МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ПЕТРЕНЧУК Антон Вікторович

Захищена система аутентифікацій на основі біометричних данних / Secure Biometric Authentication System

спеціальність: 125 - Кібербезпека та захист інформації

освітньо-професійна програма - Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
А. В. Петренчук

Науковий керівник
д. філософії, С. В. Кулина

Кваліфікаційну роботу
Допущено до захисту:

«____» _____ ___2025 р.

Завідувач кафедри
_____ **В. В. Яцків**

ТЕРНОПІЛЬ - 2025

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 - Кібербезпека та захист інформації
освітньо-професійна програма - Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В. В. Яцків
«____» _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ПЕТРЕНЧУК Антон Вікторович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Захищена система аутентифікацій на основі біометричних данних / Secure Biometric Authentication System
керівник роботи д. філософії С. В. Кулина
затверджені наказом по університету від 20 грудня 2024 року № 938.

2. Строк подання студентом закінченої кваліфікаційної роботи 5 грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити:
– дослідити існуючі алгоритми біометричної аутентифікації та їх вразливості до спуфінгу;
– визначити вимоги до автономної архітектури системи з локальним зберіганням даних;
– розробити дворівневий механізм аутентифікації (обличчя + пароль) та механізми захисту від несанкціонованого видалення;
– синтезувати та інтегрувати алгоритм виявлення обману (Liveness Detection) для захисту від спуфінг-атак;
– створити та протестувати програмний прототип системи у середовищі, що імітує реальні умови експлуатації.

5. Перелік графічного матеріалу у роботі:
– архітектура захищеної біометричної системи;
– схема дворівневого механізму аутентифікації;
– схема алгоритму розпізнавання обличчя;
– схема роботи алгоритму виявлення обману (Liveness Detection);
– графік оцінки продуктивності системи та точності розпізнавання.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 20 грудня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Теоритичні основи біометричної аутентифікації	12.2024 р. - 03.2025 р.	
2	Аналіз сучасних біометричних систем аутентифікації	03.2025 р. - 06.2025 р.	
3	Розробка захищеного модуля біометричної аутентифікації	06.2025 р. - 11.2025 р.	

Студент _____ Петренчук А. В.
підпис

Керівник роботи _____ д. філософії, Кулина С. В.
підпис

АНОТАЦІЯ

Петренчук А. В. Захищена система аутентифікацій на основі біометричних данних. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека та захист інформації», освітньо-професійна програма «Кібербезпека». – Західноукраїнський національний університет, Тернопіль, 2025.

У роботі експериментально досліджено методи та алгоритми побудови захищеної системи аутентифікації, що поєднує біометричне розпізнавання обличчя та парольний захист, забезпечуючи конфіденційність даних та стійкість до атак обману (спуфінгу).

Ключові слова: АУТЕНТИФІКАЦІЯ, БІОМЕТРИЧНІ ДАНІ, РОЗПІЗНАВАННЯ ОБЛИЧЧЯ, СПУФІНГ, КІБЕРБЕЗПЕКА.

ABSTRACT

Petrenchuk A. V. Secure Biometric Authentication System. – Manuscript.

Doctoral studies for the education level «Master» with the title 125 «Cybersecurity and Information Protection». – West Ukrainian National University, Ternopil, 2025.

The thesis experimentally investigates methods and algorithms for building a secure authentication system that combines biometric face recognition and password protection, ensuring data confidentiality and resistance to spoofing attacks.

Keywords: AUTHENTICATION, BIOMETRIC DATA, FACE RECOGNITION, SPOOFING, CYBERSECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

FRR - False Rejection Rate, рівень хибних відмов.

EER - Equal Error Rate, точка рівних помилок.

SVM - Support Vector Machine, машина опорних векторів.

CNN - Convolutional Neural Network, згорткова нейронна мережа.

SSI - Server Side Includes, включення на стороні сервера.

RGB - Red, Green, Blue, червоний, зелений, синій.

FRVT - Face Recognition Vendor Test, тест постачальників технологій розпізнавання облич.

NIST - National Institute of Standards and Technology, Національний інститут стандартів і технологій США.

