністративному моніторингу та уникненню несанкціонованого проникнення.

Розробка система контролю доступу та ідентифікації осіб на режимних об’єктах є дуже актуальною для України, особливо в умовах повномасштабного вторгнення. Багато об'єктів з обмеженим доступом містять конфіденційну інформацію чи цінні ресурси, тому така система може допомогти виявляти підозрілі особи й зменшити ризик несанкціонованого доступу.

1 СИСТЕМА КОНТРОЛЮ ДОСТУПУ ТА ІДЕНТИФІКАЦІЇ ОСІБ

1.1 Загальні відомості про системи доступу

Системи контролю доступу (Access Control Systems, СКД) є технологічними рішеннями, спрямованими на обмеження чи надання доступу до конкретних об'єктів, приміщень, інформації або ресурсів. Застосовуються в різних сферах, таких як фізична безпека будівель, комп'ютерні мережі, дані, транспорт і т.д.[4].

Система контролю та управління доступом (СКУД) є комплексом програмних і апаратних засобів, що забезпечують захист об'єкта від несанкціонованого проникнення та реєстрацію входу-виходу людей або транспорту через визначені "точки" – двері, турнікети та інше[5].

Регулювання доступу існує у двох варіантах: фізичний та логічний. Фізичний контроль обмежує входження на територію будівель, сховищ чи кімнат і доступ до конкретних фізичних активів в галузі IT. З іншого боку, логічний контроль обмежує підключення до файлів, інформації та комп’ютерних мереж.

З метою забезпечення безпеки об'єктів використовують електронні СКД, що базуються на інформації про користувача, сенсорах карт доступу, аудиті та звітах для моніторингу співробітників до закритих зон. Деякі з таких систем включають в себе панелі управління доступом, які регулюють доступ до приміщень і будівель, а також обладнання сигналізації та засоби блокування для запобігання несанкціонованому доступу чи операціям.

1.2 Компоненти системи доступу

Системи контролю доступу проводять ідентифікацію, автентифікацію та авторизацію користувачів та об'єктів, аналізуючи певні дані для входу, такі як PIN-код або пароль, різноманітні картки доступу або брелок, біометричні дані, маркери безпеки та інше.

Системи доступу можуть включати різноманітні компоненти[5], такі як ідентифікація, аутентифікація, авторизація та фізичні засоби контролю доступу (наприклад, картки, біометричні системи, замки, бар'єри тощо). Ці системи застосовуються в різних сферах, таких як фізична безпека будівель, комп'ютерні мережі, об'єкти громадського транспорту та інші галузі, де необхідно обмежувати доступ лише авторизованим користувачам.

1.2.1 Ідентифікація

Ідентифікація – це процес визначення особи в системі, зазвичай на підставі наперед відомої інформації, такої як ідентифікатор або інша попередньо визначена інформація про користувача[6]. Ця процедура служить для отримання інформації про суб'єкта системи і є першою стадією для надання доступу до неї. Після успішної ідентифікації виконуються етапи автентифікації та авторизації. Механізм ідентифікації передбачає, що суб'єкт (користувач або процес, що діє від імені користувача) повідомляє своє ім'я за допомогою унікального параметра, такого як ідентифікатор (логін). Під час ідентифікації здійснюється порівняння заявленого параметра суб'єкта з відомим іншій стороні. При успішній ідентифікації відбувається автентифікація, під час якої інша сторона переконується, що суб'єкт є тим, за кого він себе видає, наприклад, за допомогою паролю чи іншого секретного параметра.

Цифровий підпис у комп'ютері представлений як послідовність бінарних цифр і обчислюється з використанням визначених правил і параметрів. Він гарантує перевірку особи, яка зробила підпис, та цілісність даних. Для генерації цифрового підпису використовується приватний ключ, а для його перевірки – відкритий ключ. У кожного користувача є пара ключів: приватний і відкритий. Цифровий підпис гарантує, що лише власник приватного ключа може створити підпис, інші ж можуть перевірити його автентичність за допомогою відкритого ключа. Інфраструктура відкритого ключа допомагає у керуванні та

розповсюдженні цих ключів. Цей процес можна розділити на три алгоритми щодо генерації і перевірки, кожен з яких описаний нижче.

1.2.2 Автентифікація

Аутентифікація являє собою процедуру визначення правомірності користувача інформації в системі, використовуючи подані ним ідентифікатори. З точки зору забезпечення інформаційної безпеки, аутентифікація входить у склад процесу надання доступу до роботи в інформаційній системі, розташованої між ідентифікацією та авторизацією[7].

Механізм автентифікації може включати передвизначену ідентифікацію на основі логіну та конфіденційного пароля. Після введення цих ідентифікаторів система порівнює їх із значенням, збереженим у захищеній БД. При успішній автентифікації відбувається авторизація, що дозволяє користувачеві працювати в системі.

Види автентифікації включають:

– слабка (однофакторна) автентифікація, де використовується лише один фактор, такий як пароль. Цей метод може стати об'єктом злому з часом, особливо при недостатньо стійкому паролі. Людський чинник також може впливати на стійкість пароля, оскільки важко запам'ятати складні паролі;

– багатофакторна автентифікація (MFA), де є використання двох чи більше факторів для автентифікації забезпечує більший рівень безпеки. Наприклад, комбінація пароля і фізичного токена або відбитка пальця може використовуватися для забезпечення додаткового рівня захисту;

– посилена автентифікація, яка вимагає використання принаймні двох різних типів факторів для автентифікації, що підвищує рівень безпеки в операціях з платежами;

– сувора автентифікація – це процес автентифікації, під час якого використовується інформація, яку користувач не розкриває. Зазвичай це досягається за допомогою асиметричних криптографічних алгоритмів, які

використовують пару ключів: приватний для підпису чи шифрування та відкритий для перевірки, чи розшифрування. Цей підхід забезпечує високий рівень безпеки, оскільки приватний ключ залишається конфіденційним, а відкритий ключ може використовуватися для перевірки та розшифрування безпеки інформації.

Існує три основні типи факторів, які забезпечують безпеку автентифікації:

– фактор знання – коди, паролі та відповіді на контрольні питання. Ці дані легше дізнатися або підібрати, оскільки вони знаходяться в пам'яті користувача. Забезпечення надійності цього виду фактора є важливим завданням через загрозу злому паролів;

– фактор предмета (володіння) – фізичні предмети, такі як ключі, RFID-карти, комп'ютери та смартфони, на яких зберігається інформація для входу. Використання фізичних об'єктів може додатково підвищити безпеку, оскільки їх можна фізично захистити або використовувати додаткові заходи безпеки;

– фактор властивості – включає біометричні дані, такі як відбитки пальців, розпізнавання обличчя чи голосу. Використання унікальних фізіологічних чи поведінкових рис може зробити автентифікацію більш суворою, оскільки ці дані унікальні для кожної особи.

1.2.3 Авторизація

Авторизація – це управління рівнями та засобами доступу до захищеного ресурсу, що може бути як у фізичному розумінні, наприклад, доступ до кімнати готелю за допомогою картки, так і в цифрових технологіях, наприклад, в автоматизованій системі контролю доступу. Це визначає, які ресурси або функції системи може використовувати користувач або програма на основі їхнього ідентифікатора і пароля, а також може передбачати надання певних повноважень для виконання конкретних дій у системі обробки даних[8].

З погляду забезпечення інформаційної безпеки, авторизація є необхідною частиною процесу надання дозволу на використання ресурсів в інформаційній

системі. Цей етап відбувається після ідентифікації та автентифікації користувача, визначаючи, які конкретні ресурси та операції в системі він має право використовувати.

1.3 Класифікація СКУД

Класифікація СКУД здійснюється з урахуванням кількох параметрів. Розглянемо основні серед них[9].

За методом управління:

– біометрична – використовує ідентифікацію індивідуальних параметрів користувача, таких як райдужки ока чи дактилоскопічні відбитки. Забезпечує високий рівень захисту, оскільки біометричні дані важко підробити. Використовується для миттєвої перевірки особистості та ведення журналу подій;

– мережева (централізована) – надає більше можливостей, зокрема, можливість налаштовувати доступ за розкладом, контролювати графік роботи співробітників та інтегруватися з іншими системами. Керується дистанційно та підключається до ПК, часто інтегрується з відеоспостереженням та пожежно-охоронною сигналізацією;

– автономна – використовується як альтернатива замкам або установлюється разом з ними. Забезпечує контроль доступу, вводячи коди карток доступу. Проста у використанні та не вимагає підключення до ПК, але не забезпечує облік робочого часу;

– універсальна – об'єднує функції автономних і мережевих систем, може переходити в автономний режим роботи за потреби.

За рівнем ідентифікації:

– однорівневі – ідентифікація відвідувачів проводиться лише за 1 ознакою, такою як зчитування коду карти;

– багаторівневі – доступ на об'єкт здійснюється за кількома ознаками, такими як код карти та біометричні дані.

Згідно з кількістю точок доступу:

– малої ємності, коли кількість точок доступу становить менш ніж 80;

– середньої ємності, якщо їх кількість знаходиться в діапазоні від 80 до 250;

– великої ємності, якщо точок доступу понад 256.

Вибір конкретного класу та типу СКУД залежить від специфічних цілей, розмірів підприємства, кількості персоналу, характеру бізнесу та інших факторів.

1.4 Складові та принципи функціонування СКУД

Принцип дії системи контролю доступу описується наступним чином [10]: особа, яка хоче отримати доступ до конкретного об'єкта чи території, використовує спеціальний пристрій для сканування пластикової картки чи ключа. Отримана інформація передається на електронний пристрій, де той порівнює її з еталонною БД. Після цього система приймає рішення щодо того, чи дозволяти особі доступ чи ні.

У цілому для створення СКУД потрібні наступні технічні компоненти:

– ідентифікатор, який може приймати форму пластикової карти, спеціального брелка, або біометричних даних;

– зчитувач, що являє собою спеціальний пристрій для сканування ідентифікатора;

– контролер, який опрацьовує інформацію, отриману від зчитувача, та приймає рішення стосовно надання доступу до приміщення чи території;

– персональний комп'ютер (ПК), програмне забезпечення, турнікети, адаптери та інше обладнання.

Основне завдання СКУД полягає в регулюванні доступу до певної території, включаючи дві ключові функції:

– обмеження доступу до визначеної території;

– ідентифікація особи, яка має право доступу на визначену територію.

Додаткові завдання СКУД охоплюють:

1) визначення та документування тривалості роботи працівника на робочому місці;

2) розразунок оплати праці, особливо при взаємодії з бухгалтерськими системами для автоматизованого розрахунку;
3) введення бази персоналу/відвідувачів;
4) інтеграція з системою безпеки, такою як:

– система відеоспостереження, яка синхронізує архіви подій, повідомляє системі про необхідність початку запису, відправляє повідомлення для повороту камери у режим запису для документування наслідків виявленої підозрілої події.

– система ОС (охоронна сигналізація) для контролю доступу до об'єктів під охороною або автоматичного зняття та постановки на охорону приміщень;

– система ПС (пожежної сигналізації), яка отримує дані про стан пожежних сповіщувачів, автоматично розблоковує евакуаційні виходи та закриває протипожежні двері під час спрацювання сигналізації про пожежу.

Процес функціонування СКУД 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. Загальна логічна схема побудови системи контролю та управління доступом подана на рисунку 1.1 [11].

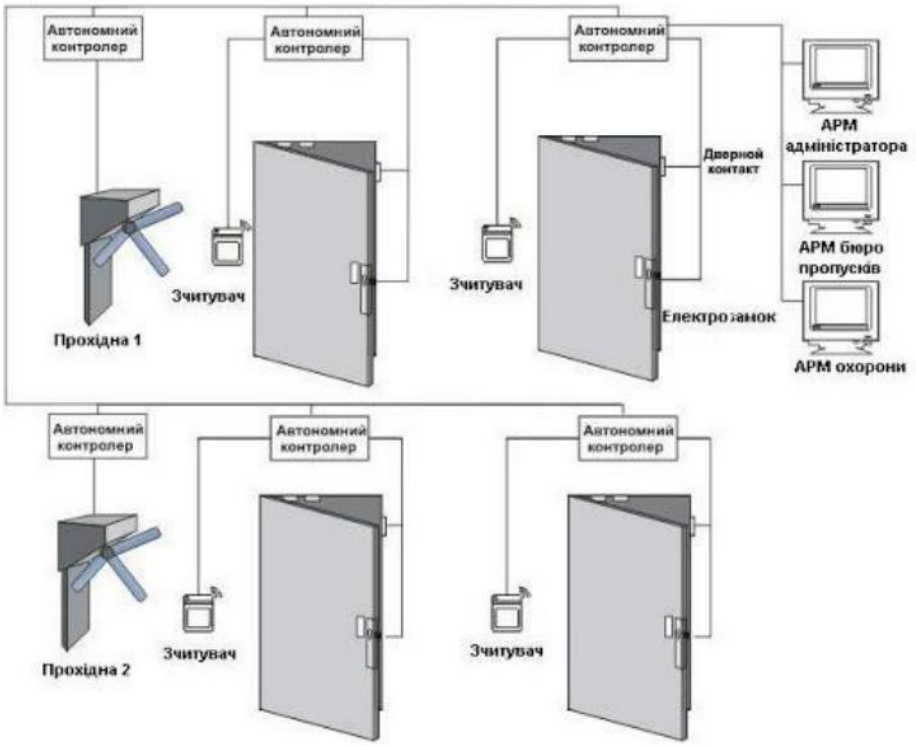

Рисунок 1.1 Загальна схема роботи СКУД

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.

1.5 Можливості СКУД

У ході своєї роботи система контролю та управління доступом (СКУД) має виконувати ряд ключових функцій (Функціональна схема Додаток Л):

– санкціонування, тобто процедура присвоєння унікального ідентифікатора, коду або реєстрації біометричних ознак кожному користувачеві та введення його даних в систему;

– завдання тимчасових інтервалів і рівня доступу, що передбачає призначення користувачам часових обмежень та визначення їх рівнів доступу, вказуючи, в які приміщення, коли і кому дозволено входити;

– ідентифікація, що являє процедуру впізнавання користувача за зазначеним ідентифікатором або біометричною ознакою;

– авторизація, що включає перевірку повноважень, яка охоплює перевірку відповідності часу та рівня доступу, встановлених під час санкціонування;

– аутентифікація, тобто визначення автентичності користувача за зазначеними ознаками ідентифікації;

– прийняття рішення на основі результатів попередніх процедур щодо надання чи відмови в доступі;

– реєстрація всіх дій в системі для подальшого аналізу та контролю;

– реагування на несанкціоновані дії, включаючи в себе висвітлення попереджень, подачу тривожних сигналів, відмову в доступі тощо.

Процедура санкціонування, яка визначає права доступу, проводиться оператором або адміністратором системи, в той час, як інші процедури можуть автоматизуватися в рамках системи. Очевидно, що повноцінна процедура аутентифікації може бути успішно виконана лише за допомогою біометричних систем.

1.6 Постановка задачі

На підставі проведеного аналізу системи контролю доступу можна прийти до висновку, що є необхідність у створенні нової системи контролю доступу та ідентифікації осіб на режимних об’єктів. Для цього можна обрати один із методів управління, який би показав високу ефективність роботи.

Перелік завдань:

1) аналіз методів біометричної ідентифікації людини;

2) аналіз архітектур НМ і їх навчання для біометричного розпізнавання;

3) технологічний аналіз програмного забезпечення та необхідних технологій;

4) проєктування біометричної СКУД

5) проєктування та розробка нейронної мережі та інтерфейсу;

6) тестування СКУД;

7) висновки.

Висновки до розділу 1

Розглянуто складові та принцип роботи систем контролю та управління доступу до різноманітних режимних об’єктів. Також оглянуто класифікацію СКУД.

На основі аналізу можливостей СКД визначено актуальність та необхідність проєктування й розробки СКУД на основі біометричної ідентифікації, яка працюватиме за рахунок особливостей кожної людини, для запобігання проникненню будь-яких небажаних людей на територію, що охороняється, й забезпечення захисту матеріальних цінностей, важливої інформації. Така система надасть більший ступінь захисту, ніж системи контролю доступу за картками, оскільки біометричні дані не можна підробити.

Визначено перелік завдань, які необхідно розробити для досягнення мети.

2 АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ ОСОБИ

2.1 Загальні відомості та види ідентифікації особи

Ідентифікація об'єкта – це процес упізнання та встановлення зв'язку із конкретним об'єктом або особою. У сфері інформаційних технологій термін "ідентифікація" вказує на визначення особистості користувача. Цей етап необхідний для того, щоб система могла приймати рішення щодо надання особі дозволу на роботу з комп'ютером, отримання доступу до конфіденційної інформації й таке інше. Таким чином, ідентифікація є ключовим поняттям в області інформаційної безпеки.

Нині існує кілька методів ідентифікації користувачів, кожен з яких має свої переваги та обмеження, що робить їх більш або менш придатними для конкретних систем. Загалом існують три основних методи ідентифікації (рис. 2.1).

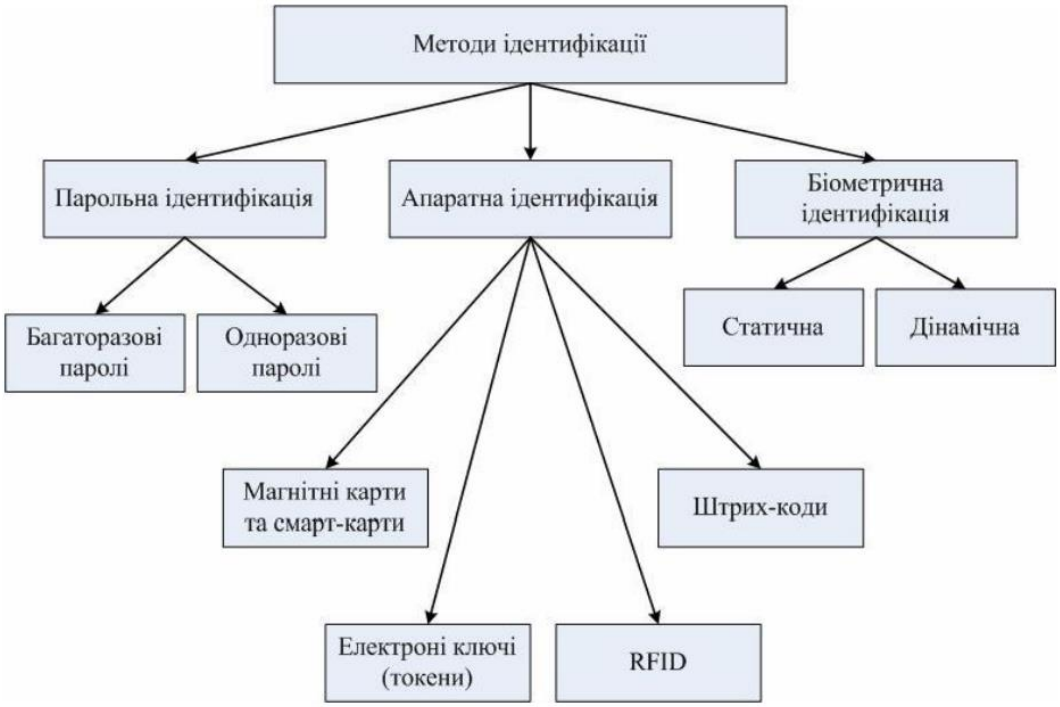

Рисунок 2.1 – Класифікація методів ідентифікації

2.1.1 Парольна ідентифікація

До недавнього часу використання паролів вважалося основним методом ідентифікації особистості користувача. Це було пов'язано з тим, що їх просто впровадити та використовувати в повсягденному житті. При реєстрації в системі кожен отримував свій набір особистих даних у формі логіна та пароля. Щоразу, коли користувач намагався увійти, мав надати ці дані, й система, аналізуючи унікальність ідентифікаторів, робить висновок про особистість користувача.

Головною перевагою парольної ідентифікації є її простота в реалізації та використанні. До того ж, такий метод не вимагає значних витрат, оскільки цей метод широко застосовується у всіх інформаційних системах та мережах. Проте такий метод має свої недоліки: по-перше, його надійність залежить від користувачів і їхньої відповідальності за створення складних паролів; по-друге, користувачі не завжди готові запам'ятовувати паролі, що може призвести до їх втрати або запису на ненадійних носіях, порушуючи рівень інформаційної безпеки.

2.1.2 Апаратна ідентифікація

У цьому сценарії ідентифікація базується на розпізнаванні особистості користувача за допомогою конкретного предмета, який перебуває в його власності. Тут розрізняють 2 види ключів: карткові (засновані на електронних картках, таких як магнітні карти чи смарткарти) та токени (пристрої з власною пам'яттю, які з'єднуються з зовнішніми портами USB).

Перший вид капрт вважають менш надійними для ідентифікації, перш за все через вразливість до копіювання інформації та чутливість до механічних пошкоджень. Однак їхня основна перевага полягає в простоті використання та реалізації.

Другий вид більш надійний, оскільки в цьому випадку можлива двофакторна ідентифікація, тобто користувач надає спочатку ключ, який виконує певні дії (наприклад, генерує відкритий та закритий ключі), і потім виконується певна дія з його боку (наприклад, введення пароля). Основною перевагою цього

методу ідентифікації є висока надійність. Проте у цьому способі ідентифікації є і суттєві недоліки, наприклад ключ можна втратити чи вкрасти, також метод потребує додаткових витрат на впровадження.

Види ідентифікаторів зображено на рисунку 2.2.

Рисунок 2.2 – Види ідентифікаторів: а – пластикова карта; б – браслет; в, г – брелоки Touch Memory

Крім того, існують ще два типи апаратної ідентифікації – штрихкодова ідентифікація та радіочастотна ідентифікація RFID[12]. Зазвичай, штрих-кодова ідентифікація використовується для ідентифікації товарів у торгівлі, але може також застосовуватися для особистої ідентифікації (особі виділяється картка зі штрих-кодом, яку вона використовує для ідентифікації). Основною перевагою цього методу є його простота в реалізації, але він має багато недоліків – інформація в штрих-коді зберігається відкрито, тому його легко підробити.