EDPB - European Data Protection Board, Європейська рада з питань захисту даних.

EDPS - European Data Protection Supervisor, Європейський наглядач із захисту даних.

MFCC - Mel-Frequency Cepstral Coefficients, кепстральні коефіцієнти мел-частот.

BGR - Blue, Green, Red, синій, зелений, червоний.

ISO - International Organization for Standardization, Міжнародна організація зі стандартизації.

IEC - International Electrotechnical Commission, Міжнародна електротехнічна комісія

GUI - Graphical User Interface, графічний інтерфейс користувача.

TAR - True Accept Rate, справжній коефіцієнт прийняття.

ANSI - American National Standards Institute, Американський національний інститут стандартів.

ВСТУП

Актуальність роботи. В умовах стрімкої цифровізації суспільства та інтеграції кіберфізичних систем, питання забезпечення надійного та зручного доступу до інформаційних ресурсів набуває критичного значення. Традиційні методи аутентифікації, засновані лише на паролях, виявилися недостатньо стійкими до сучасних кіберзагроз, таких як фішинг, підбір паролів та компрометація баз даних. Це зумовлює необхідність переходу до більш захищених та біологічно унікальних ідентифікаторів.

Біометричні системи, зокрема аутентифікація за розпізнаванням обличчя, пропонують високий рівень безпеки та зручності. Однак їх широке впровадження стримується двома основними викликами. Перший пов’язаний із захистом конфіденційності, адже біометричні шаблони є невідновлюваними даними, і їх компрометація створює для користувача незворотні ризики. Другий стосується стійкості до атак обману (спуфінгу), оскільки біометричні сенсори можуть бути введені в оману за допомогою фотографій, відеозаписів чи масок, що фактично нівелює переваги біометричної автентифікації.

Кваліфікаційна робота зосереджена на розробці захищеної системи, яка інтегрує багатофакторну аутентифікацію (пароль + обличчя) із надійним механізмом виявлення обману. Вирішення цих завдань є вкрай актуальним для спеціальності «Кібербезпека та захист інформації», оскільки дозволяє створити високонадійний захист від несанкціонованого доступу.

Мета та завдання дослідження. Метою роботи є розробка та експериментальне дослідження високонадійної системи аутентифікації на основі біометричних даних, що поєднує багатофакторний захист, високу точність розпізнавання та ефективну стійкість до спуфінг-атак.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

- дослідити існуючі алгоритми біометричної аутентифікації та їх вразливості до спуфінгу.
- визначити вимоги до автономної архітектури системи з локальним зберіганням біометричних шаблонів.

- розробити дворівневий механізм аутентифікації (обличчя + пароль) та механізми захисту від несанкціонованого видалення даних.
- синтезувати та інтегрувати алгоритм виявлення обману для захисту від спуфінг-атак.
- створити та протестувати програмний прототип системи у середовищі, що імітує реальні умови експлуатації.

Об’єкт дослідження - процеси ідентифікації та аутентифікації користувачів у сучасних інформаційних системах.

Предмет дослідження - алгоритми, методи та механізми побудови захищених систем аутентифікації на основі біометричних даних.

Методи досліджень. У роботі використано: теоретичний аналіз, алгоритмічний синтез, методи комп’ютерного зору та машинного навчання, експериментальні методи.

Наукова новизна та практичне значення. Наукова новизна одержаних результатів полягає у розробці та програмній реалізації системи аутентифікації, що поєднує двофакторну схему верифікації (біометрія обличчя + пароль) з оригінальним механізмом виявлення обману, заснованим на аналізі чіткості обличчя. Цей підхід забезпечує стійкість системи до відомих атак обману при збереженні високої конфіденційності даних завдяки локальному зберіганню.

Практичне значення. Розроблена система демонструє високу надійність і може стати основою для впровадження рішень у системах контролю фізичного доступу на захищених об'єктах, системах обліку робочого часу, захищених терміналах та робочих станціях, що працюють в автономних мережах.