Метод радіочастотної ідентифікації ґрунтується на використанні двох пристроїв – базового блоку чи пристрою зчитування та транспондера, або RFID-мітки. Принцип ідентифікації полягає в тому, що у RFID-мітці зберігається необхідна інформація для ідентифікації особи, яка передається пристрою зчитування. Іншими словами, особа, яка хоче пройти ідентифікацію, повинна мати при собі RFID-мітку. Коли вона потрапляє у зону дії зчитувача, останній висилає запит на ідентифікацію, а мітка відповідає і передає всю необхідну інформацію за допомогою радіосигналів. Основними перевагами цього методу є його відносна простота, відсутність необхідності у прямому контакті, легкість використання та висока швидкість. Однак є і деякі суттєві недоліки – по-перше,

можливість виведення із ладу системи ідентифікації при створенні сильних перешкод у радіодіапазоні, по-друге, високі витрати на встановлення такої системи ідентифікації, і по-третє, можливість крадіжки RFID-мітки та її використання для підробки особистості.

2.1.3 Біометрична ідентифікація

Біометрія – це метод ідентифікації особи за унікальними біологічними ознаками, які є характерними лише для конкретної людини. Використання біометрії в галузі інформаційної безпеки є логічним вибором, оскільки кожна особа має свої унікальні біометричні ознаки. Біометричні системи ідентифікації є складним та ефективним засобом визначення особи на основі її біометричних характеристик.

Біометрія виникла вже в XIX столітті, переважно використовуючись у криміналістиці для ідентифікації злочинців. З тих пір біометрія розвинулася в складну та ефективну систему ідентифікації особи. У контексті біометричних систем існують основні терміни, такі як:

– біометрія – це область знань, яка використовується для створення автоматизованих систем контролю доступу на основі унікальних ознак, притаманних кожній людині;

– біометричні характеристики – це ознаки, унікальні для кожної особи;

– біометричний зразок – це шаблон обраної біометричної характеристики;

– ідентифікація – перевірка наявності запропонованого ідентифікатора серед зареєстрованих;

– аутентифікація – перевірка належності пред'явленого ідентифікатора особі;

– реєстрація – створення шаблону за будь-якою біометричною характеристикою, який призначений для конкретної особи.

Перевагами біометричної ідентифікації є неможливість втрати або забуття біометричних ідентифікаторів, а також їх важкість підробки, оскільки кожна

особа володіє унікальними біометричними ознаками. Точність біометричної ідентифікації наближається до ста відсотків, що робить цей метод найбільш надійним.

До недоліків біометричної ідентифікації можна віднести великі витрати на реалізацію такої системи. Однак, незважаючи на це, біометрична ідентифікація залишається найбільш надійним методом. Крім того, її можна використовувати як частину комплексної ідентифікації, одночасно з іншими методами, або проводити ідентифікацію за декількома біометричними характеристиками, що значно підвищує надійність цього процесу.

2.2 Огляд сучасних методів біометричної ідентифікації

У період розвитку біометричної ідентифікації використання обмежувалося трьома основними біометричними ідентифікаторами: відбитками пальців, голосом та підписом. Існувала загальна думка, що першими ідентифікаторами були саме підпис та розпізнавання за голосом, але як виявилося, в Єгипті на той час вже використовували й розпізнавання відбитків пальців. Подальший прогрес у сфері медицини призвів до виявлення додаткових унікальних біометричних ознак людини, які можна також використовувати для її ідентифікації.

Способи біометричної ідентифікації наведено на рисунку 2.3.

Рисунок 2.3 – Способи біометричної ідентифікації

Всі ці способи ідентифікації людини поділяються на 2 групи, а саме:

– фізіологічні (статичні), які базуються на фізіологічних характеристиках людини, що притаманні їй з народження і не можуть бути змінені (Додаток А);

– психологічні (динамічні), які базуються на поведінкових характеристиках людини, особливостях, що проявляються у підсвідомих рухах під час виконання будь-якої дії (Додаток Б).

Слід відзначити, що психологічні методи є менш надійними в порівнянні з фізіологічними.

Методи біометричної ідентифікації наведено в таблиці 2.1:

Таблиця 2.1 – Методи біометричної ідентифікації[13]

№	Фізіологічні методи	Психологічні методи
1	за відбитками пальців	за голосом
2	за формою долоні	за підписом
3	за сітчаткою ока	за почерком
4	за геометрією обличчя	за клавіатурним почерком
5	за розташуванням вен на лицьовій стороні долоні	
6	за термограмою обличчя (розташування артерій під шкірою обличчя)	
7	за райдужною оболонкою ока	
8	за геометрією вуха	
9	за допомогою ДНК	

Біометрична ідентифікація людини основана на унікальних ознаках, притаманні кожній людині окремо. І ймовірність співпадіння цих характеристик у двох різних людей надзвичайно низька. Наприклад, ймовірність того, що в двох різних людей відбитки пальців на однакових пальцях руки будуть ідентичними,

практично дорівнює нулю і становить 1/24 мільйона[13]. Основні характеристики більшості методів наведено в таблиці 2.2.

Таблиця 2.2 – Основні характеристики методів біометричної ідентифікації

Метод біометричної ідентифікації	Відмова СКУД у %	Помилка розпізнавання у %	Ціна методу
Геометрика лодоні	менше за 4	менше 1	800 - 3500 у.о.
Відбиток пальця	2-6	мінімальна	50 - 800 у.о.
Сітківка ока	мінімальна	до 8	3000-4500 у.о.
Райдужка ока	менше за 2	мінімальна	300-5000 у.о.
Обличчя	До 7	менше 5	1000 у.о.
Звичайний почерк	до 5	5	-
Клавіатурний почерк	Від 3 до 10	10	-
Голос	до 5	5	1-5000 у.о.

Фізіологічні та психічні методи є взаємопов'язаними та доповнюють один одного. Статичні методи відрізняються тим, що вони не залежать від психологічного стану користувача, вимагають мінімальних зусиль від нього і, таким чином, забезпечують ефективну реалізацію біометричної ідентифікації для обробки великих потоків людей.

Психічні (динамічні) методи біометричної ідентифікації, зазвичай, виявляються менш складними в провадженні, бо вони часто обходяться без дорогого обладнання. Для реалізації методу достатньо мати програмні засоби, які не вимагають складного технічного обслуговування.

2.2.1 Статичні біометричні характеристики

Основні статичні біометричні характеристики та їх реалізаця наведена в таблиці 2.3 [13].

Таблиця 2.3 – Реалізація статичних ознак

Біометричний показник	Пристрій для считування	Зразок біометричної характеристики	Що саме буде досліджуватись

Геометрична будова руки	Запатентований 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

Біометричний показник	Пристрій для считування	Зразок біометричної характеристики	Що саме буде досліджуватись
Відбиток пальців	Периферійний пристрій настільного комп’ютера, карта стандарту PC card, миша, мікросхема або зчитувальний пристрій, вбудований в клавіатуру	Зображення відбитку пальців (оптичне, на кремнієвому фотоприймачі, ультразвукове, або безконтактне)	Розташування і напрям гребінчастих виступів і розгалужень на відбитку пальців, дрібні деталі
Сітківка ока	Запатентований 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)	Відносне розташування і форма носа, розташування скул

1) Розпізнання за формою кисті руки – це процес визначення особливостей та параметрів руки людини за її геометричною структурою лодоні[13].

Підходи для розпізнання за формою кисті руки базуються на:

– геометричні параметри руки, тобто використання розмірів, форми та інших геометричних характеристик руки для ідентифікації особи чи для вирізнення різних рук. Параметри включають довжину та ширину пальців, об'єм кисті, відстані між суглобами, кутові параметри та інші геометричні особливості;

– образові характеристики, що враховує образи або відбитки, які можуть бути видимі на поверхні руки. Образи на з'єднаннях між фалангами пальців

можуть включати відбитки шкіри, які можуть бути використані для ідентифікації. Візерунки кровоносних судин також можуть служити як унікальні ознаки, особливо в інфрачервоному або іншому спектральному діапазоні.

Головні ознаки геометричної будови руки, які можна враховувати в розпізнаванні, включають:

– вимірювання довжини кожного пальця та долоні може надати характеристики, що відрізняють руку однієї особи від іншої;

– врахування ширини і об'єму кисті руки може бути корисним для унікального визначення особи;

– вимірювання кутів між сусідніми пальцями чи між пальцями та долонею може надати інформацію про форму руки;

– розмір та відстань між суглобами на пальцях може бути використано для ідентифікації;

– врахування кількості та розміщення суглобів на кожному пальці;

– визначення форми контуру долоні.

На рисунку 2.4 зображено долонь, яка включає 5 основних ліній (зліва), контрольні точки та геометричні ознаки руки (праворуч)[13].

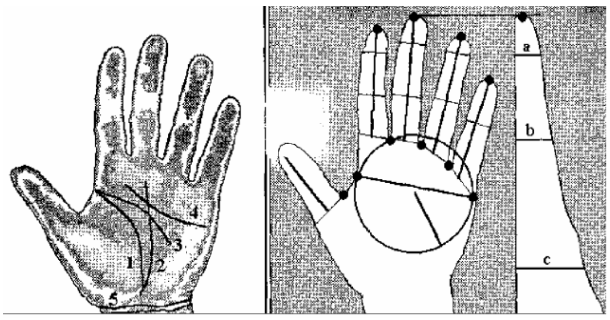

Рисунок 2.4 – Рисунок долоні

Для розпізнавання за геометричною будовою руки можуть використовуватися технології комп'ютерного зору, 3D-сканування, а також алгоритми машинного навчання.

2) Розпізнавання за відбитком пальців є одним із найпоширеніших і найефективніших методів біометричної ідентифікації. Ось основні етапи та характеристики розпізнавання за відбитком пальців:

– процес збору відбитків може бути здійснений за допомогою спеціальних сканерів пальців, які можуть бути оптичними (використовують світловий промінь), капацитивними (вимірюють електричні властивості шкіри на поверхні пальця), акустичними або ультразвуковими (обидва використовують звукові хвилі для створення образу внутрішньої структури пальця);

– обробляється для виділення унікальних характеристик, які відокремлюють один відбиток від іншого. Ці характеристики можуть включати розташування та довжину ліній, гранул, точок розгалуження, арок та інші особливості;

– на основі виділених характеристик створюється унікальний шаблон для кожного відбитку пальця. Цей шаблон може бути збережений у базі даних для подальшого порівняння;

– порівняння та ідентифікація, тобто відбиток пальця порівнюється з раніше збереженими шаблонами в базі даних. За допомогою алгоритмів порівняння визначається ступінь відповідності між новим відбитком і тими, що вже є в базі.

Зазвичай для створення унікального "папілярного шаблону", який служить основою для ідентифікації особи використовують:

– кінцеві точки (ending points) – це точки, де папілярні лінії відбитку пальця закінчуються або змінюють свій напрям. Кінцеві точки можуть бути використані для визначення крайніх точок папілярних ліній;

– точки розгалуження (bifurcation points) – це точки, де є розділення папілярних ліній на дві частини.

Алгоритми розпізнавання використовують розташування та характеристики цих точок (рис. 2.5) для створення унікального числового представлення відбитку пальця, яке може бути порівняно з іншими зареєстрованими відбитками пальців у базі даних для ідентифікації особи.

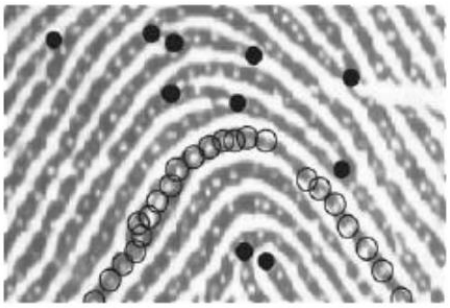

Рисунок 2.5 – Відбитки пальців

На рисунку 2.5 відмічено чорним колом кінцеві точки і точки розгалуження, а порожнім – пори[13]. В цьому методі досить таки складно отримати якісне зображення відбитку. Тому зараз все частіше використовують електронні безфарбові сканери пальців. Такі сканери дозволяють отримувати зображення папілярного візерунку з високою якістю, яке може бути використане для автоматизованого розпізнавання відбитків пальців. Крім того, за допомогою електронних сканерів можна враховувати інші параметри, такі як тривимірна геометрія пальця, що робить систему розпізнавання більш точною і менш вразливою до зовнішніх факторів, таких як кутові зміщення чи тиск.

3) Розпізнавання за сітківкою ока є одним із біометричних методів ідентифікації, який використовує унікальні характеристики сітківки для визначення особи. Сітківка (ретина) знаходиться на задній частині ока і відповідає за прийом світла та передачу зображення до мозку через зірковий нерв.

Зазвичай для отримання біометричних даних використовують сканери, які включають інфрачервоне або світлодіодне випромінювання, для отримання високороздільних зображень сітківки. Отримане зображення сітківки аналізується для виділення унікальних характеристик, таких як відстані між судинами, розташування основних пунктів, розгалуження судин і т.д. На основі витягнутих характеристик створюється біометричний шаблон, який може бути використаний для подальшого порівняння.

4) Розпізнавання за обличчям – це біометричний метод ідентифікації, який використовує унікальні характеристики обличчя. Збір даних включає в себе використання відеокамер, фотографій для зафіксування обличчя особи, також веб-камер в мобільних пристроях чи інших оптичних пристроїв. Зображення може

бути піддане попередній обробці, такій як вирівнювання, щоб забезпечити однаковий кут огляду для всіх обличчів. Далі використовуються алгоритми для виділення унікальних особливостей, таких як розташування очей, носа, рота, форма обличчя тощо. Важливо враховувати, що точність розпізнавання за обличчям залежить від якості вхідних зображень та вибраного методу обробки.

2.2.2 Динамічні біометричні характеристики

Основні динамічні характеристики та їх реалізації наведена в таблиці 2.4[13].

Таблиця 2.4 – Реалізація психологічних біометричних характеристик

Біометричний показник	Пристрій для считування	Зразок біометричної характеристики	Що саме буде досліджуватись
голос	мікрофон	мовний файл	тембр, мплітуда, гучність
почерк	екран для написання	зображення напису/підпису	зображення ліній, натиск, коливань пера
клавіатурний почерк	клавіатура	динаміка натискання клавіш	затримка клавіш та швидкість натиску наступної

1) Ідентифікація особи за голосом є одним із методів біометричної ідентифікації, який базується на унікальних характеристиках голосу кожної людини. Кожна особа має унікальні звукові особливості, такі як тембр, інтонація, ритм та інші аспекти, які можуть служити як біометричні ознаки для її ідентифікації. Процес ідентифікації за голосом зазвичай включає в себе реєстрацію або створення голосового зразка особи, який потім може бути збережений у системі. Під час ідентифікації система порівнює вхідний голосовий сигнал з зареєстрованим зразком, визначаючи відповідність та підтверджуючи особу. Цей метод може бути використаний у різноманітних сценаріях, таких як системи голосового визнавання для автентифікації користувачів у банківських системах, контролю доступу або інших областях, де важлива точна ідентифікація особи. Ймовірність помилки розпізнавання становить від 1% до 2%.

Важливі аспекти процесу ідентифікації особи за голосом:

– мовний шаблон – це унікальне представлення голосу конкретної особи, яке служить основою для подальшого порівняння. Мовний шаблон може включати різноманітні характеристики голосу, такі як інтонація, розмір мовленнєвого апарату, ритм та інші параметри;

– голосовий ключ – це цифровий відбиток голосу, який вводиться в систему для ідентифікації. Він може бути отриманий шляхом аналізу і обробки аудіозапису;

– характеристики мовного сигналу, такі як:

1. амплітуда і потужність (гучність), що вимірюють інтенсивність звуку, що може варіюватися залежно від відстані до мікрофону та інших факторів;
2. часові характеристики, що включають в себе ритм та швидкість мовлення, паузи, інтонацію та інші аспекти, що залежать від часу;
3. частотні характеристики (тембр), що визначають зміни в частоті голосу, що можуть бути характерними для конкретної особи;
4. енергетичні характеристики, що відображають енергію, витрачену на висловлення певного звуку або слів;
5. фазові характеристики, що враховують зміни у фазі звуку, що можуть впливати на сприйняття голосу.

Для полегшення аналізу мовного сигналу в системах розпізнавання за голосом можна використовувати деякі техніки та підходи. Ось кілька способів:

– перетворення аналогового сигналу в цифровий шляхом дискретизації зменшує обсяг даних і полегшує їх обробку;

– використання вейвлет-перетворення дозволяє отримати представлення сигналу в декількох масштабах та частотах, полегшуючи виділення ключових особливостей;

– виділення значущих характеристик, таких як частотні зони, інтонація та інші аспекти мови, може спростити подальший аналіз;

– застосування алгоритмів машинного навчання, таких як нейронні мережі, для автоматизованого вивчення та розпізнавання особливостей голосу;

– застосування методів фільтрації та зменшення шумів для полегшення виділення сигналу від фонового шуму;

– врахування контексту інформації, наприклад, історії користувача чи конкретного середовища, може покращити точність розпізнавання.

2) Ідентифікація за рукописним підписом базується на унікальних особливостях та рисах, які притаманні рукопису конкретної особи. Цей процес зазвичай включає в себе наступні етапи:

– отримання зразка рукопису від користувача. Це може бути здійснено через написання певного тексту або підпису на папері чи електронному пристрої;

– отримання цифрового відображення рукопису, яке може бути використане для подальшого аналізу. Цей етап може включати в себе використання технологій, які перетворюють аналоговий рукопис у цифрову форму;

– виділення ключових особливостей рукопису, таких як форма літер, розмір, напрямок та інші унікальні риси, які можуть слугувати для ідентифікації;

– створення унікального шаблону, що представляє собою характеристики рукопису конкретної особи;

– збереження шаблону в системі та подальше порівняння зразка рукопису, надісланого для ідентифікації. Визначення ступеня відповідності шаблону та ідентифікація особи.

Параметрами, які служать для створення унікального "цифрового відбитка" рукопису кожної людини є:

– графологічні особливості, тобто аналіз різних аспектів написання, такі як розмір та форма літер, нахил, пропорції, ширина ліній, тиск на папір, швидкість написання тощо. Такі особливості є унікальними для кожної людини;

– аналіз динаміки письма, тобто швидкість, ритм, тиск письма, зміни у написанні під час написання слова або фрази;

– просторові особливості написання, такі як розташування літер на папері, відстань між ними, кут нахилу;

– біометричні параметри, тобто використовуються технології, які перетворюють графічне зображення написання в біометричний шаблон для подальшого порівняння.

Точність ідентифікації за рукописним підписом залежить від ряду факторів, включаючи якість системи, використовувані алгоритми та умови використання. Наприклад, якщо вихідний зразок невірно зіскановано або відображено, це може призвести до низької точності ідентифікації. Чинники, такі як освітлення та якість обладнання, також можуть впливати на точність системи.

2.3 Переваги й недоліки методів біометричної автентифікації

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[17].

Біометричні системи аутентифікації здійснюють два типи помилок[17]:

– 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.

Таблиця 2.5 – Переваги та недоліки біометричної системи

№	Переваги	Недоліки
1	Надають високий рівень ідентифікації, оскільки базуються на унікальних фізичних або динамічних характеристиках	Характеристики можуть змінюватися внаслідок травм чи старіння, що може вплинути на ефективність системи.

	особи	
2	Високий рівень безпеки, бо біометричні ознаки неповторні, що зводить до мінімуму кількість помилок при впізнанні	Системи можуть допускати помилки в розпізнаванні через певні фактори.
3	Біометричні характеристики не можуть бути втрачені чи забуті	Для створення зразків біометрії потрібні спеціальні зчитувальні пристрої. А зберігання може породжувати проблеми щодо приватності та безпеки

Продовження таблиці 2.5

№	Переваги	Недоліки
4	Процес аутентифікації за допомогою біометрії є швидким та зручним для користувача,	Можуть бути обмануті за допомогою технік, таких як використання фотографій чи інших видів маскування
5	Пристрої аутентифікації зручні та бюджетні	Немає певних стандартів, а це ускладнює обмін біометричними даними між різними системами

Таблиця 2.6 – Переваги та недоліки розпізнавання за відбитком пальців

№	Переваги	Недоліки
1	Розпізнавання за відбитком пальців вважається одним із найбільш надійних біометричних методів ідентифікації завдяки унікальній природній структурі папіллярних ліній кожної людини	Зберігання і обробка відбитків пальців може порушити приватність особи, оскільки ці дані можуть потрапити в недоброзичливі руки або бути використані без дозволу
2	Процес збору і порівняння відбитків пальців зазвичай дуже швидкий, що дозволяє швидко визначити особу	В деяких випадках, наприклад, при травмуванні пальців або хворобах шкіри, система розпізнавання за відбитком пальця може бути менш надійною
3	Важко підробити відбиток пальця, що робить цей метод малоймовірним для обману	Використання розпізнавання за відбитком пальця може вимагати спеціального обладнання, що збільшує витрати

4	Людям зручно використовувати власні відбитки пальців для ідентифікації, наприклад, на смартфонах або для входу до приміщень	В ряді справ розпізнавання за відбитком пальця може бути предметом спору через можливість помилок або недоліків у процесі збору даних
5	Розпізнавання за відбитком пальців може бути впроваджене на різних рівнях, від особистого використання до корпоративних і державних систем безпеки	

Переваги та недоліки розпізнавання за обличчям наведено в таблиці 2.7:

Таблиця 2.7 – Переваги та недоліки розпізнавання за обличчям

№	Переваги	Недоліки
1	Для проведення розпізнавання за обличчям не потрібний фізичний контакт з об'єктом ідентифікації. Це зручно та гігієнічно, особливо в контексті систем безпеки та входу на об'єкти	Різноманітні чинники навколишнього середовища можуть впливати на ефективність пристрою, такі як рівень освітлення, положення камери та інші фактори.
2	Для считування можуть бути використані існуючі інструменти, й також існуюче обладнення для обробки зображення	Розпізнавання за обличчям може стати менш надійним в ситуаціях, коли особа змінила свій зовнішній вигляд через зачіску, окуляри, макіяж, або під впливом інших факторів, таких як освітлення
3	Риси обличчя є унікальними для кожної людини, і важко їх підробити, що робить цей метод малоймовірним для обману	Системи розпізнавання за обличчям можуть бути обмануті за допомогою зображень або фотографій, які подаються замість живого обличчя
4	Розпізнавання за обличчям може бути використане в ситуаціях, коли ідентифікована особа перебуває на віддаленій відстані від системи, наприклад, під час онлайн– авторизації	Розпізнавання за обличчям вимагає наявності спеціалізованого обладнання та програмного забезпечення, що може збільшувати витрати

Переваги та недоліки розпізнавання за райдужною оболонкою ока наведено в таблиці 2.8:

Таблиця 2.8 – Переваги та недоліки розпізнавання за райдужною оболонкою ока

№	Переваги	Недоліки
1	Кожна особа має унікальний візерунок райдужної оболонки ока, що робить цей метод дуже надійним для ідентифікації	Розробка та впровадження систем ідентифікації за райдужною оболонкою може бути дорогим процесом
2	Матеріал не змінюється з віком	Деякі обставини, такі як освітлення, стан здоров'я ока або носіння контактних лінз, можуть впливати на ефективність ідентифікації за райдужною оболонкою

Продовження таблиці 2.8

№	Переваги	Недоліки
3	Системи мають високу точність розпізнавання	
4	Для проведення ідентифікації за райдужною оболонкою ока не потрібно фізичного контакту, що робить його гігієнічним і неінвазивним	
5	Ідентифікація може проводитися на віддаленій відстані, що дозволяє використовувати цей метод для віддалених аутентифікаційних процесів	
6	Процес збору і порівняння даних райдужної оболонки ока може бути досить швидким	
7	Якщо дані райдужної оболонки правильно збережені та оброблені, то цей метод є дуже відмовостійким	

Переваги та недоліки розпізнавання за голосом наведено в таблиці 2.9:

Таблиця 2.9 – Переваги та недоліки розпізнавання за голосом

№	Переваги	Недоліки
1	Голос кожної особи унікальний, і характеристики голосу включають в себе такі параметри, як тембр, інтонація, швидкість мовлення і акцент, що робить голосову ідентифікацію досить надійною	Характеристики голосу можуть змінюватися внаслідок застуди, горлачки, зміни настрою або фізичного стану особи, що може впливати на точність ідентифікації
2	Для голосової ідентифікації не потрібно фізичного контакту з об'єктом ідентифікації. Вона може бути проведена без участі особи і може бути здійснена на віддаленій відстані	Голосова ідентифікація може бути обманута за допомогою записів голосу особи чи синтезованих голосових команд

3	Інтуїтивно зрозумілий людині спосіб взаємодії з системою	Точність ідентифікації може залежати від якості мікрофону, який використовується для збору голосових даних
4	Немає необхідності запам'ятовувати паролі чи носити з собою біометричні картки або пристрої	Вплив психологічного стану особи на результати ідентифікації та аутентифікації
5	Голосова ідентифікація може бути використана в різних галузях, включаючи банківську справу, телекомунікації, доступ до інформаційних систем, системи безпеки та інші	

2.4 Методи розпізнавання облич та відбитків пальців

Розпізнавання обличчя – це процес визначення або підтвердження ідентичності особи на основі її фізичних рис, які можна виявити на зображенні обличчя. Схема загального принципу розпізнавання обличчя наведено у Додатку В, що включає в себе такі етапи:

1) захоплення зображень обличчя з джерел, таких як камери відеоспостереження, веб-камери, смартфони тощо. Тобто це перевіряється наявність на зображенні обличчя й після виявлення передача на попередню обробку;
2) попередня обробка зображення для видалення шуму та стандартизації розмірів, колірної палітри і освітлення;
3) визначення важливих точок на обличчі, таких як очі, ніс, рот, для подальшого аналізу;
4) виділення унікальних особливостей обличчя, які можуть використовуватися для ідентифікації, таких як форма обличчя, розташування ключових точок тощо;
5) використання отриманих особливостей для створення унікального шаблону обличчя, який може бути використаний для подальшого порівняння;
6) зберігання шаблонів обличчя в базі даних та порівняння нового зображення обличчя з наявними шаблонами для ідентифікації особи;

7) прийняття рішення про те, чи зображення обличчя відповідає існуючому шаблону, і в призначення ідентифікатора або відхилення запиту;
8) можливість системи розпізнавання обличчя оновлювати шаблони з часом для покращення точності ідентифікації;
9) розробка механізмів для захисту особистих даних та запобігання можливості використання технології розпізнавання обличчя для незаконних цілей;
10) використання розпізнавання обличчя у різних галузях, таких як безпека, автоматизована ідентифікація, контроль доступу, реклама тощо.

Існує кілька методів і підходів до розпізнавання обличчя, які можуть варіюватися за складністю, точністю і швидкістю. Найпоширенішими з них є:

– метод знаходження ключових точок (Feature-based methods): Цей метод визначає та використовує ключові точки, такі як очі, ніс і рот, для визначення форми обличчя і його особливостей. Метод може використовувати деякі алгоритми для локалізації цих точок;

– метод використання геометричних особливостей (Geometry-based methods): Він базується на геометричних властивостях обличчя, таких як відстані між очима або пропорції обличчя. Цей метод може використовувати геометричні шаблони для порівняння;

– методи засновані на текстурних ознаках (Texture-based methods): Ці методи аналізують текстурні особливості обличчя, такі як розподіл текстур, і використовують їх для розпізнавання. Можуть використовуватися методи аналізу текстури або штучні нейронні мережі;

– методи засновані на виокремленні признаків (Feature-based methods): Використовують аналіз обличчя для виділення конкретних особливостей, таких як контури, лінії і кольорові характеристики. Далі ці признаки використовуються для розпізнавання;

– методи глибокого навчання (Deep Learning methods): Використовують глибокі нейронні мережі, такі як згорткові нейронні мережі (CNN) або рекурентні нейронні мережі (RNN), для вивчення представлення обличчя. Глибокі навчальні моделі можуть автоматично визначати признаки та шаблони;

– методи засновані на моделях 3D-обличчя (3D Face Modeling methods): Використовують інформацію про 3D-структуру обличчя для розпізнавання. Це може включати в себе використання триизмерних моделей обличчя;

– методи засновані на знаходженні контурів (Contour-based methods): Визначають контури обличчя та використовують їх для розпізнавання. Метод може використовувати алгоритми знаходження контурів, такі як алгоритм Кенні;

– методи засновані на гібридних підходах (Hybrid methods): Використовують комбінацію різних методів для покращення точності ідентифікації.

Зазвичай, сучасні системи розпізнавання обличчя використовують комбінації цих методів, особливо з використанням глибокого навчання для ефективності та точності.

Переваги й недоліки кожного з методів наведено в таблиці 2.10.

Таблиця 2.10 – Переваги та недоліки методів і підходів до розпізнавання обличчя

Метод	Переваги	Недоліки
Метод знаходження ключових точок	Ефективний для визначення унікальних рис обличчя, таких як очі, ніс, та рот. Можливість використання в реальному часі.	Вразливість до змін в освітленні та позахисність до обману за допомогою фотографій.
Метод використання геометричних особливостей	Здатність враховувати геометричні параметри обличчя, такі як відстані між точками. Можливість використання для визначення положення та орієнтації обличчя.	Вимагає точної геометричної моделі, що може бути складною. Вразливість до змін у формі обличчя.
Методи засновані на текстурних ознаках	Здатність враховувати текстурні особливості обличчя, що може бути корисно при роботі з фотографіями в різних умовах освітлення.	Чутливість до змін текстури (наприклад, внаслідок старіння чи макіяжу). Відсутність реалізації в реальному часі у великому масштабі.

Методи засновані на виокремленні признаків	Ефективність у виокремленні унікальних рис обличчя. Можливість використання для різних завдань, включаючи розпізнавання емоцій.	Вразливість до змін в зовнішності та умовах освітлення.
Методи глибокого навчання	Здатність автоматично вивчати сложкі залежності та покращувати продуктивність з великою кількістю даних. Добрі результати у розпізнаванні обличчя в різних умовах.	Висока вартість навчання та потреба в великих обсягах даних. Можливість "вивчення" стереотипів та алгоритмічного біасу.
Методи засновані на моделях 3D-обличчя	Здатність враховувати тривимірні аспекти обличчя, що корисно при розпізнаванні обличчя в різних позах та умовах.	Вимагає спеціального обладнання для створення 3D-моделей. Складніше в реалізації.

Продовження таблиці 2.10

Метод	Переваги	Недоліки
Методи засновані на знаходженні контурів	Ефективність у визначенні границь обличчя та відокремленні його від фону.	Вразливість до змін у формі обличчя та фону. Може не ефективно працювати з частково прихованими обличчями.
Методи засновані на гібридних підходах	Можливість поєднати переваги різних методів для отримання кращої ефективності та стійкості.	Складніше в реалізації та вимагає додаткових зусиль для оптимізації та налаштування.

Розпізнавання відбитку пальця – це процес ідентифікації або верифікації особи на основі унікальних фізичних характеристиках пальцевого відбитку, таких як відстані між лініями, дугами, кількість і форма вихідних точок і інші. Схема загального принципу розпізнавання за відбитком пальця наведено у Додатку В, що включає в себе такі етапи:

1) захоплення образу папілярних ліній та особливостей відбитка пальця за допомогою пристроїв, таких як сканери відбитків пальців;

2) обробка отриманого зображення для видалення шуму, стандартизації розмірів і усунення артефактів;
3) визначення основних характеристик відбитка пальця, таких як розмір та форма основних ліній, розташування дуг, кількість та розташування вихідних точок;
4) створення унікального математичного представлення відбитка пальця, яке може бути використане для порівняння;
5) збереження шаблонів в базі даних та порівняння нового відбитка пальця з наявними шаблонами для визначення ідентифікації;
6) визначення того, чи відбиток пальця відповідає існуючому шаблону, і в призначенні ідентифікатора або відхиленні запиту;
7) можливість системи розпізнавання відбитка пальця оновлювати шаблони з часом для покращення точності ідентифікації;
8) використання технологій для уникнення атак із використанням фальшивих відбитків пальців, таких як відбитки, надруковані на папері чи інших матеріалах;
9) розробка механізмів для захисту особистих даних та запобігання можливості використання технології розпізнавання відбитку пальця для незаконних цілей;
10) використання розпізнавання відбитку пальця у різних галузях, таких як безпека, контроль доступу, мобільні пристрої, банківські послуги тощо.

Розпізнавання відбитку пальця базується на різноманітних методах та підходах, що включають в себе як традиційні методи обробки зображень, так і сучасні техніки машинного навчання. Найпоширеніші методи та підходи до розпізнавання відбитків пальця включають:

– метод знаходження особливостей (Minutiae-based methods): Одним з найпоширеніших підходів є використання особливостей відбитку пальця, таких як кількість, розташування та тип папілярних ліній, кількість і розташування вихідних точок (мінютій). Метод включає в себе визначення цих характеристик та їх використання для створення унікального шаблону;

– метод знаходження глобальних особливостей (Ridge-based methods): Використовує аналіз глобальних властивостей відбитку пальця, таких як форма, густота і орієнтація папілярних ліній;

– метод глибокого навчання (Deep Learning methods): Застосування глибоких нейронних мереж для автоматичного визначення та екстракції характеристик відбитку пальця. Глибокі нейронні мережі, такі як згорткові нейронні мережі (CNN) або рекурентні нейронні мережі (RNN), дозволяють вивчати високорівневі представлення зображень відбитків пальців;

– методи кореляції (Correlation-based methods): Використовують кореляційні алгоритми для порівняння двох відбитків пальців. Вони вимірюють ступінь подібності між паттернами;

– методи, засновані на структурних ознаках (Structural Feature-based methods): Оцінюють структурні ознаки відбитку пальця, такі як арки, петлі і відгалуження, для визначення унікальності відбитка;

– методи на основі геометричних параметрів (Geometric-based methods): Використовують геометричні параметри, такі як довжина, ширина та форма папілярних ліній, для розпізнавання відбитку;

– методи на основі термальних зображень (Thermal-based methods): Використовують термальні зображення пальця для отримання унікальних особливостей, що можуть бути стійкими до змін в об'єктивних умовах;

– методи на основі 3D-відбитків (3D Fingerprint methods): Використовують триизмерні моделі папілярних ліній для отримання більш точного представлення відбитка пальця;

– методи антифальшивого розпізнавання (Anti-Spoofing methods): Включають в себе заходи безпеки для уникнення атак із використанням фальшивих відбитків, таких як застосування термальних або спектральних характеристик для розпізнавання живого тканини.

Ці методи можуть використовуватися як самостійно, так і в поєднанні для досягнення більшої точності та ефективності розпізнавання відбитків пальців в різних умовах. Переваги й недоліки кожного з методів наведено в таблиці 2.11.

Таблиця 2.11 – Переваги та недоліки методів і підходів до розпізнавання відбитків пальця.

Метод	Переваги	Недоліки
Метод знаходження особливостей	Мінютії (мікроскопічні особливості) відбитка пальця є унікальними, що забезпечує високу точність розпізнавання. Простота алгоритмів виявлення мінютій дозволяє їх використання у великих системах.	Метод чутливий до якості та орієнтації відбитка пальця. Для найкращих результатів потрібно використовувати високоякісні сканери.
Метод знаходження глобальних особливостей	Робота на основі основних структур жолобків може бути швидше у порівнянні з методами на основі мінютій. Може бути менше чутливим до шуму та менших артефактів на зображенні.	Може втрачати деякі деталі, що призводить до меншої точності порівняння в порівнянні з методами на основі мінютій. Глобальні особливості можуть бути менше унікальними, що може призводити до вищого рівня помилок.

Продовження таблиці 2.11

Метод	Переваги	Недоліки
Метод глибокого навчання	Глибоке навчання дозволяє системі автоматично вивчати корисні характеристики зображення без вручну створених правил. Здатність глибоких мереж до ефективного вивчення складних залежностей призводить до високої точності розпізнавання. Можливість розпізнавання в реальному часі.	Глибоке навчання вимагає великої кількості даних для ефективного навчання. Розробка та впровадження глибоких мереж може бути складним завданням.
Методи кореляції	Використання кореляційних методів може забезпечити високу швидкість в порівнянні з іншими методами.	Метод може бути чутливим до змін розміру та позиції пальця. Зображення з високим рівнем шуму може призвести до помилок у розпізнаванні.

Методи, засновані на структурних ознаках	Використання структурних особливостей може забезпечити вищий рівень унікальності.	Може бути менше ефективним у великих системах або завданнях в реальному часі.
Методи на основі геометричних параметрів	Геометричні методи можуть бути менше чутливими до змін у формі та розмірі пальця.	Для найкращих результатів потрібно використовувати якісні відбитки пальців.
Методи на основі термальних зображень	Термальні зображення не залежать від освітлення, що робить метод стійким до змін у сенсорних умовах.	Системи, які використовують термальні зображення, можуть бути вартісними у встановленні та обслуговуванні.
Методи на основі 3D-відбитків	3D-відбитки можуть бути менше вразливими до підробки за допомогою фотографій або інших засобів.	Системи, які використовують 3D-відбитки, можуть бути вартісними та складними в обслуговуванні.
Методи антифальшивого розпізнавання	Антифальшиві методи зменшують ризик використання підроблених відбитків або живих зразків.	Антифальшиві методи можуть викликати помилкові відмови в розпізнаванні живих пальців через різні умови.

Висновок до розділу 2

Розглянуто сучасні методи біометричної ідентифікації людини та їх класифікацію. На основі переваг/недоліків кожного методу обрано фізіологічні методи біометричної ідентифікації осіб.

На основі аналізу всіх фізіологічних (статичних) методів ідентифікації осіб обрано розпізнавання за обличчям та розпізнавання за відбитком пальця. Дані методи є швидкими та зручними способами, особливо в контексті системи безпеки та входу на різноманітні об'єкти. Ці 2 метода важко підробити, що робить їх малоймовірними для обману.

Переглянуто основні методи та підходи розпізнавання. Проаналізувавши переваги й недоліки кожного, для розробки системи обрано метод глибокого навчання за допомогою НМ.

3 РОЗРОБКА СИСТЕМИ

3.1 Модель предметної області та опис системи

Система контролю та управління доступу з розпізнаванням обличчя та відбитків пальців включає ряд компонентів для ефективної ідентифікації та контролю осіб. Основні складові такої системи можуть включати:

1) біометричні сенсори:

– сенсори відбитків пальців, які використовуються для сканування унікальних особливостей папілярних ліній пальців;

– камери для розпізнавання обличчя, які використовуються для захоплення зображень обличчя та подальшого аналізу.

2) біометричне програмне забезпечення:

– обчислювальні алгоритми для аналізу та порівняння відбитків пальців;

– алгоритми розпізнавання обличчя для визначення унікальних характеристик обличчя та порівняння їх зі збереженими шаблонами.

3) контролери доступу:

– контролери дверей та бар'єрів, електронні пристрої для управління фізичним доступом;

– електронні замки, що забезпечують безпечний доступ на основі біометричної ідентифікації.

4) серверне програмне забезпечення:

– база даних біометричних шаблонів, де зберігаються унікальні біометричні дані користувачів, що мають доступ до об’єкта;

– система управління користувачами для додавання, видалення та редагування даних користувачів.

5) мережеві пристрої для зв'язку між біометричними сенсорами, контролерами та серверами.

6) живлення:

– забезпечення основного електроживлення для нормальної роботи пристроїв.

– забезпечення неперервної роботи в разі відключення основного живлення шляхом підключення резервного.

Загальна схема роботи СКУД зображена в Додатку Н.

Поєднання всіх компонентів системи контролю доступу та управління пропусками (СКУД) з розпізнаванням обличчя та відбитків пальців вимагає налаштування та інтеграції. Нижче наведено опис кроків для поєднання компонентів СКУД:

– вибір виробників біометричних сенсорів, контролерів доступу та іншого обладнання;

– встановлення сенсорів відбитків пальців та камери для розпізнавання обличчя на точках доступу (біля дверей);

– підключення біометричних сенсорів до контролера доступу;

– встановлення та налаштування програмного забезпечення, яке управляє базою даних біометричних шаблонів та іншими аспектами системи;

– підключення основного та резервного живлення;

– додатково можна розробити інтеграція з іншими системами безпеки, такими як системи відеоспостереження, щоб отримати повний обсяг заходів безпеки;

– налаштування права доступу та додавання користувачів до системи, вказавши їхні біометричні дані та іншу необхідну інформацію;

– тестування системи для перевірки правильності роботи розпізнавання та оптимізація налаштування для досягнення оптимальної продуктивності та точності;

– навчання персоналу, який буде використовувати або керувати системою, правильною експлуатацією та реагуванню на виниклі ситуації;

– періодично треба проводити обслуговування, оновлення та аудит системи для забезпечення її надійності та безпеки з часом.

Управління СКУД відбувається з сервера системи, що контролюється адміністратором. Операційна система для сервера є Windows. Перш за все, необхідно розробити простий і зрозумілий інтерфейс на дану ОС для адміністратора, в якому можна буде додавати та видаляти користувачів, а також керувати правом доступу до об’єкта. Адміністратор СКУД за допомогою настільного пристрою, який підключається до робочого ПК через USB порт, сканує відбитки працівників (людей, які мають доступ до об’єкту) тим самим створює (оновлює) еталонну базу даних. Після чого дані з сервера надходять в пам’ять контролера, які підключені за допомогою перетворювача інтерфейсів.

В системі для набору БД відбитків використаємо настільний USB сканер відбитків пальців SLK20R (рис. 3.1), характеристики якого зображено на рисунку 3.2[22].

Рисунок 3.1 – Настільний USB сканер

Модель	SLK20R
Тип сенсора	Оптичний
CPU	280 MHz DSP
Флеш пам’ять	32 MB
SoC	RTOS
Якість зображення	2 млн пікселей CMOS
Шифрування данних	Так
Робота при яскравому освітленні	Так
Захист від бризок води	Так
Робота з проблемними пальцях	Так, сухі, мокрі, грубі
Струм	5V:200mA сканування; 5V:60mA idle (очікування відбитка)
Захист від підроблених відбитків	Так
LED подсвітка	Біла
Сертифікати	FCC, CE, RoHS, PIV
Живлення	5V (USB)

Струм	200mA
Інтерфейс	USB 2.0 / USB1.1
Роз’єм інтерфейса	USB Type A
Роздільна здатність зображення	500-1000 dpi
Область сканування	15.24 * 20.32 мм (FAP20)
Зона вікна сканування	16.5*23 мм
Розмір зображення	300*400 pixel (FAP20)
Розмір	49 * 44 * 20мм (L*W*H)
Формат зображення	RAW,BMP,JPG
Шаблони	ZKFinger V10.0 ; ISO19794-2 ; ANSI-378
Розмір шаблону	1- 4KB (ZKFinger V10.0);1568 B (ISO 19794-2)
Рівнів сірого	256
Вага	0.12кг
Температура експлуатації	-20 °C ~ +50 °C; 90% r.h.

Рисунок 3.2 – Характеристики настільного USB сканера

Для підключення його до ПК необхідно завантажити відповідне SDK або програмне забезпечення на офіційний вебсайт виробника. Перед підключенням сканера до ПК необхідно встановити драйвери, які надає виробник. Зазвичай, драйвери можна знайти в комплекті з SDK або на веб-сайті виробника. Підключити сканер до доступного USB-порту на ПК. Відкрити програмне забезпечення, яке було завантажено й, ознайомившись з інструкцією користування, використати його для реєстрації відбитків пальців користувачів, які мають доступ.

Контролер доступу підключається до сервера шляхом використання RS-485, який є стандартом для передачі даних за допомогою збалансованого двожильного кабелю. Використовуємо його для здійснення зв'язку між пристроями на відстані, і це дозволяє використовувати високі швидкості передачі даних. Швидкість обміну даними максимум 115200 біт/сек. Живлення від USB-порту комп'ютера, що робить його зручним у використанні та відсутнім в потребі у додатковому джерелі електроживлення. Також наявні індикації режиму прийому/передачі є корисною функцією, яка дозволяє вам визначити, в якому режимі працює ваш пристрій — чи він зараз передає або приймає дані. підключення до комп'ютера. Підключення версія шини даних USB 2.0.

На схемі у Додатку Н на вході до об’єкта із зовнішньої сторони встановлюється сенсор сканування біометричних даних. Коли людина підходить до дверей, то відбувається сканування відбитка на сенсорі та сканування обличчя. З внутрішньої сторони дверей встановлюється звичайна кнопка виходу, яка дозволяє без сканувань покинути територію контрольованого об'єкта. Ці точки контролю доступу (ТКД) є ключовими елементами СКУД і відповідають за фізичний контроль доступу осіб до приміщень чи будівель.

В залежності від будови приміщення об’єкта можна буде встановити 2 вида ТКД, а саме двері з одностороннім контролем входу або турнікети в приміщенні будівлі. Перший означає, що точка доступу регулює лише один напрямок руху. Особи, які мають дозвіл, можуть вільно пройти через цю точку контролю, в той час, як ті, хто не має дозволу, будуть обмежені в доступі. Другий варіант

використовуються для організації проходу через прохідні зони об’єкта, де потрібно контролювати доступ. Турнікети можуть мати різні варіанти виконання, такі як поворотні, триплавкові або карусельні.

Прохід цих точок відбувається наступним чином:

– якщо це вхід до об’єкта, то біля ТКД користувач сканує власні біометричні дані (обличчя або відбиток пальця). Вбудовані сенсори або камери біля дверей або турнікету активуються, щоб виявити присутність особи. Зібрані біометричні дані порівнюються зі зразком, який раніше був збережений під час реєстрації користувача адміністратором системи. Система контролю доступу приймає рішення щодо того, чи надати доступ особі на основі порівняння біометричних даних. Якщо особа успішно перейшла всі етапи і її ідентифікація була підтверджена, точка контролю доступу відчиняється, дозволяючи особі пройти (відбувається одноразове відкриття замка дверей, або одноразовий прокрут турнікета);

– якщо це зворотний прохід дверей на вихід, то користувач просто натискає кнопку виходу, яка розташована біля ТКД й тим самим здійснює прохід.

Кожна точка контролю доступу має свій контролер доступу, виконавчий механізм (турнікет, електричний замок), зчитувачі, датчики положення та пульти управління. Також ТКД мають бути підключені до джерела живлення, яке працює від електричної мережі. Основне живлення подається до всіх компонентів системи, включаючи контролери доступу, зчитувачі, механізми блокування дверей, турнікети та інші пристрої. Це забезпечує стабільну та надійну роботу СКУД. Однак для забезпечення надійності роботи системи в умовах можливих перебоїв електропостачання часто використовується додаткове джерело живлення, як, наприклад, резервний акумулятор. Резервний акумулятор може служити для збереження живлення в разі тимчасової втрати основного електропостачання, щоб система продовжувала працювати принаймні обмежений час. Також, у великих об'єктах чи будівлях може бути розглянутий варіант використання додаткових джерел живлення, таких як генератори або інші системи

аварійного живлення, для підтримки роботи СКУД у випадку великих перебоїв електроенергії.

3.2 Розробка програмного забезпечення

Можна визначити декілька ключових аспектів, які важливі для розгляду ПЗ при впровадженні системи розпізнавання(рис.3.3).

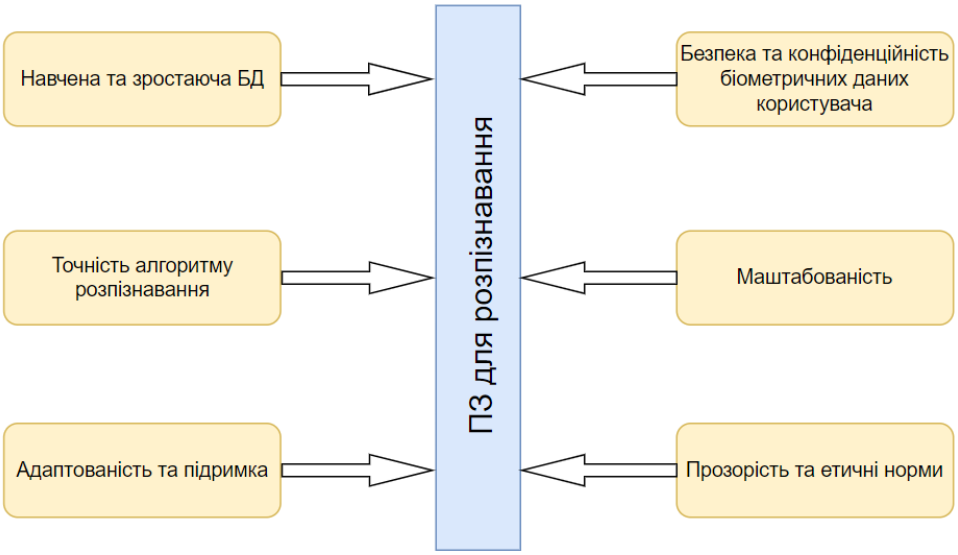

Рисунок 3.3 – Схема обов’язкових вимог до ПЗ

1) навчальна та зростаюча база даних (БД). Навчальні дані повинні бути різноманітними за статтю, етнічним походженням, освітленням, ракурсами та виразами обличчя. Це допомагає системі стати більш універсальною та точною в розпізнаванні різних типів облич. Важливо використовувати різні роздільності зображень для тренування, щоб система могла ефективно працювати з різними джерелами та умовами;
2) безпека та конфіденційність користувача. Забезпечити шифрування та очищення даних, щоб забезпечити високий рівень конфіденційності. Постачальники програмного забезпечення повинні мати ефективні плани на випадок витоку даних, включаючи заходи безпеки та політики контролю доступу;

3) точність алгоритму. Забезпечити низький коефіцієнт помилкового прийняття (КПП) і високий коефіцієнт помилкового відхилення (КПВ). У практиці для систем безпеки бажано, щоб КПП був низьким (мінімізує помилкові допуски) і КПВ був високим (мінімізує помилкові відмови в доступі);
4) масштабованість. Має бути можливість для розгортання в кількох локаціях, забезпечуючи спрощені процеси інтеграції та управління;
5) адаптованість і підтримка. Мають бути резервні варіанти та механізми відновлення для забезпечення неперервності роботи системи навіть у випадку збою й належна технічна підтримка для налаштування обладнання та вирішення можливих проблем. Людська підтримка може бути необхідною для ефективного управління системою та реагування на непередбачені ситуації;
6) прозорість і етичні норми. Вивчення методів, які використовує постачальник для збору навчальних даних й переконання в тому, що вони етичні та відповідають законам щодо конфіденційності та приватності. А також забезпечення прозорості у використанні даних і уникання неетичних методів, які можуть порушити конфіденційність користувачів.

Структура процесу розпізнавання. Схема роботи біометричної системи ідентифікації наведена у Додатку Ж, яка включає в себе наступні етапи:

– сенсорний етап, тобто робиться збір даних з сенсорної панелі чи камери;

– попередня обробка, тобто обробка отриманого зображення для видалення шуму та непотрібної інформації;

– екстракція ознак, тобто виділення важливих характеристик, які потрібні для подальшого аналізу;

– витягнення характеристик, тобто виділення ключових атрибутів, які будуть використовуватися для подальшого порівняння;

– порівняння витягнутих характеристик з відомими образами чи шаблонами в БД для прийняття рішення, використовуючи моделі та методи ідентифікації;

– етап прийняття рішень. Оцінка ступеня впевненості в рішенні, можливо, з використанням ймовірностей;

– подання результатів розпізнавання користувачу.

Структурна схема системи пошуку та розпізнавання об’єктів наведена в Додатку К, що включає:

– модуль пошуку;

– модуль розпізнавання;

– модуль відображення.

3.2.1 Використані технології

1) Для реалізації своєї системи я обрала мову програмування Python[19]. Завдяки їй можна вирішити широкий спектор завдань у сфері машинного навчання та Data Science. Також мову активно використовують в WEB-технологіях, у різних наукових аналізах та дослідженнях.

Python має безліч бібліотек та інструментів, що дозволяють розробникам створювати найрізноманітніші проєкти. На рисунку 3.4 зображено загальний логотим мови та бібліотеки, фреймворки для її розширення.

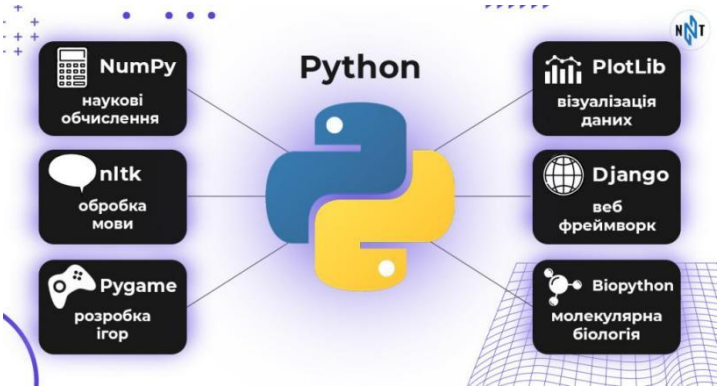

Рисунок 3.4 – Бібліотеки та фреймворки Python

Переваги мови:

– синтаксис Python не можна недооцінити, оскільки від дуже простий. Було прибрано все зайве й сам код залишився чистим і зрозумілим;

– підтримує різноманітні парадигми програмування, включаючи процедурне, об'єктно-орієнтоване та функціональне програмування;

– мова вражає своєю гнучкістю, це одна із причин популярності по всьому світу;

– розширюваність мови, бо існують багато бібліотек/фреймворків, які здатні вирішувати безліч завдань;

– стандарт PEP для написання коду є ще однією важливою перевагою. Він робить код підтримуваним і читабельним, навіть при зміні програмістів;

– має відкритий код, що дозволяє кому завгодно брати участь в його розробці і вдосконаленні. Багато нового функціоналу вносять сторонні розробники, що робить його дуже динамічною мовою.

2) Також мною був використаний інструмент Google Colab, який є зручним і легким інструментом для створення нейронних мереж.

Google Colaboratory, часто називають просто Colab (рис. 3.5), – це безкоштовна хмарна платформа, створена Google, щоб дозволити користувачам писати та виконувати код на Python у режимі спільного використання. Colab побудований на основі Jupyter Notebooks та забезпечує середовище для виконання коду, візуалізації даних та проведення експериментів у галузі машинного навчання.

Рисунок 3.5 – TensorFlow

Основні особливості та аспекти Google Colab:

– надає безкоштовний доступ до графічних обчислювальних одиниць (GPU) та тензорних обчислювальних одиниць (TPU), що може бути корисним для глибокого навчання;

– тісно інтегрований з Google Drive. Ви можете зберігати свої проєкти безпосередньо на диску, ділитися ними за допомогою посилання (буде загальнодоступним) й мати до них доступ з будь-якого пристрою;

– над проєктом одночасно може працювати декілька користувачів. Все коригування, розробка, внесені одним користувачем, відображаються іншим в реальному часі;

– має багато популярних бібліотек, таких як TensorFlow, PyTorch та OpenCV, встановлені наперед у Colab, що полегшує роботу у галузі машинного навчання;

– дозволяє легко імпортувати набори даних з різних джерел.

В порівнянні з центральним процесором (CPU), який виконує операції послідовно, GPU та TPU дозволяють проводити обробку паралельно, тим самим збільшуючи ефективність. Використання GPU спрощує роботу з графікою та іншими важкими обчислювальними завданнями, а TPU є ідеальним для тренування НМ.

Не кожний може дозволити собі вартість цих процесорів, а Google Colaboratory дає можливість користуватися цими потужностями безкоштовно протягом 12 годин (далі дані та файли будуть видалені, й доведеться починати спочатку).

3) Також для реалізації системи необхідні певні бібліотеки

а) TensorFlow – бібліотека, що дає можливість навчати штучний інтелект для вирішення різноманітних задач. Це інструмент для створення та навчання нейромереж. На рисунку 3.6 зображений логотип.

Рисунок 3.6 – TensorFlow

Фреймворк TensorFlow це відносно простий інструмент, який дозволяє швидко створювати нейромережі будь-якої складності. Він дуже доброзичливий для початківців, тому що містить багато прикладів і вже готових моделей машинного навчання, які можна вбудувати в будь– яку програму. А розвиненим розробникам TensorFlow надає тонкі налаштування та API для прискореного навчання.

Бібліотека розроблена мовою програмування Python і використовує швидкої мови C++, що сприяє ефективності обчислень та вирішення математичних завдань[20]. Створена Google як розширення внутрішньої бібліотеки компанії, TensorFlow є безкоштовною та має відкритий вихідний код, доступний на GitHub.

TensorFlow надає гнучкість та контроль завдяки функціональному API Keras і API підкласів моделей для розробки складних топологій. З метою швидкого прототипування та ефективної налагодження рекомендується використовувати активне виконання.

Цим можливості фреймворку TensorFlow не обмежуються. Бібліотеку також можна використовувати для навчання моделей на смартфонах та розумних пристроях (TensorFlow Lite) та створення корпоративних нейромереж (TensorFlow Extended).

b) Keras – бібліотека, спрямована на глибоке машинне навчання. На рисунку 3.7 зображено логотип цієї бібліотеки. Вона призначена для швидкого створення та налаштування моделей, які розповсюджують та обчислюють інформацію під час навчання. Однак Keras не виконує складних математичних обчислень і використовується як надбудова над іншими бібліотеками. З його допомогою легко будувати, навчати та використовувати нейронні мережі[20].

Рисунок 3.7 – Keras

Розроблена як гнучка та модульна бібліотека, яка не має проблем з налаштуванням чи модифікацією. Вона безкоштовна та має відкритий код.

Її застосування включає:

– дозволяє швидко та ефективно створювати різноманітні архітектури моделей НМ;

– легко налаштовувати параметри шарів, що спрощує оптимізацію та надає високу точності роботи;

– надає зручні засоби для обробки вхідних та вихідних даних моделі;

– легко вибирати та обробляти набори даних для навчання;

– дозволяє візуалізувати архітектуру та параметри моделі.

Це звісно можна реалізувати без використання даної бібліотеки, але це займе більше часу та буде суттєво складніше.

c) OpenCV (Open Source Computer Vision Library) – це відкрита бібліотека, призначена для використання алгоритмів комп'ютерного зору та обробки зображень[20]. Вона реалізована мовою програмування C++, також підтримує інші. OpenCV допускає роботу на різних платформах та операційних системах. Логотип бібліотеки зображено на рисунку 3.8.

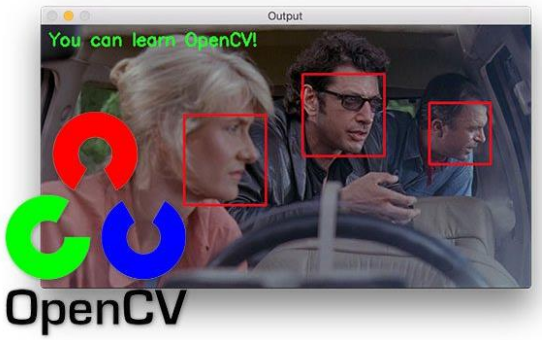

Рисунок 3.8 – OpenCV

Використовується для розв'язання широкого спектру завдань у сферах комп'ютерного зору та обробки зображень. Основні області застосування включають:

– дозволяє виявляти та аналізувати об'єкти на зображеннях, визначати їх форми, відстань та виконувати обробку;

– надає інструменти для роботи з алгоритмами машинного навчання, такі як класифікацію, виявлення різних характеристик та інше;

– використовується для створення системрозпізнавання біометричних даних чи певних рухів на відеозаписах або в реальному часі;

– ефективно допомагає в діагностиці та медицині;

– нагляду по відеокамерам;

– розпізнавання та обробки тексту;

– віртуальна реальність.

Це лише декілька прикладів використання OpenCV, і бібліотека продовжує розвиватися, впроваджуючи нові функції та можливості для різноманітних областей застосування.

d) Matplotlib Matplotlib – це пакет для візуалізації даних у Python, який надає можливість працювати з даними на різних рівнях:

– за допомогою модуля Pyplot, який розглядає графік як єдине ціле, спрощуючи процес створення;

– через об'єктно-орієнтований інтерфейс, де кожна фігура або її частина є окремим об'єктом. Це дає можливість вибірково змінювати їх властивості та відображення.

Бібліотека дозволяє будувати різноманітні типи графіків, діаграми, а також комбінувати їх. Приклади візуалізації даних представлені на рисунку 3.9.

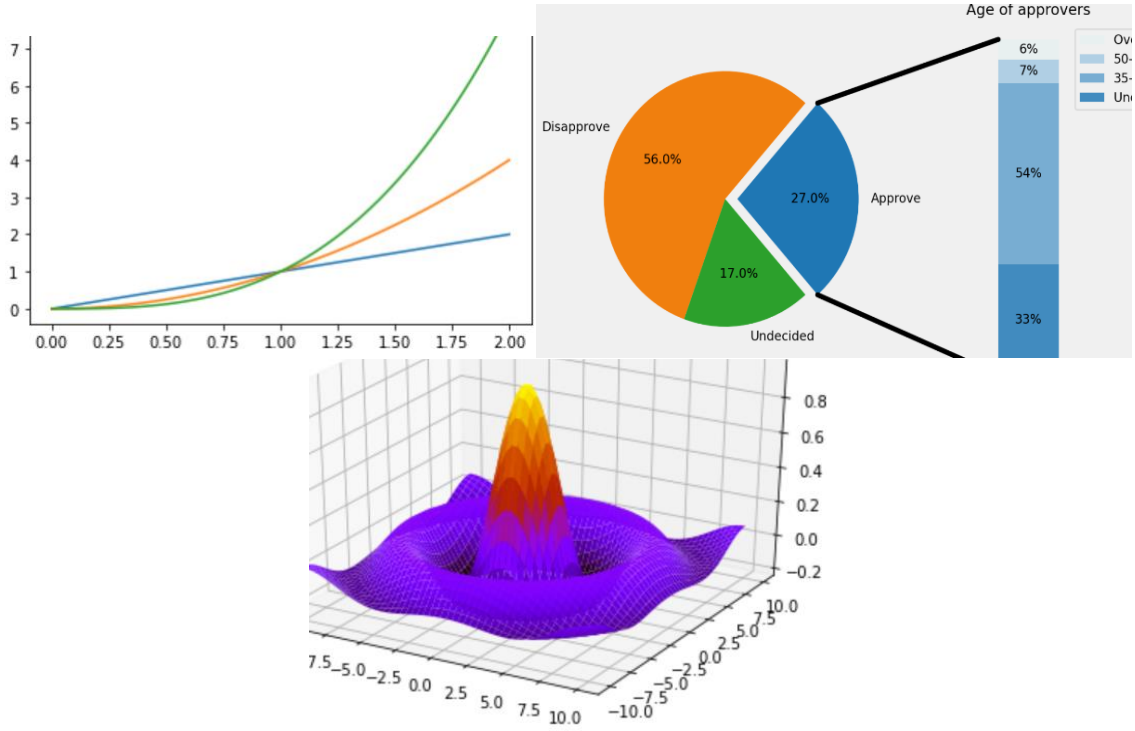

Рисунок 3.9 – Візуалізації даних за допомогою Matplotlib

і) NumPy (Numerical Python) – це бібліотека, яка надає можливість використання багатовимірних масивів та матриць, та використання величезних наборів математичних функцій для роботи з цими масивами.

Основним об'єктом NumPy є масив (ndarray), що представляє собою ефективний та гнучкий спосіб виконання операцій з числовими даними.

NumPy є важливим інструментом для наукових обчислень у Python та використовується в багатьох областях, включаючи обробку сигналів, обробку зображень, машинне навчання та інші.

3.2.2 Основні моменти реалізації НМ для розпізнавання облич

1) НМ на архітектурі VGG16

Першим кроком було створення датасету. Був створений власний датасет, який складається з 60 фото для навчання та 18 для тестування відомих осіб (6 осіб по 10 фото кожного, та 6 осіб по 3 відповідно)

Набір для навчання НМ Face_id зображено на рисунку 3.10.

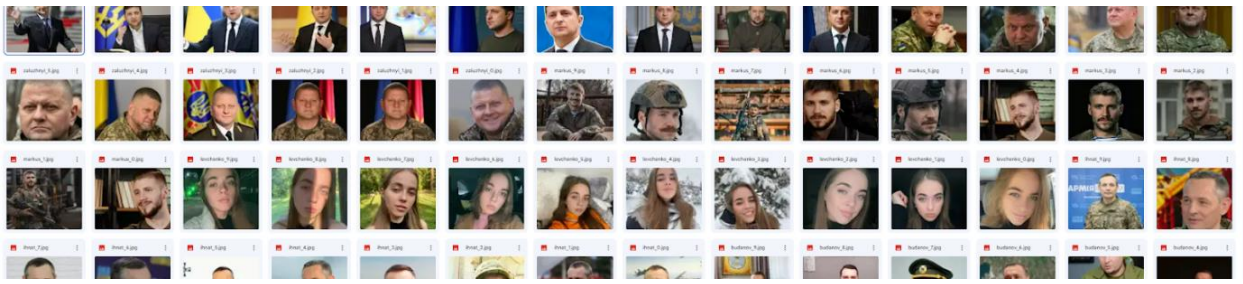

Рисунок 3.10 – Датасет для навчання мережі Face_id

Набір для тестування НМ Face_id зображено на рисунку 3.11.

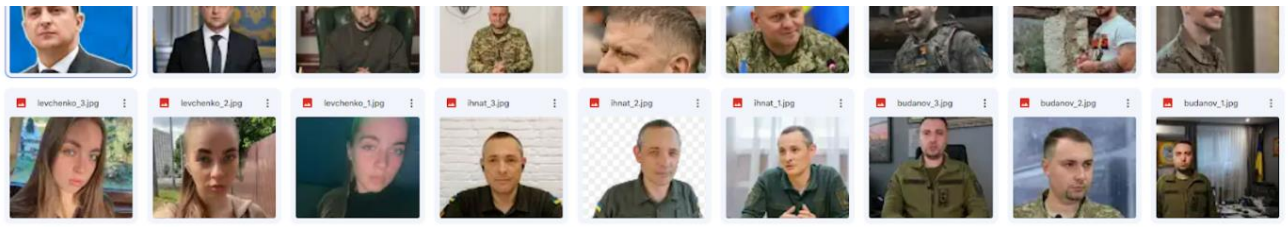

Рисунок 3.11 – Датасет для тестування мережі Face_id

Обробка вхідних даних мого датасету. Використовуючи dlib cnn face detector – я на звичайному фото шукаю саме обличчя на та вирізаю його. Після вилучення облич з фото, вони зберігаються в папку Images_crop, сортуючи за окремими особами.

На рисунку 3.12 зображено папки осіб, де зберігаються зображення.

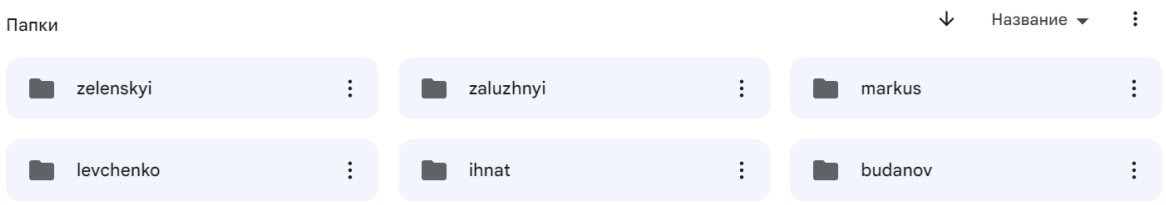

Рисунок 3.12 – Папки з особами, де зберігаються обрізані зображення облич

Кожна з цих папок має по 10 зображень для навчання НМ. Приклад зображено на рисунку 3.13.

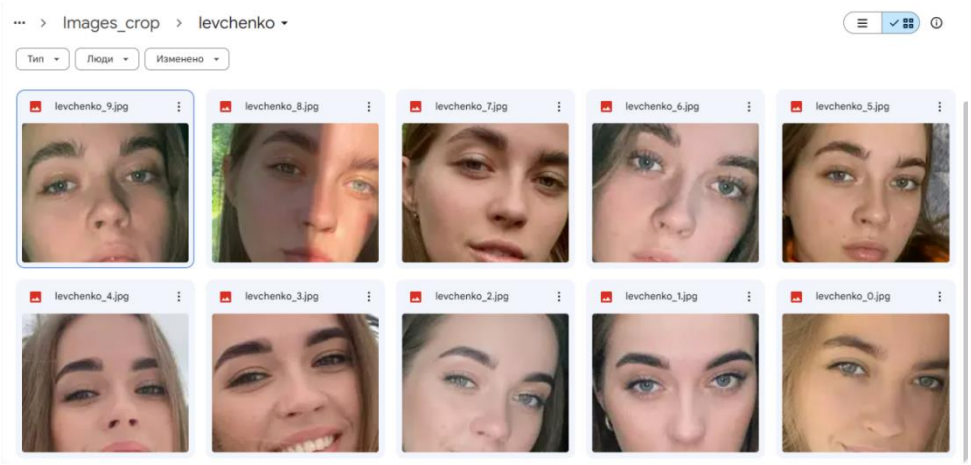

Рисунок 3.13 – Приклад вирізаного обличчя з фото

Було також визначено 6 моїх класів, які зображено на рисунку 3.14.

```
[ ]  person_rep

{0: 'zaluzhnyi',
 1: 'ihnat',
 2: 'levchenko',
 3: 'markus',
 4: 'zelenskyi',
 5: 'budanov'}
```

Рисунок 3.14 – Визначені 6 моїх класів

Для першої мережі використаємо архітектуру VGG16 (Visual Geometry Group 16) – це одна з архітектур глибоких згорткових нейронних мереж. Ця модель стала відомою своєю простотою та глибиною.

Основні характеристики VGG16:

– архітектура включає 16 шарів (13 згорткових і 3 повнозв'язаних) (рис.3.15);

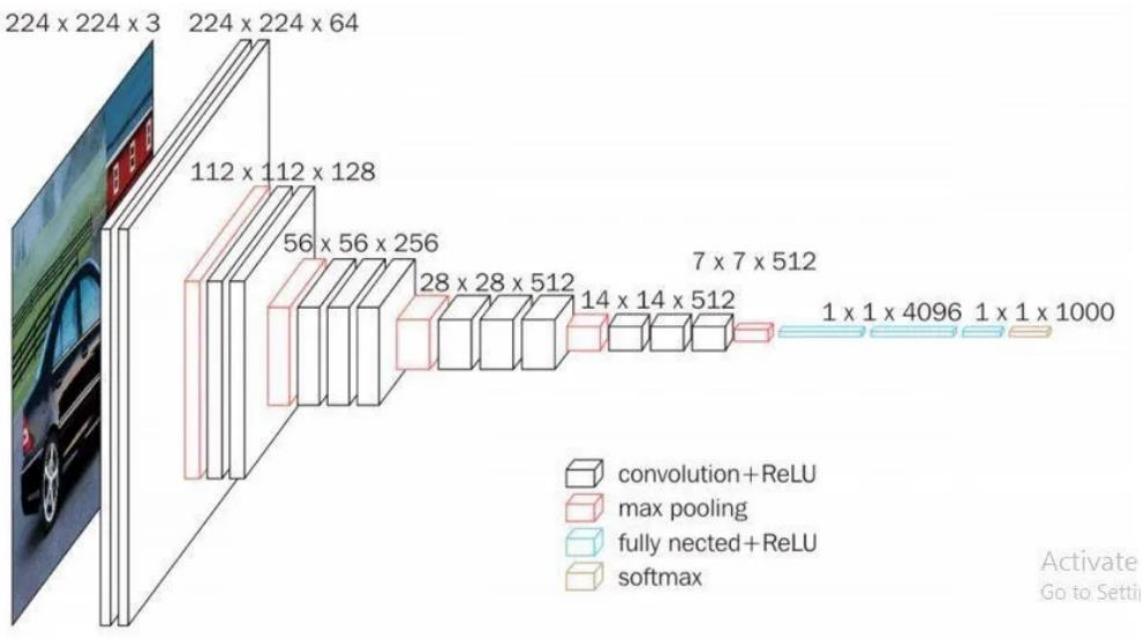

Рисунок 3.15 – Архітектура VGG16

– розмір фільтрів всіх шарів згортки 3x3, а максимальне згорткове зменшення відбувається за допомогою пулінгу розміром 2x2;

– активаційна функція – ReLU (ректифікована лінійна активація) використовується після кожного згорткового та повнозв'язаного шару;

– глибина мережі. Загальна кількість параметрів у VGG16 досить велика, що дозволяє їй вивчати складні ознаки зображень.

Навчання відбувалось у 100 епох. Результат навчання зображено на рисунку 3.16.

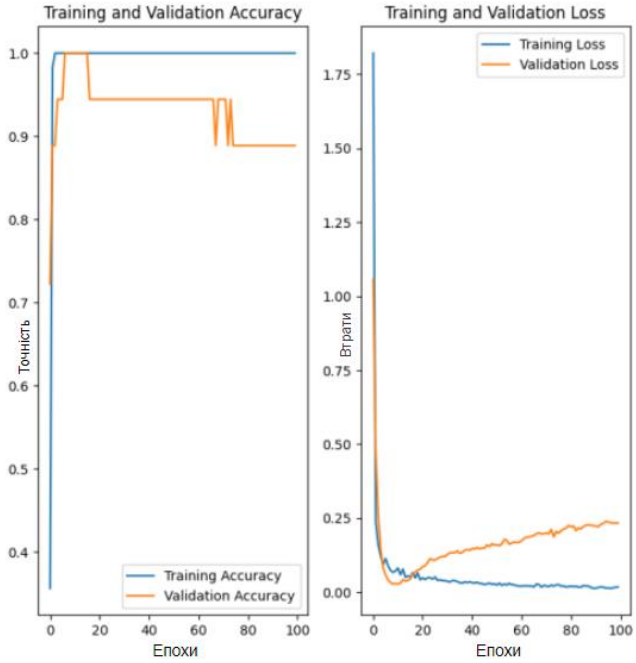

Рисунок 3.16 – Результат навчання мережі для розпізнавання облич на фото

З графіків залежності точності та помилки видно дуже сильне перенавчання. Це призводить до того, що модель заучує дані, й потім більш погано буде працювати на нових, раніше невідомих їй даних. Це треба покращити, тому щоб позбутись перенавчання трішки змінимо модель. Для цього добавляємо Dropout та змінимо активаційні функції. Після цього моя модель буде виглядати так, як зображено на рисунку 3.17.

```
classifier_model=Sequential()
classifier_model.add(Dense(units=100,input_dim=x_train.shape[1],kernel_initializer='glorot_uniform'))
classifier_model.add(BatchNormalization())
classifier_model.add(Activation('tanh'))
classifier_model.add(Dropout(0.3))
classifier_model.add(Dense(units=10,kernel_initializer='glorot_uniform'))
classifier_model.add(BatchNormalization())
classifier_model.add(Activation('tanh'))
classifier_model.add(Dropout(0.2))
classifier_model.add(Dense(units=6,kernel_initializer='he_uniform'))
classifier_model.add(Activation('softmax'))
classifier_model.compile(loss=tf.keras.losses.SparseCategoricalCrossentropy(),optimizer='nadam',metrics=['accuracy'])
```

Рисунок 3.17 – Покращена НМ для розпізнавання облич на фото

Опис моделі:

– sequential(): Створення порожньої послідовної моделі, до якої будуть послідовно додаватися шари;

– dense(units=100,input_dim=x_train.shape[1],kernel_initializer='glorot_uniform'): Перший шар нейронної мережі. Це повнозв'язковий шар зі 100 нейронами, вхідний розмірності, що дорівнює кількості ознак у навчальних даних (x_train.shape[1]). Вага ініціалізується з використанням методу "glorot_uniform". Ідея цього методу полягає в тому, щоб ініціалізувати ваги так, щоб враховувалися розміри вхідного та вихідного шарів. Це робиться для того, щоб уникнути проблеми зникливого градієнту при навчанні глибоких нейронних мереж, поліпшуючи стабільність та швидкість збіжності навчання;

– batchNormalization(): Шар нормалізації міні-пакетів. Він нормалізує активації попереднього шару, що може допомогти у прискоренні навчання та запобіганні проблемам із загасанням/вибухом градієнтів;

– dense(units=15, kernel_initializer='glorot_uniform'): Другий повнозв'язковий шар із 15 нейронами. Вага також ініціалізується з використанням методу "glorot_uniform";

– batchNormalization(): Ще один шар нормалізації міні-пакетів;

– dense(units=6, kernel_initializer='he_uniform'): Третій повнозв'язний шар із 6 нейронами. Тут ваги ініціалізуються методом рівномірного масштабування дисперсії;

– activation('softmax'): Шар активації softmax, який використовується для перетворення вихідних значень на ймовірність. Softmax зазвичай використовується у задачах класифікації;

– classifier_model.compile(...): Компіляція моделі. Задаються функція втрат (SparseCategoricalCrossentropy), оптимізатор (nadam) та метрика для відстеження продуктивності моделі (accuracy).

Архітектура покращеної мережі наведена у Додатку М.

Графік навчання зображено на рисунку 3.18.

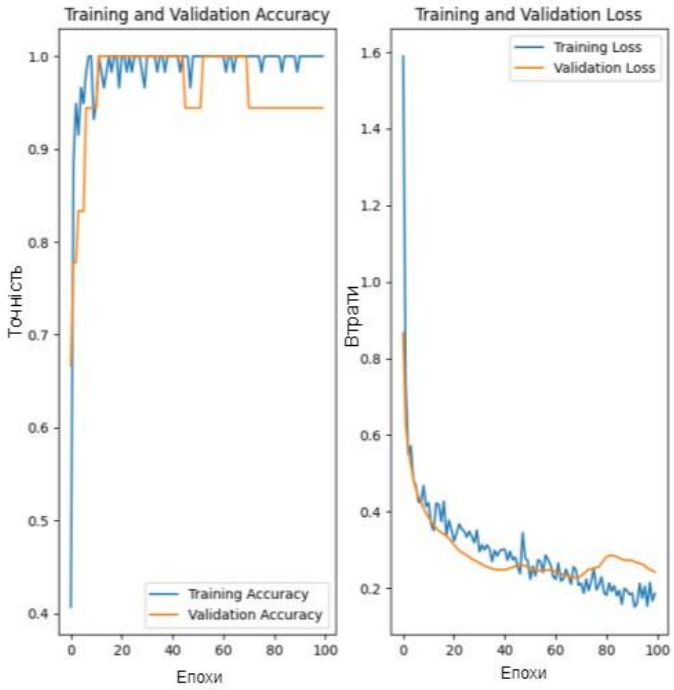

Рисунок 3.18 – Результат навчання мережі для розпізнавання облич на фото

Проаналізувавши графік, можна сказати те, що при збільшенні епох навчання, збільшується точність (accuracy). На іншому навпаки зменшується помилка, тобто функція втрат. Також можна зробити висновок щодо оптимальної кількості епох навчання – від 35 до 40 епох.

Протестуємо НМ на моєму тестовому фото. Результат роботи зображено на рисунку 3.19.

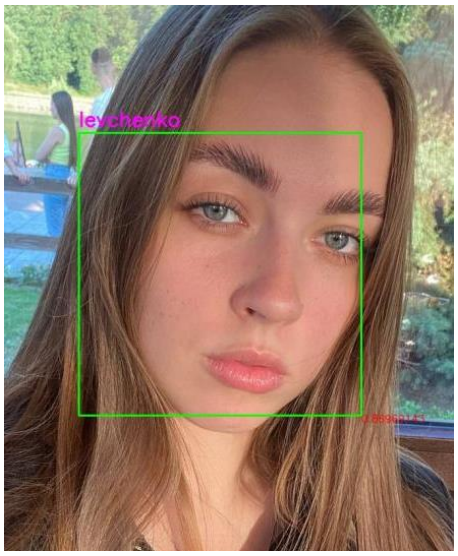

Рисунок 3.19 – Результат роботи мережі

НМ розпізнала мене як levchenko – це вірно, але точність цього розпізнавання лише 87%, що не є найкрашим варіантом.

2) Розпізнавання на основі RetinaFace

Розглянемо модель згорткової НМ RetinaFace, яка знаходить обличчя на зображені. Архітектура мережі складається з 4 основних частин, кожна з яких має своє призначення:

– backbone - основна (базова) мережа, що служить для отримання ознак з зображення, що надходить на вхід. Ця частина мережі є варіативною і до її основи можуть входити класифікаційні нейромережі, такі як ResNet, VGG, EfficientNet та інші;

– feature Pyramid Net (FPN) – згорткова нейронна мережа, побудована у вигляді піраміди, що служить для поєднання переваг карт ознак нижніх і верхніх рівнів мережі, перші мають високу роздільну здатність, але низьку семантичну, узагальнюючу здатність; другі - навпаки;

– classification Subnet – підмережа, що витягує з FPN інформацію про класи об'єктів, вирішуючи завдання класифікації;

– regression Subnet – підмережа, що витягує з FPN інформацію про координати об'єктів на зображенні, вирішуючи завдання регресії.

Навчати дану НМ буду на наборі даних FDDB – це набір мічених облич із набору даних Labeled Faces in the Wild. Містить в собі 5171 облич, де зображення також мають різну роздільну здатність[21]. Набір даних містить складні позиції, розфокусовані обличчя та низьку роздільну здатність. Включаються зображення як у відтінках сірого, так і в кольорі. Приклад даних зображено на рисунку 3.20.

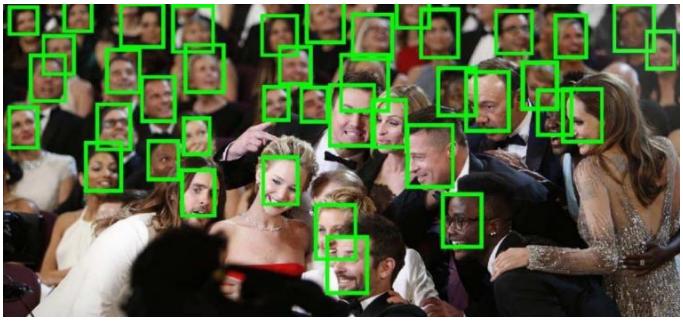

Рисунок 3.20 – Приклад даних датасету

Далі імпортуємо необхідні бібліотеки та модулі для подальшого використання в програмі (рис 3.21).

```
import numbers
import os
import queue as Queue
import threading
from typing import Iterable

import mxnet as mx
import numpy as np
import torch
from functools import partial
from torch import distributed
from torch.utils.data import DataLoader, Dataset
from torchvision import transforms
from torchvision.datasets import ImageFolder
```

Рисунок 3.21 – Імпорт бібліотек та необхідних модулів

Даний датасет розповсюджується у вигляді архіву з зображеннями та текстовим файлом анотації. Кожен рядок текстового файла може містити від одного до декількох наборів координат облич, тому я перегруповую дані, щоб вони могли використовуватись у процесі тренування (рис. 3.22).

```
img = cv2.imread(self.imgs_path[index])
height, width, _ = img.shape

labels = self.words[index]
annotations = np.zeros((0, 15))
if len(labels) == 0:
    return annotations
for idx, label in enumerate(labels):
    annotation = np.zeros((1, 15))
    # bbox
    annotation[0, 0] = label[0]  # x1
    annotation[0, 1] = label[1]  # y1
    annotation[0, 2] = label[0] + label[2]  # x2
    annotation[0, 3] = label[1] + label[3]  # y2
    # landmarks
    annotation[0, 4] = label[4]    # 10_x
    annotation[0, 5] = label[5]    # 10_y
    annotation[0, 6] = label[7]    # 11_x
    annotation[0, 7] = label[8]    # 11_y
    annotation[0, 8] = label[10]   # 12_x
    annotation[0, 9] = label[11]   # 12_y
    annotation[0, 10] = label[13]  # 13_x
    annotation[0, 11] = label[14]  # 13_y
    annotation[0, 12] = label[16]  # 14_x
    annotation[0, 13] = label[17]  # 14_y
    if (annotation[0, 4]<0):
        annotation[0, 14] = -1
    else:
        annotation[0, 14] = 1

    annotations = np.append(annotations, annotation, axis=0)
target = np.array(annotations)
if self.preproc is not None:
    img, target = self.preproc(img, target)

return torch.from_numpy(img), target
```

Рисунок 3.22 – Обробка даних

Основні компоненти архітектури включають в себе базову мережу (backbone), мережу піраміди функцій (FPN) для роботи з різними рівнями абстракції та одноступеневі головки (SSH) для класифікації, прогнозування обмежувальних рамок і прогнозування орієнтирів (landmarks).

Backbone відповідає за витягнення різних рівнів абстракції з вхідних зображень. FPN допомагає об'єднати ці різні рівні для покращення роботи з об'єктами різних розмірів. SSH використовуються для вирішення конкретних завдань, таких як класифікація, прогнозування обмежувальних рамок та прогнозування орієнтирів. Кожна з головок спеціалізується на виконанні певного завдання. На рисунку 3.23 приведено код, який створює модель нейронної мережі для виявлення обличчя за архітектурою RetinaNet.

```
self.body = _utils.IntermediateLayerGetter(backbone, cfg['return_layers'])
in_channels_stage2 = cfg['in_channel']
in_channels_list = [
    in_channels_stage2 * 2,
    in_channels_stage2 * 4,
    in_channels_stage2 * 8,
]
out_channels = cfg['out_channel']
self.fpn = FPN(in_channels_list,out_channels)
self.ssh1 = SSH(out_channels, out_channels)
self.ssh2 = SSH(out_channels, out_channels)
self.ssh3 = SSH(out_channels, out_channels)

self.ClassHead = self._make_class_head(fpn_num=3, inchannels=cfg['out_channel'])
self.BboxHead = self._make_bbox_head(fpn_num=3, inchannels=cfg['out_channel'])
self.LandmarkHead = self._make_landmark_head(fpn_num=3, inchannels=cfg['out_channel'])
```

Рисунок 3.23 – Модель НМ для виявлення ознак обличчя

Параметри тренування даної НМ зображені на рисунку 3.24.

```
cfg_re50 = {
    'name': 'Resnet50',
    'min_sizes': [[16, 32], [64, 128], [256, 512]],
    'steps': [8, 16, 32],
    'variance': [0.1, 0.2],
    'clip': False,
    'loc_weight': 2.0,
    'gpu_train': True,
    'batch_size': 24,
    'ngpu': 4,
    'epoch': 100,
    'decay1': 70,
    'decay2': 90,
    'image_size': 840,
    'pretrain': True,
    'return_layers': {'layer2': 1, 'layer3': 2, 'layer4': 3},
    'in_channel': 256,
    'out_channel': 256
```

Рисунок 3.24 – Параметри тренування НМ для виявлення ознак обличчя

Головний цикл навчання НМ зображена на рисунку 3.25. Можна побачити, що одна ітерація навчання НМ має типову послідовність дій навчання. Це збереження проміжних параметрів, оптимізації коефіцієнту навчання, отримання оброблених даних, прохід даних через мережу, обчислення втрат за допомогою функції втрат, та оптимізація тренованих параметрів.

```
for iteration in range(start_iter, max_iter):
    if iteration % epoch_size == 0:
        # create batch iterator
        batch_iterator = iter(data.DataLoader(
            dataset, batch_size, shuffle=True, num_workers=num_workers, collate_fn=detection_collate
        ))
        if (epoch % 10 == 0 and epoch > 0) or (epoch % 5 == 0 and epoch > cfg['decay1']):
            torch.save(net.state_dict(), save_folder + cfg['name']+ '_epoch_' + str(epoch) + '.pth')
        epoch += 1

    if iteration in stepvalues:
        step_index += 1
    lr = adjust_learning_rate(optimizer, gamma, epoch, step_index, iteration, epoch_size)

    # load train data
    images, targets = next(batch_iterator)
    images = images.cuda()
    targets = [anno.cuda() for anno in targets]

    # forward
    out = net(images)

    # backprop
    optimizer.zero_grad()
    loss_l, loss_c, loss_landm = criterion(out, priors, targets)
    loss = cfg['loc_weight'] * loss_l + loss_c + loss_landm
    loss.backward()
    optimizer.step()
```

Рисунок 3.25 – Головний цикл навчання НМ для виявлення ознак обличчя

Результат навчання зображено на рисунку 3.26.

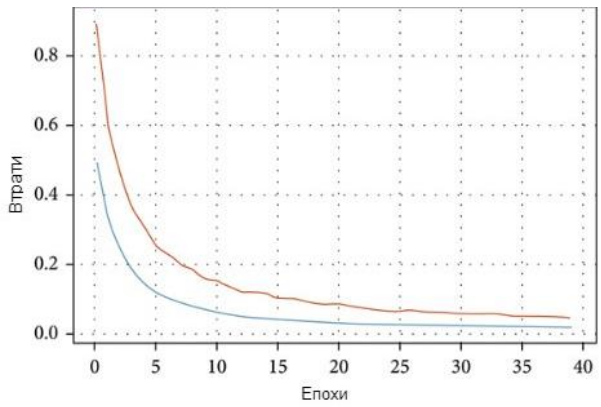

Рисунок 3.26 – Графік значення функції втрат після кожної епохи навчання

З графіку видно, що з кожною епохою функція втрат зменшується й прямує до 0, що збільшує точність розпізнавання.

На рисунку 3.27 приведені приклади датасету, який використовувався для навчання НМ кодувальника обличь.

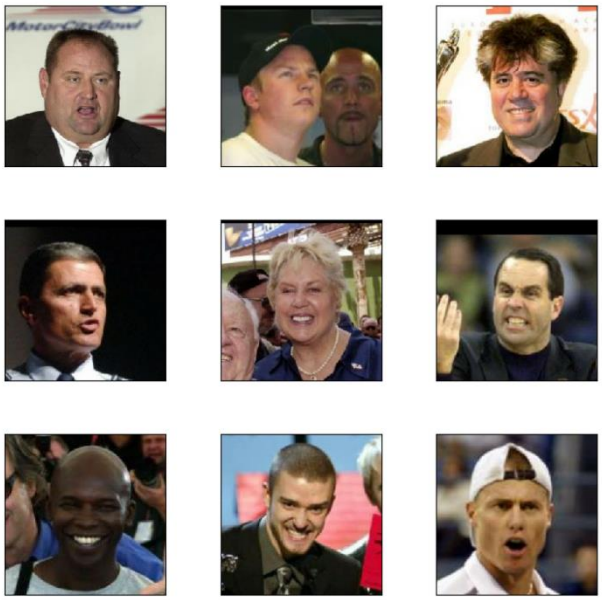

Рисунок 3.27 – Приклад даних датасету

Далі імпортуємо необхідні бібліотеки та модулі для подальшого використання в програмі (рис 3.28).

```
import argparse
import logging
import os
from datetime import datetime

import numpy as np
import torch
from backbones import get_model
from dataset import get_dataloader
from losses import CombinedMarginLoss
from lr_scheduler import PolynomialLRWarmup
from partial_fc_v2 import PartialFC_V2
from torch import distributed
from torch.utils.data import DataLoader
from torch.utils.tensorboard import SummaryWriter
```

Рисунок 3.28 – Імпорт бібліотек та необхідних модулів

Даний датасет розповсюджується у бінарному форматі бібліотеки mxnet. Тому, етап обробки даних складається з двох кроків: завантаження і перетворення бінарних даних у об’єкти тензорів, та доповнення і нормалізація даних (рис. 3. 29).

```
    self.transform = transforms.Compose(
        [transforms.ToPILImage(),
         transforms.RandomHorizontalFlip(),
         transforms.ToTensor(),
         transforms.Normalize(mean=[0.5, 0.5, 0.5], std=[0.5, 0.5,
         ])
    self.root_dir = root_dir
    self.local_rank = local_rank
    path_imgrec = os.path.join(root_dir, 'train.rec')
    path_imgidx = os.path.join(root_dir, 'train.idx')
    self.imgrec = mx.recordio.MXIndexedRecordIO(path_imgidx, path_
    s = self.imgrec.read_idx(0)
    header, _ = mx.recordio.unpack(s)
    if header.flag > 0:
        self.header0 = (int(header.label[0]), int(header.label[1])
        self.imgidx = np.array(range(1, int(header.label[0])))
    else:
        self.imgidx = np.array(list(self.imgrec.keys))

def __getitem__(self, index):
    idx = self.imgidx[index]
    s = self.imgrec.read_idx(idx)
    header, img = mx.recordio.unpack(s)
    label = header.label
    if not isinstance(label, numbers.Number):
        label = label[0]
    label = torch.tensor(label, dtype=torch.long)
    sample = mx.image.imdecode(img).asnumpy()
    if self.transform is not None:
        sample = self.transform(sample)
    return sample, label

def __len__(self):
    return len(self.imgidx)
```

Рисунок 3.29 – Обробка даних

На рисунку 3.30 можна побачити код, який створює модель нейронної мережі для кодування облич за архітектурою ResNet, але без останніх повно зв'язних слоїв. Вони замінені на функцію “сплощення” матриці у вектор.

```
class IResNet(nn.Module):
    fc_scale = 7 * 7
    def __init__(self,
                 block, layers, dropout=0, num_features=512, zero_init_residual=False,
                 groups=1, width_per_group=64, replace_stride_with_dilation=None, fp16=False):
        super(IResNet, self).__init__()
        self.extra_gflops = 0.0
        self.fp16 = fp16
        self.inplanes = 64
        self.dilation = 1
        if replace_stride_with_dilation is None:
            replace_stride_with_dilation = [False, False, False]
        if len(replace_stride_with_dilation) != 3:
            raise ValueError("replace_stride_with_dilation should be None "
                             "or a 3-element tuple, got {}".format(replace_stride_with_dilation))
        self.groups = groups
        self.base_width = width_per_group
        self.conv1 = nn.Conv2d(3, self.inplanes, kernel_size=3, stride=1, padding=1, bias=False)
        self.bn1 = nn.BatchNorm2d(self.inplanes, eps=1e-05)
        self.prelu = nn.PReLU(self.inplanes)
        self.layer1 = self._make_layer(block, 64, layers[0], stride=2)
        self.layer2 = self._make_layer(block,
                                       128,
                                       layers[1],
                                       stride=2,
                                       dilate=replace_stride_with_dilation[0])
        self.layer3 = self._make_layer(block,
                                       256,
                                       layers[2],
                                       stride=2,
                                       dilate=replace_stride_with_dilation[1])
        self.layer4 = self._make_layer(block,
                                       512,
                                       layers[3],
                                       stride=2,
                                       dilate=replace_stride_with_dilation[2])
        self.bn2 = nn.BatchNorm2d(512 * block.expansion, eps=1e-05,)
        self.dropout = nn.Dropout(p=dropout, inplace=True)
        self.fc = nn.Linear(512 * block.expansion * self.fc_scale, num_features)
        self.features = nn.BatchNorm1d(num_features, eps=1e-05)
        nn.init.constant_(self.features.weight, 1.0)
        self.features.weight.requires_grad = False
```

Рисунок 3.30 – Модель HM для кодування обличь

Гіперпараметри для HM кодувальника зображені на рисунку 3.31.

```
config.margin_list = (1.0, 0.5, 0.0)
config.network = "r50"
config.resume = False
config.output = None
config.embedding_size = 512
config.sample_rate = 1.0
config.fp16 = True
config.momentum = 0.9
config.weight_decay = 5e-4
config.batch_size = 128
```

```
config.batch_size = 128
config.lr = 0.1
config.verbose = 2000
config.dali = False

config.rec = "/train_tmp/faces_emore"
config.num_classes = 85742
config.num_image = 5822653
config.num_epoch = 20
config.warmup_epoch = 0
```

Рисунок 3.31 – Гіперпараметри для НМ кодувальника

На рисунку 3.32 зображено частину коду цикл навчання НМ. Кожна ітерація навчання НМ має типову послідовність дій навчання. Але, також я додала код для роботи з різними оптимізаціями навчання - наприклад, використання 16-ти бітних чисел замість 32-х, що зменшує використання пам’яті пристрою.

```
for epoch in range(start_epoch, cfg.num_epoch):

    if isinstance(train_loader, DataLoader):
        train_loader.sampler.set_epoch(epoch)
    for _, (img, local_labels) in enumerate(train_loader):
        global_step += 1
        local_embeddings = backbone(img)
        loss: torch.Tensor = module_partial_fc(local_embeddings, local_labels)

        if cfg.fp16:
            amp.scale(loss).backward()
            if global_step % cfg.gradient_acc == 0:
                amp.unscale_(opt)
                torch.nn.utils.clip_grad_norm_(backbone.parameters(), 5)
                amp.step(opt)
                amp.update()
                opt.zero_grad()
        else:
            loss.backward()
            if global_step % cfg.gradient_acc == 0:
                torch.nn.utils.clip_grad_norm_(backbone.parameters(), 5)
                opt.step()
                opt.zero_grad()
        lr_scheduler.step()

        with torch.no_grad():
            if wandb_logger:
                wandb_logger.log({
                    'Loss/Step Loss': loss.item(),
                    'Loss/Train Loss': loss_am.avg,
                    'Process/Step': global_step,
                    'Process/Epoch': epoch
                })

            loss_am.update(loss.item(), 1)
            callback_logging(global_step, loss_am, epoch, cfg.fp16, lr_scheduler.get_last_lr()[0], amp)
```

Рисунок 3.32 – Частинка коду тренування нейронної мережі

Графік результатів тренування НМ зображений на рисунку 3.33.

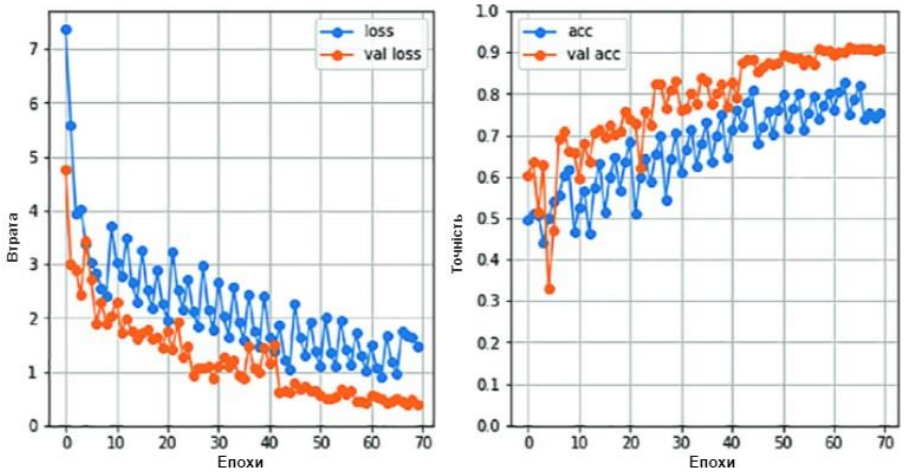

Рисунок 3.33 – Результат тренування нейронної мережі

З графіків видно, що з кожною епохою функція втрат loss зменшується, а точність acc зростає.

3.2.3 Основні моменти реалізації НМ для розпізнавання відбитків пальців

Першим кроком було створення папок (рис 3.34) з зображеннями для навчання. Для цього я створила 4 папки, в які додала сканування 4 власних пальця (рис 3.34).

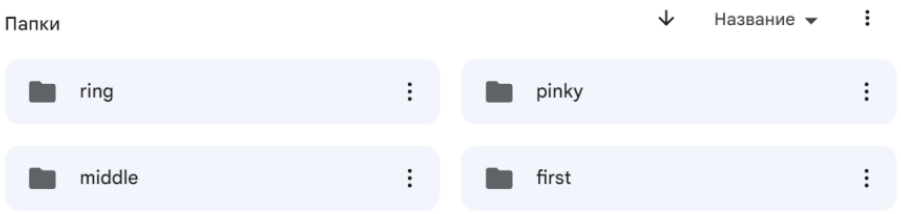

Рисунок 4.34 – Папки з фото

Далі імпортуємо необхідні бібліотеки та модулі для подальшого використання в програмі (рис 3.35).

```
import os
import numpy as np
import pandas as pd
import time

import matplotlib.pyplot as plt
import cv2
```

```
import imageio
import imgaug as ia
import imgaug.augmenters as iaa

from tensorflow import keras
from PIL import Image
```

Рисунок 3.35 – Імпорт бібліотек та необхідних модулів

– Os для роботи з операційною системою, забезпечує функції для взаємодії з операційною системою, такі як робота з файловою системою;

– numpy (np) бібліотека для використання масивів та математичних операцій;

– pandas (pd) бібліотека для обробки та аналізу даних у вигляді таблиць (DataFrame);

– time модуль для вимірювання часу виконання коду;

– matplotlib.pyplot as plt бібліотека для створення графіків та візуалізації даних;

– cv2 OpenCV бібліотека для комп'ютерного зору та обробки зображень;

– Imageio бібліотека для читання та запису різних форматів зображень та відео;

– imgaug (ia) бібліотека для аугментації зображень;

– imgaug.augmenters as iaa модуль для визначення аугментаційних операцій;

– tensorflow.keras високорівневий API над TensorFlow для побудови та тренування нейронних мереж.

Обробка вхідних даних мого датасету включає створення синтетичних зображень за допомогою технік аугментації даних (рис. 3.36). Аугментація даних використовується для розширення обсягу тренувального набору даних, щоб покращити здатність моделі глибинного навчання до узагальнення та зменшити перенавчання.

Техніки аугментації даних:

– iaa.Flipud: Вертикальне відображення з ймовірністю 100%. В результаті отримується зображення, яке віддзеркалено вертикально;

– iaa.Affine: Обертання зображення, діапазон дії від 50° проти до -50° за стрілкою годинника. Це створює дві версії обернених зображень;

– iaa.Crop: Вирізання частини зображення від країв на випадковий відсоток. Також створює дві версії вирізаних зображень;

– iaa.GammaContrast: Збільшення гамми для покращення контрасту. Створює дві версії зображень з різними рівнями контрасту;

– iaa.GaussianBlur: Застосовує гаусівське розмиття зображення з вказаним значенням розміру ядра розмиття sigma. Створює дві версії розмитих зображень.

Й в кінці кожної техніки зберігаю створені синтетичні зображення за вказаними шляхами та іменами файлів за допомогою cv2.imwrite(save_filename, augmented_image). Приклад датасету одного з пальців зображено на рисунку 3.36.

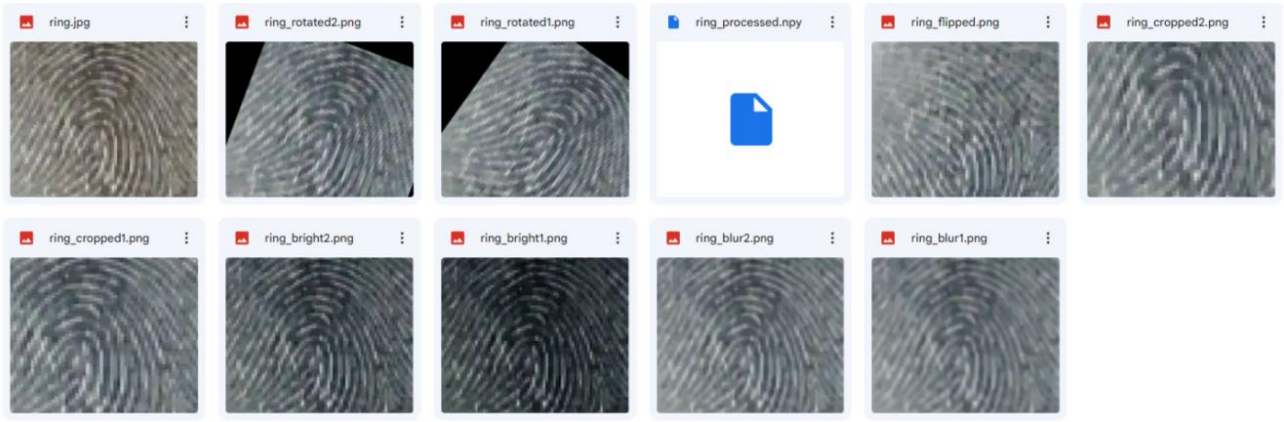

Рисунок 3.36 – Збільшення датасету

Для реалізації я використовую згорткову нейронну мережу, модель якої складається з таких шарів:

– reshape(input_shape=input_shape, target_shape=convolution_shape): Цей шар змінює форму вхідного тензора, перетворюючи його на форму, яка відповідає тривимірному тензору (зображенню) розміром convolution_shape (self.__DIMEN x self.__DIMEN x 3);

– conv2D(64, kernel_size=kernel_size_1, strides=strides, activation='relu'): Перший згортковий шар з 64 фільтрами, ядро яких має розмір kernel_size_1, функцією активації ReLU. Шар виконує згортку зображення з ядром, використовуючи вказаний крок strides;

– maxPooling2D(strides=2): Пулінг– шар (шар субдискретизації) з ядром 2x2, який виконує операцію максимального пулінгу та зменшує розмірність зображення;

– conv2D(128, kernel_size=kernel_size_2, strides=strides, activation='relu'): Другий згортковий шар з 128 фільтрами та ядром розміру kernel_size_2. Знову ж таки, використовується функція активації ReLU;

– maxPooling2D(strides=2): Другий шар максимального пулінгу з ядром 2x2.

– conv2D(128, kernel_size=kernel_size_3, strides=strides, activation='relu'): Третій згортковий шар із 128 фільтрами та ядром розміру kernel_size_3. Функція активації – ReLU;

– maxPooling2D(strides=2): Третій шар максимального пулінгу з ядром 2x2.

– conv2D(256, kernel_size=kernel_size_3, strides=strides, activation='relu'): Четвертий згортковий шар з 256 фільтрами та ядром розміру kernel_size_3. Функція активації – ReLU;

– flatten(): Шар, що перетворює вихідні дані попереднього шару на одномірний вектор;

– dense(1024, activation='relu'): Повнозв'язний шар з 1024 нейронами та функцією активації ReLU;

– dense(1024, activation=activations.sigmoid): Ще один повнозв'язний шар із 1024 нейронами, але з сигмоїдною функцією активації. Цей шар створює вектор ознак, який використовуватиметься для порівняння пар зображень.

Параметри НМ для розпізнавання відбитків пальців зображена на рисунку 3.37.

```
Model: "model"
__________________________________________________________________________________________________
 Layer (type)                Output Shape              Param #   Connected to
==================================================================================================
 input_1 (InputLayer)        [(None, 150528)]          0         []

 input_2 (InputLayer)        [(None, 150528)]          0         []

 sequential (Sequential)     (None, 1024)              1071158   ['input_1[0][0]',
                                                       40         'input_2[0][0]']

 lambda (Lambda)             (None, 1024)              0         ['sequential[0][0]',
                                                                  'sequential[1][0]']

 dense_2 (Dense)             (None, 1)                 1025      ['lambda[0][0]']

==================================================================================================
Total params: 107116865 (408.62 MB)
Trainable params: 107116865 (408.62 MB)
Non-trainable params: 0 (0.00 Byte)
```

Рисунок 3.37 – Параметри НМ для розпізнавання відбитків пальців

Навчання НМ відбувається 15 епох. Й результат навчання зображено на рисунку 3.38.

Рисунок 3.38 – Графік функції втрат

3.3 Розробка інтерфейсу

Було спроектовано візуальну частину системи, для цього розроблено додаток у програмному середовищі PyCharm, включаючи код з НМ для розпізнавання обличчя. Головний екран зображено на рисунку 3.39.

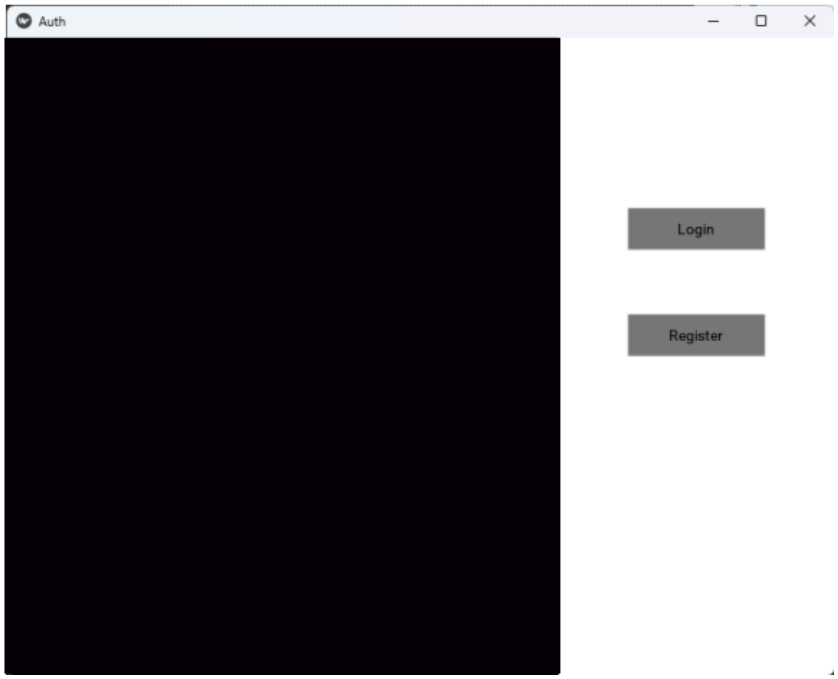

Рисунок 3.39 – Екран додатку

Щоб у чорній стороні екрану можна бачити фото з камери, потрібно отримати доступ до веб-камери, адже саме завдяки їй можна сфотографувати людину для розпізнання. Для інтеграції веб-камери у додаток я використовувала об’єкт Camer бібліотеки kivy, яка була обрана для створення графічного користувацького інтерфейсу. Цей об’єкт зчитує потік даних з камери та відображає його по кадрах на графічному елементі.

Для того щоб під’єднати камеру до НМ я перевизначила метод on_tex класу Camera у своєму класі CameraWidget, тому що саме він викликається при отриманні нових даних з пристрою, та відображенні їх на графічному елементі. Також ці данні вже у форматі кадру, тому їх легко передати на вхід до НМ (рис. 3.40).

```
def on_tex(self, camera):
    texture = camera.texture
    size = texture.size
    frame = texture.pixels

    self.or_img = Image.frombytes(mode='RGBA', size=size, data=frame).convert('RGB')

    img = self.or_img.copy()
    self.detections = detect.run(img, run_id=self.run_id, return_image=True)

    detections_texture: Texture = Texture.create(size=size)
    detections_texture.blit_buffer(img.tobytes(), colorfmt='rgb', bufferfmt='ubyte')
    detections_texture.flip_vertical()

    self.texture = texture = detections_texture
    self.texture_size = list(texture.size)
    self.canvas.ask_update()
```

Рисунок 3.40 – Підключення камери

Для реалізації сценаріїв аутентифікаї та реєстрації у системі у клас CameraWidget були додані методи register та login (рис. 3.41).

```
def register(self, username):
    for i, detection in enumerate(self.detections):
        face_img = det2ext.align_face(self.or_img, detection[5:])
        vector = extract.run(face_img)[0]
        UserService.register_user(username=username, vector=vector)

def login(self, username):
    for i, detection in enumerate(self.detections):
        face_img = det2ext.align_face(self.or_img, detection[5:])
        vector = extract.run(face_img)[0]
        has_access = UserService.has_access(username=username, vector=vector)
        print(f"Test User has access: {has_access}")
```

Рисунок 3.41 – Методи реєстрації та входу

Зі своєї веб-камери я зробила фото для подальшого тестування (рис. 3.42).

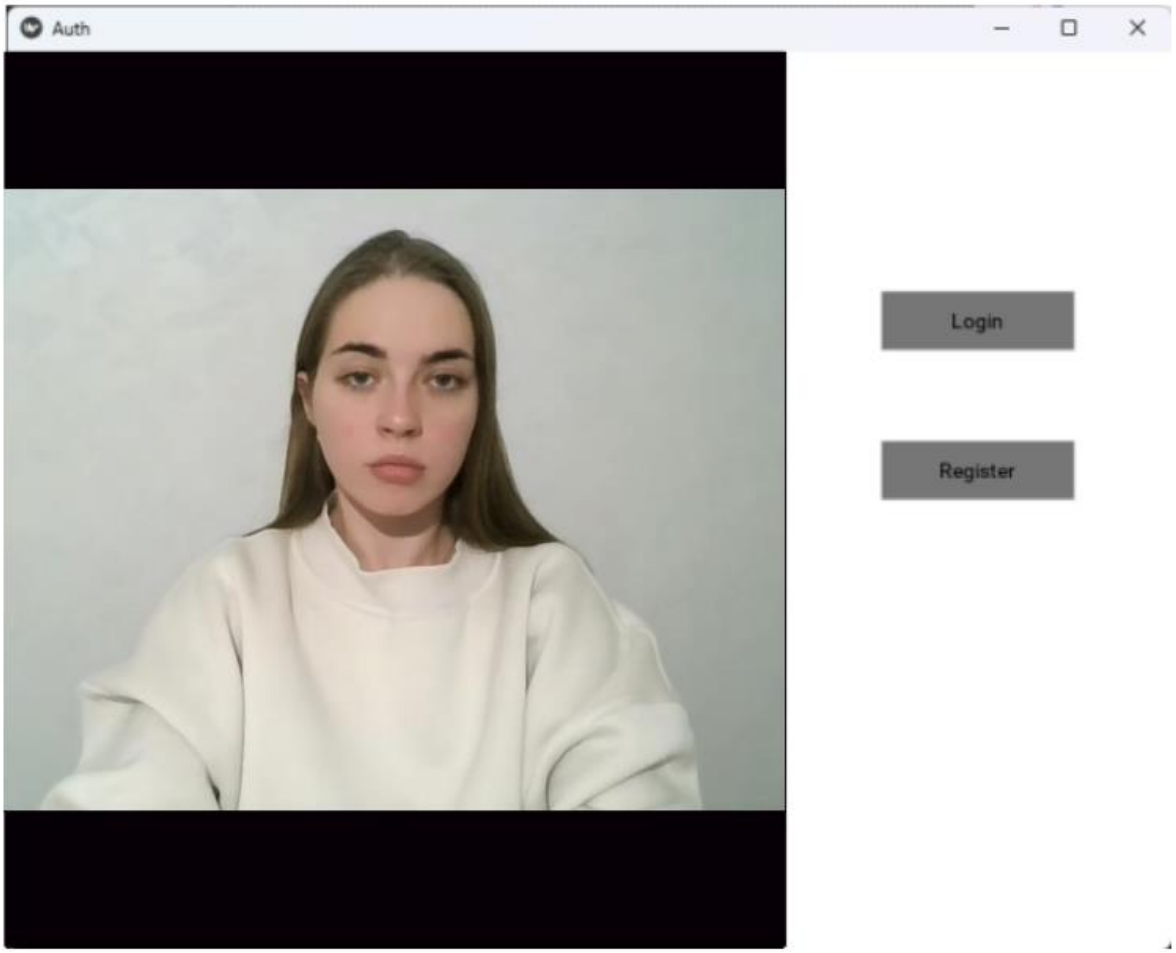

Рисунок 3.42 – Скрін екрану додатку

Висновок до розділу 3

Спроєктовано та описано біометричну систему контролю допуску та ідентифікації осіб на режимних об’єктах, основні складові якої включають:

– біометричні сенсори;

– біометричне програмне забезпечення;

– контролери доступу;

– серверне програмне забезпечення;

– мережеві пристрої для зв'язку між біометричними сенсорами, контролерами та серверами;

– живлення.

Зроблено аналіз вимог до системи, й на цього визначено ключові аспектів, які важливі при впровадженні системи розпізнавання.

Обрані мова програмування (Python), програмне середовище (Colab та PyCharm) та опис використаних технологій, а саме використано бібліотеки TensorFlow, Keras, OpenCV, NumPy та пакет Matplotlib.

Розроблено НМ для розпізнавання обличчя та відбитків пальців, що базуються на архітектурі згорткових нейронних мереж (ЗНМ), оскільки вони ефективно показують себе з завданнями обробки зображень, і саме тому вони широко використовуються у задачах розпізнавання об'єктів. НМ на архітектурі RetinaFace показала кращі результат точності, ніж НМ з архітектурою VGG16. Тому для реалізації системи було обрано її.

Розроблено інтерфейс для адміністратора системи контролю та управління доступом на режимних об’єктах на основі розпізнавання обличчя.

4 ТЕСТУВАННЯ СИСТЕМИ

4.1 Тестування нейронних мереж

4.1.1 НМ для відбитків пальців.

Проаналізуємо оптимальну кількість епох навчання НМ для відбитків пальців, для цього я спочатку навчала мережу 15 епох, й потім збільшила кількість рівно в 2 рази, тобто навчання тривало 30 епох. Результат функції втрат наведено на рисунках 4.1 та 4.2 відповідно.

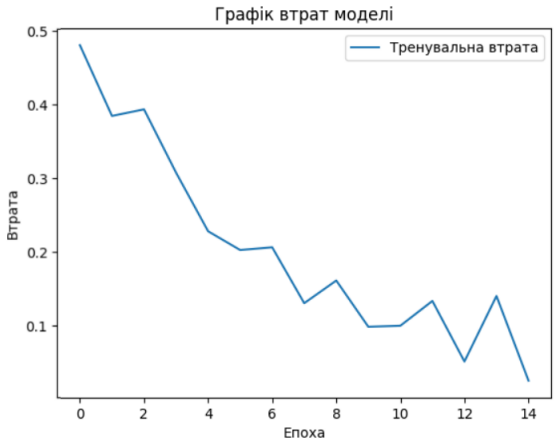

Рисунок 4.1 – Графік функції втрат при 15 епохах

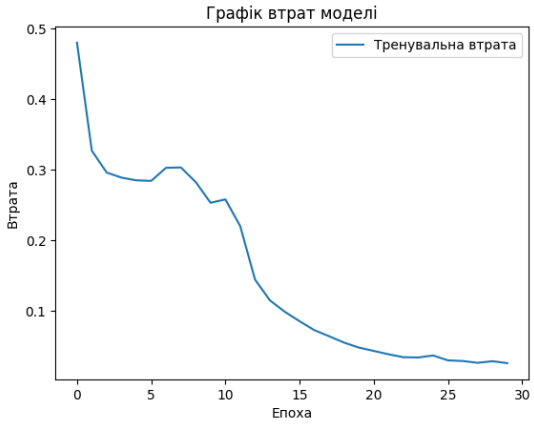

Рисунок 4.2 – Графік функції втрат при 30 епохах

З графіку можна зробити висновок, що більш якісніше та плавніше відбувається навчання при 30 епохах, тим саме точність розпізнавання систематично збільшується з кожною епохою. А помилка прямує до 0.

Тепер протестуємо оновлену НМ для відбитків пальців. Для цього з датчику сканування до системи поступає тестовий відбиток (рис. 4.3).

Рисунок 4.3 – Відбиток для тестування

Після чого тестовий шаблон зберігаємо в базі даних та за допомогою НМ й в подальшому порівнюємо новий відбиток з наявними шаблонами для визначення ідентифікації. Тобто відбувається визначення того, чи відбиток пальця відповідає існуючому шаблону, і якщо так - то доступ буде дозволено, якщо все ж таки ні, то відхиленні запиту. Результат зображено на рисунку 4.4.

```
first
1/1 [==============================] - 0s 20ms/step
[3.215877e-05]
first
1/1 [==============================] - 0s 20ms/step
[1.7746976e-05]
middle
1/1 [==============================] - 0s 19ms/step
[0.00501333]
middle
1/1 [==============================] - 0s 21ms/step
[0.00407963]
ring
1/1 [==============================] - 0s 30ms/step
[0.9002592]
IMAGE ring_test.jpg is ring with confidence of 0.9002591967582703
ring
1/1 [==============================] - 0s 23ms/step
[0.98359597]
IMAGE ring_test.jpg is ring with confidence of 0.9835959672927856
pinky
1/1 [==============================] - 0s 22ms/step
[0.00535351]
pinky
1/1 [==============================] - 0s 23ms/step
[2.2634285e-05]
```

Рисунок 4.4 – Результат тестування НМ для розпізнавання відбитків пальців

З результатів видно, що точність розпізнавання тестового зразка сягає 90 та 98%. Такі результати є досить високими, тому покращення мережі на даному етапі не потрібно. Використання даної НМ є доцільним у різних галузях, таких як безпека, контроль доступу, мобільні пристрої, банківські послуги тощо.

4.1.2 НМ розпізнавання обличчя

1) Проаналізуємо оптимальну кількість епох навчання НМ для розпізнавання обличчя. Для першої версії НМ я використовувала 25 епох для навчання. Для другої версії я збільшила кількість до 50. Результат наведено на рисунках 4.5 та 4.6 відповідно.

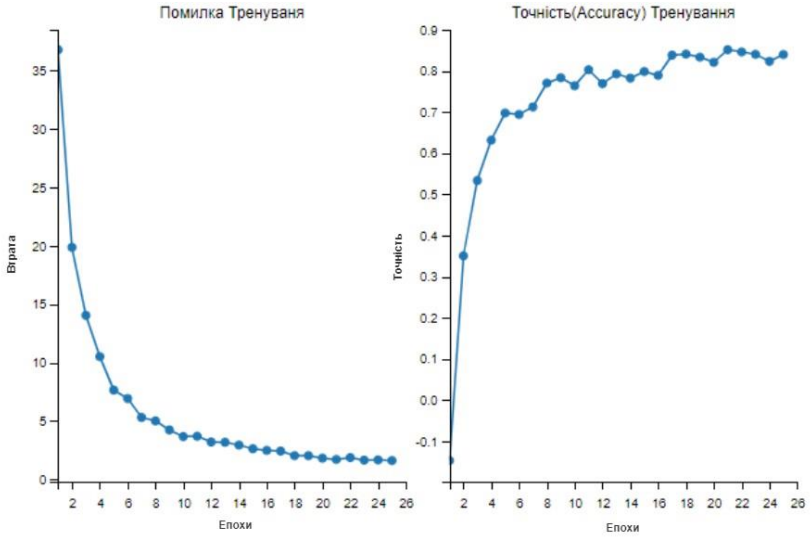

Рисунок 4.5 – Графік навчання при 25 епохах

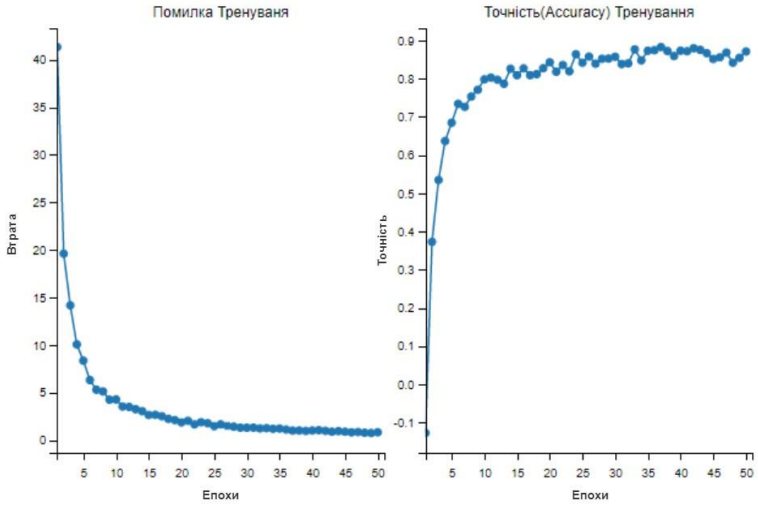

Рисунок 4.6 – Графік навчання при 50 епохах

При навчанні на 25-ти епохах помилка становила 1.62, а точність - 0.83. При навчанні на 50-ти я отримала помилку у 0.81 і точність у 0.87. Також проаналізувавши графіки можна зробити висновок, що збільшення кількості епох не дає суттєвого приросту точності.

2) Іншим методом покращення точності НМ є вибір оптимізатора параметрів. Я провела два експерименти з SGD та Adam оптимізаторами на 50-ти епохах. Результати можна побачити на рисунку 4.7.

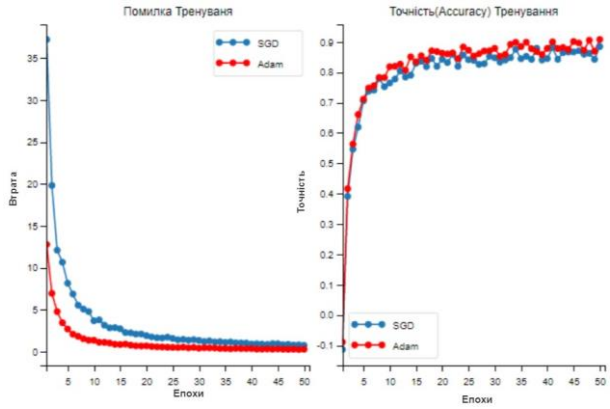

Рисунок 4.7 – Історія навчання НМ з SGD та Adam оптимізаторами

4.2 Тестування системи

Тепер протестуємо дану систему на моєму новому фото (рис. 4.8) з веб камери. Для цього система дає доступ до камери й робить нове фото.

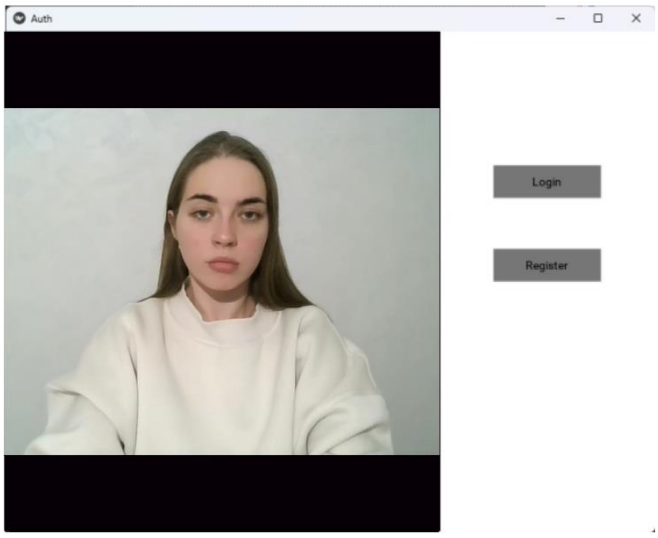

Рисунок 4.8 – Тестове фото з веб камери

Після натискання кнопки Register фото зберігається в БД для подальшої обробки. Тепер ми можемо перевірити чи система нас розпізнає натиснувши кнопку Login. Маємо результат розпізнавання, зображений на рисунках 4.9.

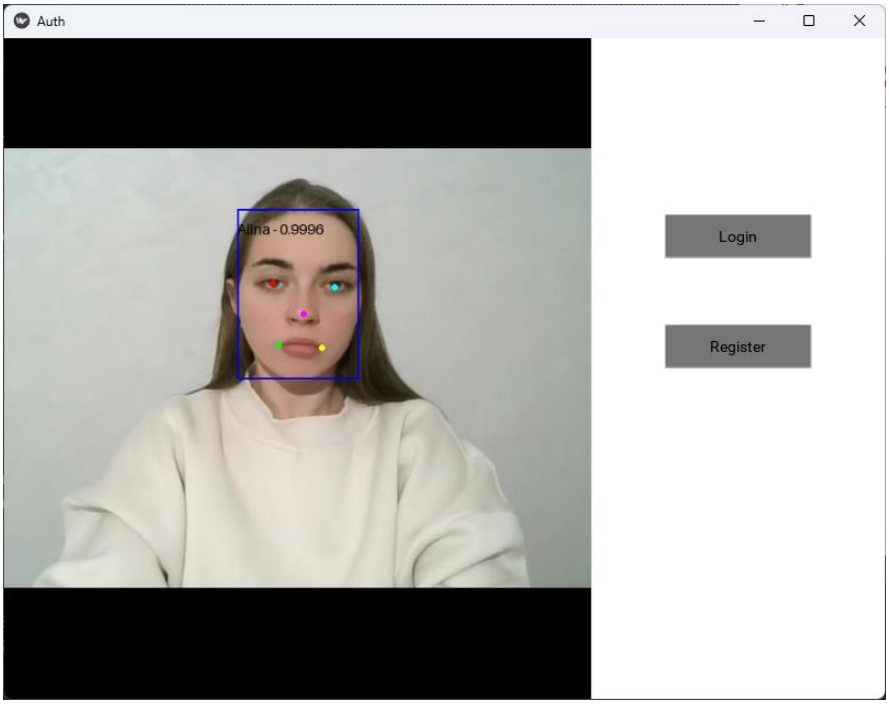

Рисунок 4.9 – Тестове фото з розпізнаванням

Точність розпізнавання тестового зразка 99%.

Висновок до розділу 4

Покращено НМ для більш точного розпізнавання шляхом зміни кількості епох навчання, оптимізатора. Зміна оптимізатора не дає суттєвих покращень навчання. А збільшивши кількість епох, точність зросла з 83% до 87%, тим самим відбулося покращення.

Проведено тестування системи на основі тестового фото з власної веб-камери. З результатів СКУД розпізнала мене на 99% й тим самим правильність надання доступу до об’єкту. Це достатній результат для СКУД й впровадження такої системи.

5 РОЗРОБКА СТАРТАП– ПРОЄКТУ

5.1 Опис ідеї проекту

Таблиця 5.1 – Опис ідеї стартап– проєкту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Створення системи контролю доступу для режимних об'єктів, використовуючи розпізнавання обличчя та розпізнавання за відбитком пальця. Ця технологічна платформа дає можливість швидко та якісно ідентифікувати осіб, що мають доступ, та забезпечить безпеку об'єкта й інформації, що там знаходиться.	1.Використання системи в промисловості та на виробництві	1. Надійність та безпечність на підприємстві 2. Безпека працівників через контроль доступу 3. Швидкість доступу без карток та інших додаткових паролів, які можна загубити чи забути 4. Відстеження робочих змін та робочого часу
	2.Контроль доступу до медичних зон та лікарень	1. Ідентифікація медичного персоналу 2. Захист медичних пристроїв та медикаментів 3. Захист аналізів та конфіденційності
	3. Забезпечення безпеки та контролю доступу в фінансових та освітніх установах, а також у військових об’єктах.	1. Зручність у користуванні, швидкий доступ, захист від вірусів 2. Забезпечення інформацією щодо безпеки в Інтернеті, швидкий доступ онлайн–банкінгу 3. Використання безпечних паролів та уникання кіберзагроз 4. Захист сейфових та дорогоцінних активів

Таблиця 5.2 – Аналіз потенційних техніко-економічних переваг ідеї порівняно із пропозиціями конкурентів передбачає:

№ п/п	Техніко–економічні характеристики ідеї	(потенційні) товари/концепції конкурентів				W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	HID GLOBAL	NEC CORPORATION	ZKTeco			
1.	Вартість	Низька	висока через репутацію та широкий спектр технологій	може варіюватися від великих систем до менших рішень	Середня, залежить від конкретних умов та обсягів			+
2.	Точність та ефективність	Висока	Середня	Висока	Висока		+	
3.	Швидкість розпізнавання	Висока	Висока (залежить від конкретних продуктів)	Висока	Середня		+	
4.	Простота використання	Висока	Середня	Середня	Середня			+
4.	Задоволеність покупців	Середня	Висока	Потребує додаткового дослідження та аналізу відгуків покупців.	Індивідуальні відгуки та задоволеність покупців можуть варіюватися		+	
5.	Рентабельність	Середня	залежить від обсягів та умов	Середня	Середня		+	

Мій проєкт має перевагу у простоті використання та його вартості.

5.2 Технологічний аудит ідеї проекту

В цьому пункті необхідно провести технологічну сторону проєкту.

Таблиця 5.3 – Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1.	Розробка системи розпізнавання за допомогою хмарних технологій	TensorFlow, Keras, Python, Google Colab, Azure Machine Learning, Amazon SageMaker	Так, наявні	Доступні для встановлення та використання на ПК
2.	Розробка системи розпізнавання обличчя як повноцінної програми	PyCharm, VSCode,	Так, наявні	Доступні для всіх користувачів у безкоштовній версії
3.	Система розпізнавання в мобільних додатках	GPUImage, OpenCV, Android SD та jQuery Mobile	Так, наявні	Доступні
Обрана технологія реалізації ідеї проекту: 2				

Висновок: технологічна реалізація проєкту можлива, й дану систему можна розробити за допомогою мови програмування Python та середовища для програмної розробки з розширеннями PyCharm. Ці технології дозволяють створювати різноманітні проекти, від систем безпеки та розпізнавання емоцій до застосувань у сферах освіти, медицини та промисловості. Важливою є також можливість їх інтеграції з іншими технологіями для створення комплексних рішень.

Загалом, технологічна база для втілення ідей щодо розпізнавання обличчя виглядає потужною та досить доступною, що відкриває широкі перспективи для успішної реалізації цих проектів.

5.3 Аналіз ринкових можливостей запуску стартап– проекту

Таблиця 5.4 – Попередня характеристика потенційного ринку стартап–проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	4
2	Загальний обсяг продаж, грн/ум.од	2000000 грн/ ум.од за місяць
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Можливі обмеження у вигляді високих витрат на рекламу, потреба у великому капіталовкладенні та наявність кваліфікованих працівників
5	Специфічні вимоги до стандартизації та сертифікації	Відсутні
6	Середня норма рентабельності в галузі (або по ринку), %	20%

Висновок: Ця характеристика ринку надає загальний огляд ключових показників для стартап– проекту, який використовує технології розпізнавання обличчя. Враховуючи постійну динаміку ринку, є сенс розробити нові системи розпізнавання обличчя на основі нових алгоритмів, які працюють ще швидше та краще, ніж попередні системи.

Таблиця 5.5 – Характеристика потенційних клієнтів стартап– проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1.	Потреба системи контролю доступу та ідентифікації осіб на режимних об’єктах	Корпорації, Урядові установи, Банки, Медичні установи	Можуть мати відмінності у вимогах до рівня безпеки та інтеграції (відрізняються за видом господарської діяльності)	Висока надійність, точність ідентифікації, легка інтеграція, конфіденційність даних.
2.	Потреба автоматизованої системи управління логістикою для малих та середніх підприємств	Малий та середній бізнес у сфері логістики	Менеджери складу, водії, адміністратори мають різні завдання та перспективи	Оптимізація маршрутів, легкість використання, відстеження в реальному часі
3.	Потреба промисловості та виробництва у захисті інформації	Клієнти банків та підприємств виробництва	Відмінність полягає у тому що перше – це підприємство, а друге – сфера обслуговування	Здатність запуску проектів на короткий проміжок часу

Таблиця 5.6 – Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1.	Конкуренція	Збільшення конкурентів в галузі або поява нових конкурентів	Проведення аналізу конкурентів та розробка стратегії позиціонування на ринку
2.	Технологічні загрози	Застарілі технології, які використовує компанія	Постійне вдосконалення та впровадження нових технологічних рішень

Продовження таблиці 5.6 – Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
3.	Наявність працівників підприємств	Для створення системи розпізнавання обличчя потрібні кваліфіковані працівники у цій сфері	Наявність бонусів ,підвищення заробітної плати, забезпечення комфортних умов для працівників
4.	Економічні загрози	Економічна нестабільність та фінансові кризи	Аналіз фінансової стійкості та гнучкості бізнесу. Розробка резервних планів та стратегій управління

Таблиця 5.7 – Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1.	Ринкові можливості	Виявлення нових ринків, де компанія може розширити свою присутність	Розробка стратегії входження на нові ринки. Маркетингові дослідження та аналіз потенційних ринків
2.	Новий продукт	Вихід нового товару збільшує кількість робочих місць та дає змогу отримати більшу можливість варіантів клієнтам для придбання певного продукту	Розробка нового функціонального продукту ,яка стає кращою ніж інші
3.	Партнерські можливості	Укладання стратегічних партнерських угод або співпраця з іншими компаніями	Пошук потенційних партнерів. Розвиток і підтримка

Таблиця 5.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Вказати тип конкуренції – монополія	Один гравець контролює ринок	Забезпечення високої якості продукції та обслуговування для зберігання позицій монополіста
2. За рівнем конкурентної боротьби – національна	Актуальна на рівні всієї країни	Розширення мережі збуту та обслуговування для охоплення всієї країни
3. За галузевою ознакою – міжгалузева	Конкуренція між підприємствами різних галузей	Розширення асортименту продукції для виходу на нові ринки та галузі. Надання послуг та документів інтерфейсу для різних цілей підприємства
4. Конкуренція за видами товарів: – між бажаннями	Боротьба за вибір споживача між різними продуктами	Розширення асортименту та введення нових продуктів . Акцент на брендування.
5. За характером конкурентних переваг – цінова / нецінова	Цінова – змагання за клієнта через найнижчі ціни Нецінова – змагання за клієнта через нецінові фактори	Надання пробного періоду. Розробка гнучкої ціноутворювальної політики, акцій та знижок. Акцент на якості, інноваціях, обслуговуванні для цінностей споживачів
6. За інтенсивністю – марочна	Конкуренція між виробниками конкретних марок	Вдосконалення маркетингових стратегій та позицій на ринку. Забезпечення публічності бренду.

Таблиця 5.9 – Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари–замінники
Складові аналізу	HID GLOBAL, NEC CORPORATION, ZKTeco	Бар’єри входження в ринок включають високі витрати на дослідження та розробку	Пов’язані з високою залежністю від постачальників (конкуренція постачальників)	Логістичний аспект, надійність системи, рівень безпеки, технічна підтримка та вартість рішень	Наявність альтернативних технологій або рішень у сфері ідентифікації, зручність в користуванні
Висновки:	Висока, з урахуванням високих витрат на дослідження і розробку в галузі ідентифікаційних технологій	Вхід на ринок може бути важким через високі бар'єри, але потенційні конкуренти можуть з'явитися, працюючи над новаторськими технологіями. Потенційних клієнтів є багато. Терміни залежать від розробки проєкту	Так, постачальники диктують умови роботи на ринку, самостійно встановлюють ціни на ресурси та рекламу компанії і тд….	Так,клієнти диктують умови роботи на ринку, враховуючи їхні вимоги щодо якості,безпеки та ефективності підтримки системи. Можуть пропонувати оптову ціну , але це не вигідно для власників системи	Обмеження для роботи на ринку через товари замінники можуть включати наявність альтернативних технологій або конкретних продуктів, які задовольняють потреби клієнта. Пропонують кращі тарифи для клієнтів.

Висновок. Ринок ідентифікаційних систем характеризується високим рівнем конкуренції. Клієнти визначають умови роботи на ринку, вимагаючи високу

якість, безпеку та технічну підтримку. Обмеження для роботи на ринку включають високі бар'єри для входу через великі витрати на дослідження і розробку, а також наявність конкурентів та товарів– замінників. Компанії повинні стежити за потребами клієнтів, дотримуватися стандартів безпеки та динамічно реагувати на зміни на ринку щоб забезпечити успіх.

Проаналізувавши дані таблиці маємо те, що вихід на ринок ускладнений через олігархічну структуру ринку. Основні конкуренти постійно вдосконалюють свої продукти, щоб зробити їх кращими за інші. Однак це не означає, що не варто виходити на ринок. На мій погляд, найкраща ідея — розробляти та виводити продукти на ринок за привабливими цінами для користувачів початкового рівня та оптовими цінами для підприємств. Цей вид реклами, хоча і є дещо невигідним для власника системи, допомагає йому залишатися на ринку та конкурувати з аналогічними продуктами.

Таблиця 5.10 – Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1	Точність ідентифікації	Система є ключовим чинником для ефективного контролю доступу .
2	Актуальність технології	Система має сучасні алгоритми, які використовують для певних сучасних підприємств
3.	Вартість впровадження	Важливий фактор, який впливає на економічну вигідність проекту, тому що проекти з меншими витратами можуть мати конкурентну перевагу,привертаючи увагу потенційних клієнтів
4	Швидкість	Цей фактор зручний для клієнта, тому що займає мало часу

Таблиця 5.11 – Порівняльний аналіз сильних та слабких сторін.

№ п/п	Фактор конкурентоспроможності	Бали 1– 20	Рейтинг товарів– конкурентів у порівнянні з … (назва підприємства)						
			–3	–2	–1	0	+1	+2	+3
1	Точність ідентифікації	19						2	
2	Актуальність технології	19		2		1			
3	Вартість впровадження	18					1		
4	Швидкість системи	20				1,2			

Таблиця 5.12 – SWOT- аналіз стартап– проекту

Сильні сторони: 1. Ефективність 2. Швидкість та точність 3. Задоволеність клієнтів 4. Наявність висококваліфікованих фахівців	Слабкі сторони: 1. Фінансові обмеження 2. Відсутність початкових інвестицій 3. Відсутність фотографії реальних людей для тестування :
Можливості: 1. Партнерські угоди 2. Використання нових технологій та маркетингових стратегій 3. Гнучкість та швидка адаптація 4. Розширення функціоналу продукту 5. Інвестиції	Загрози: 1. Зростання конкуренції 2. Відмова від співпраці 3. Крадіжка даних 4. Зростання кіберзагроз 5. Недостатньо коштів на маркетинг

Таблиця 5.13 – Альтернативи ринкового впровадження стартап– проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Тестування на обмеженому ринку	Середня	6– 12 місяців
2	Користування системою на певний проміжок часу	Висока	2 місяці
3	Реклама	Залежить від компанії	3– 5 місяців
4	Стратегічне партнерство	Залежить від успішності переговорів	Від 6 місяців до 2 років

Альтернативним рішенням для виходу на ринок з урахуванням ресурсів і термінів є оголошення про свій продукт на заходах в сфері ІТ.

Отже, "Прискорений вивід на ринок" виглядає оптимальною альтернативою, враховуючи ймовірність отримання ресурсів та стислі строки реалізації.

5.4 Розроблення ринкової стратегії проекту

Таблиця 5.14 – Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачі в сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Великі підприємства	Висока готовність	Значний попит,оскільки компанія шукає інноваційні рішення для ідентифікації та безпеки	Висока	Середня, оскільки необхідно конкурувати з існуючими постачальниками
2	Малі підприємства	Низька готовність	Високий попит	Низька	Висока
3	Середні підприємства	Середня готовність	Високий попит	Низька	Висока
Які цільові групи обрано: 2,3					

З таблиці можна зробити висновок, що найкращим рішенням є орієнтація на малий і середній бізнес, оскільки великі компанії, швидше за все, вже мають власу СКУД. А готовність малих та середніх підприємст до використання нових технологій надає високий попит на інноваційні рішення роблять цю групу

привабливою для введення продукту на ринок. Оскільки мій проєкт є універсальним для будь - якої сфери й є стандартизованою програмою, то оптимальним є використання масового маркетингу.

Таблиця 5.15 – Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку*
1	Прискорений вихід на ринок та забезпечення швидкості	Проведення реклами та задоволення потреб компаній різних галузей	Висока точність ідентифікації, актуальність технології, використання чогось нового та нижча ціна порівняно з конкурентами	Стратегія швидкого впровадження та стратегія диференціації

Таблиця 5.16 – Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
1.	Так, проект має елементи першопрохідця, оскільки пропонує інноваційні ідентифікаційні системи, але є конкуренти на ринку.	Компанія буде шукати як нових споживачів, так і забирати існуючих у конкурентів, зосереджуючись на виведенні на ринок інноваційних рішень та активному маркетингу	Ні, компанія буде ставити акцент на унікальність та вдосконалення існуючих рішень, замість простого копіювання. Основний фокус – висока точність ідентифікації та використання передових технологій.	Компанія прагне вирізнятися від конкурентів шляхом надання унікальних та вдосконалених ідентифікаційних систем. Фокус на інноваціях, високій якості та ефективному маркетингу для створення унікального образу на ринку.

Таблиця 5.17– Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап–проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
1	Вимогами є швидкість і точність роботи системи	Стратегія диференціації	Висока точність, низька обманливість, інтеграція з іншими системами	Простота,конфіденційність даних, мінімальна кількість помилкових пропусків

5.5 Розроблення маркетингової програми стартап– проекту

Таблиця 5.18 – Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Забезпечення високого рівня безпеки	Захист від вторгнення, що забезпечує високий рівень безпеки об’єктів	Використання певних технологій розпізнавання обличчя та відбитків пальця для максимальної точності ідентифікації
2	Швидкість та гнучкість у використанні	Швидке розпізнавання обличчя, легкість інтеграції з іншими системами	Відкритий інтерфейс для інтеграції з різними обладнаннями та програмним забезпеченням . Легкість налаштування під конкретні потреби та мінімальна швидкість розпізнавання обличчя
3	Ефективність	Забезпечення безпеки та конфіденційності важливих даних і матеріалів	Відсутність помилок, відсутність можливості фальшивої ідентифікації завдяки високій надійності та складній системі перевірки

Таблиця 5.19 – Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>I. Товар за задумом</td><td colspan="3">Система контролю допуску та ідентифікації осіб на режимних об’єктах (там розпізнавання обличчя та розпізнавання за відбитком пальця)</td></tr>
<tr><td rowspan="4">II. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх /Тл/Е/Ор</td></tr>
<tr><td>1.Швидкість
2.Модульність та сумісність
3. Універсальність системи</td><td>М
Нм
М</td><td>Тх
Ор
Тх</td></tr>
<tr><td colspan="3">Якість: ISO 27001 для інформаційної безпеки або ISO 9001 для систем управління якістю</td></tr>
<tr><td colspan="3">Пакування: забезпечує захист системи під час транспортування та зберігання. Відповідає вимогам до стійкості від зовнішніх впливів та забезпечує надійну доставку продукту до клієнта.</td></tr>
<tr><td></td><td colspan="3">Марка: SecureGuard IdentityAccess</td></tr>
<tr><td rowspan="2">III. Товар із підкріпленням</td><td colspan="3">До продажу: рекламні заходи, демонстрації системи на виставці , консультації для допомоги клієнтам зрозуміти переваги системи, врахування індивідуальних потреб клієнта , наявність повної документації та кошти на ліцензію</td></tr>
<tr><td colspan="3">Після продажу: забезпечення новими функціями та виправлення помилок для підтримки актуальності, 24/7 технічну підтримку для вирішення питань та вирішення проблем користувачів, гарантійні сервіси, підтримка з боку клієнтів та розробників</td></tr>
<tr><td colspan="4">За рахунок чого потенційний товар буде захищено від копіювання: авторських прав, захист інтелектуальної власності, ліцензії та угоди для використання продукту без дозволу.</td></tr>
</table>

Таблиця 5.20 – Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1	Визначення цін на товари, які можуть виконувати схожі функції або задовольняти схожі потреби споживачів.	Аналіз цін на продукти, що мають аналогічні характеристики та призначення, для встановлення конкурентоспроможної цінової політики.	Урахування економічного статусу та доходів цільової аудиторії для визначення того, як вони сприйматимуть ціну товару.	Верхня межа: Максимальна цінова точка, яку споживачі готові платити за продукт. Нижня межа: Мінімальна цінова точка, що враховує витрати на виробництво та прибуток, який компанія прагне отримати.

Таблиця 5.21 – Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	Вивчення особливостей та уподобань цільової аудиторії щодо процесу закупівлі товарів.	Визначення обов’язків і функцій, які постачальник повинен виконувати в системі збуту, включаючи маркетинг, продажі, обслуговування клієнтів тощо.	Канал одного рівня	Розробка ефективної та оптимальної системи збуту, яка враховує потреби ринку, ефективність та ефективність роботи кожного ланцюга.

Таблиця 5.22 – Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуютьс я цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомленн я	Концепція рекламного звернення
1	Моделі та технології ведення бізнесу	Соц. мережі, електронна пошта, Teams, Zoom	Позиція продукту як універсального інструменту, який може бути успішно використаний у різних сферах, включаючи бізнес, офіси, громадські місця та інші.	Залучення уваги та висвітлення переваг, інтеграція логотипу та назви бренду для підсилення довіри, заохочення до купівлі пробного матеріалу	Проста система,яка доступна для всіх користувачів у швидкому режимі

Висновок до розділу 5.

На основі маркетингового аналізу стартап-проєкту було прийнято рішення про доцільність запуску цього продукту, оскільки ці системи завжди користуються попитом. Деякі великі корпорації інвестують значні кошти в розвиток своїх систем, проте це не є оптимальним варіантом для невеликих та середніх підприємств.

Проаналізувавши існуючий ринок потенційних клієнтів, я виявила, що потенційних клієнтів багато, а саме в малих підприємствах, банках та військових частинах, яким потрібний захист та контроль доступу. Також проведено огляд цінової стратегії системи, й у висновку маю, що ця система привертає їх через свою доступність, але за якістю не поступається продукції великих корпорацій.

Із плином часу, є сенс спробувати вийти на ринок, який належить конкуренту. Однак система повинна постійно вдосконалюватися та оновлюватись у міру появи нових технологій.

Аналіз системи контролю допуску та ідентифікації осіб на режимних об’єктах, зокрема використання розпізнавання обличчя та відбитків пальців, дозволяє зробити важливі висновки:

– Можливість ринкової комерціалізації: Проект має значний потенціал для ринкової комерціалізації, оскільки існує високий попит на вдосконалені системи безпеки та ідентифікації.

– Перспективи впровадження: Є перспективи успішного впровадження, особливо в сферах, де важлива безпека та контроль доступу. Бар'єри входження можуть включати високі технологічні стандарти та питання конфіденційності.

– Альтернативні варіанти впровадження: Доцільним варіантом може бути встановлення партнерств з об'єктами безпеки та іншими відомствами для впровадження продукту.

– Доцільність подальшої імплементації: Подальша імплементація проекту є доцільною, з огляду на стійкий ріст сектору безпеки та постійну потребу в ефективних системах контролю допуску та ідентифікації осіб.

ВИСНОВКИ

Вирішено поставлену задачу, а саме розроблено систему контролю доступу та ідентифікації осіб на режимних об’єктах. Для цього зроблено:

1) Аналіз методів біометричної ідентифікації, й на основі нього обрано методи розпізнавання за обличчям та розпізнавання за відбитком пальця. Вони є швидкі та зручні, а також їх важко підробити, що дуже важливо в системі контролю допуску.

2) Аналіз методів та підходів розпізнавання, на основі якого обрано та реалізовано метод глибокого навчання за допомогою НМ.

3) Аналіз вимог до системи, й на цього визначено ключові аспектів, які важливі при впровадженні системи.

4) Спроєктовано та описано біометричну систему контролю допуску та ідентифікації осіб на режимних об’єктах.

5) На основі аналізу різних програмних засобів зроблений вибір технологій, а саме використано:

– мова програмування Python, оскільки дана мова широко використовується у сфері машинного навчання;

– Colab та PyCharm як програмне середовище для розробки;

– використано бібліотеки TensorFlow, Keras, OpenCV, NumPy та пакет Matplotlib для навчання штучного інтелекту, а також для використання алгоритмів комп'ютерного зору й візуалізації даних.

6) Розроблено НМ для розпізнавання обличчя та відбитків пальців, що базуються на архітектурі згорткових нейронних мереж. НМ на архітектурі RetinaFace показала кращі результат точності (99%) розпізнавання обличчя, ніж НМ з архітектурою VGG16 (87%). НМ розпізнавання відбитків показала точність 90% та 98%, що є гарним результатом.

7) Проведено тестування системи на основі мого фото з власної веб-камери. В результаті отримали точність розпізнавання %. Поріг проходження встановлено як 80%, тому система ефективно розпізнала мене як “Відповідає еталонним

даним” й надає мені доступ. А сторонніх людей, яких немає в БД розпізнає як “Немає збігу” й через це доступ до об’єкту не надано.

8) Розроблено маркетинговий аналіз стартап-проєкту, на основі якого прийнято рішення про доцільність запуску цього продукту. На основі аналізу ринку потенційних клієнтів, виявлено, що потенційних клієнтів багато, а саме в малі підприємства, банки та військові частини. Також проведено огляд цінової стратегії системи, й у висновку маю, що ця система привертає їх через свою доступність, але за якістю не поступається продукції великих корпорацій. Проект має значний потенціал для ринкової комерціалізації, оскільки існує високий попит на вдосконалені системи безпеки та ідентифікації.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кафедра Інформаційних Систем та Технологій. URL: https://ist.kpi.ua/ (дата звернення: 24.11.2023).

2. Дорошенко А. Ю., Савчук О. В. Наукова робота за темою магістерської дисертації : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2023. 286 с. URL: https://ela.kpi.ua/handle/123456789/57340

3. ДСТУ 3582:2013 https://lib.zsmu.edu.ua/upload/intext/dstu_3582_2013.pdf

4. СКУД: https://deps.ua/ua/knowegable– base/reference– information/7824.html#q1

5. СКУД: https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BA%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8E_%D1%96_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC

6. Ідентифікація: https://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0)

7. Автентифікація: https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F

8. Авторизація: https://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F

9. Класифікація систем контролю доступу:

https://idcard.com.ua/ua/blog/chto– takoe– skud– i– kak– eto– rabotaet/, https://ssbb.ua/sistemy– kontrolya– dostupa/sistema– kontrolyu– dostupu/klassifikaciya– skud/ , https://us– plast.ru/info/klassifikatsiya– skud/

10. Принцип роботи СКУД: https://zakarpattya.net.ua/News/200909-Systemy-kontroliu-dostupu-shcho-tse-take-i-iak-pratsiuie#:~:text=%D0%9F%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D0%B8%20%D0%A1%D0%9A%D0%A3%D0%94%20%D0%BD%D0%B0%D1%81%D1%82%D1%83%D0%BF%D0%B

11. http://solis.in.ua/klasyfikatsiya-system-kontrolyu-dostupu.html

12. БІОМЕТРИЧНІ ТЕХНОЛОГІЇ Навчальний посібник Царьов Р. Ю., Лемеха Т. М.

13. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних Ц18 закладів] / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.: іл. https://core.ac.uk/download/pdf/47227947.pdf

14. Сучасні методи біометричної ідентифікації: https://ela.kpi.ua/bitstream/123456789/9839/1/26.pdf

15. Програмне забезпечення для розпізнавання облич: https://www.spiceworks.com/it-security/identity-access-management/articles/facial-recognition-software/

16. Форми біометричної аутентифікації: https://worldvision.com.ua/articles/formi– biometricheskoy– autentifikatsii

17. Переваги й недоліки біометричного захисту: https://worldvision.com.ua/preimushchestva-i-nedostatki-biometricheskoy-sistemy-autentifikatsii/

18. Методи розпізнавання осіб: https://habr.com/ru/companies/synesis/articles/238129/

19. Python: https://freehost.com.ua/ukr/faq/wiki/chto-takoe-jazik-programmirovanija-python/

20. Найкращі AI з відкритим вихідним кодом: https://ts2.pl/uk/%D0%BD%D0%B0%D0%B2%D1%96%D0%B3%D0%B0%D1%86%D1%96%D1%8F-%D0%B2-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%96-%D0%BC%D0%B0%D1%88%D0%B8%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE-%D0%BD%D0%B0%D0%B2%D1%87%D0%B0%D0%BD/#gsc.tab=0

21. https://paperswithcode.com/dataset/fddb

22. Настільний USB сканер відбитків пальців SLK20R https://zktecoua.com/ua/products/scanner-zkteco-slk20r/