Результати дослідження. За підсумками роботи розроблено програмний прототип системи, який успішно реалізує двофакторну аутентифікацію та локальне зберігання біометричних шаблонів. Впроваджений метод виявлення обману (перевірка чіткості) ефективно запобігає спробам доступу за допомогою фотографій. Система також включає журнал подій для аудиту та механізм захисту від небажаного видалення облікових записів. Експериментальне

тестування підтвердило стабільність, зручність та готовність системи до практичного застосування.

Публікації та апробація КР.

1. Петренчук, А., Дзівак О. Системи аутентифікацій на основі біометричних данних. Захист інформації: Збірник матеріалів науково-практичного симпозіуму, 30.11.2024. – Тернопіль, 2024. – С. 25–27.

2. Петренчук, А., Кулина С. Системи аутентифікації на основі біометричних даних. Інформаційно-комп’ютерні технології: Матеріали XV Міжнар. наук.-техн. конф., 28–29 березня 2025. – Житомир, 2025. – С. 141–142.

1. ТЕОРЕТИЧНІ ОСНОВИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

1.1. Основи аутентифікації та біометричних технологій

Аутентифікація є однією з найважливіших складових систем інформаційної безпеки, що забезпечує контроль доступу до ресурсів, захист конфіденційних даних і запобігання несанкціонованому використанню облікових записів. В епоху цифровізації та глобальної інтеграції інформаційних технологій питання перевірки автентичності користувача стає центральним у побудові безпечного інформаційного середовища [1].

Під терміном аутентифікація розуміють процес перевірки достовірності заявленої особи або об’єкта, який намагається отримати доступ до певної системи чи ресурсу. Тобто це процес підтвердження того, що користувач є саме тією особою, за яку себе видає. У найпростішій формі аутентифікація може здійснюватися за паролем, кодом, або іншим секретом, відомим лише власнику облікового запису. Проте такі методи мають низку недоліків, а саме паролі які можна забути, вкрасти, підібрати або передати іншій особі [2].

Щоб усунути ці вразливості, почали активно впроваджуватись біометричні технології, як базуються на унікальних фізичних і поведінкових характеристиках людини. Біометрична аутентифікація не потребує запам’ятовування паролів або носіння фізичних токенів - вона ґрунтується на самій природі користувача, на його обличчі, голосі, відбитках пальців, манері ходьби, динаміці набору тексту та інших ознаках, які складно підробити або передати [3].

Згідно з сучасними науковими дослідженнями, зокрема роботою Ryu та інші [4], опублікованою в журналі IEEE Access, становлення біометричних систем стало ключовим етапом у розвитку безпечних технологій ідентифікації. Біометрія дозволила суттєво знизити кількість атак, пов’язаних із крадіжкою облікових даних, водночас зробивши процес входу в систему більш зручним і прозорим для користувачів.

Історично склалося три основні принципи традиційної аутентифікації або як їх ще називають підходи до аутентифікації, що базуються на різних типах доказів особи:

1. На основі знань - “щось, що користувач знає”. Це може бути пароль, PIN-код, відповідь на секретне запитання. Основна перевага методу - простота реалізації. Проте слабкі паролі, фішинг, соціальна інженерія та зловмисники, які можуть отримати доступ до бази даних, роблять цей підхід вразливим.

2. На основі володіння - “щось, що користувач має”. Прикладами є банківські картки, токени доступу, ключі, смартфони з кодами доступу. Недолік - можливість втрати або крадіжки пристрою, що робить користувача вразливим до компрометації.

3. На основі біометрії - “щось, чим користувач є”. Унікальні характеристики тіла або поведінки забезпечують найвищий рівень достовірності. Біометричні дані практично неможливо підробити, вони залишаються стабільними впродовж тривалого часу і дозволяють здійснювати автентифікацію навіть у фоновому режимі (без активних дій користувача).

Сутність біометричної аутентифікації ґрунтується на аналізі фізіологічних та поведінкових характеристик людини [5]. Фізіологічні ознаки включають відбитки пальців, структуру райдужної оболонки, риси обличчя, форму долоні, голос, геометрію вух тощо. Поведінкові - це манера ходьби, почерк, ритм набору тексту, динаміка рухів миші та інші патерни, які виявляють індивідуальність.

На відміну від звичайної одноразової перевірки, сучасні системи можуть проводити безперервну аутентифікацію. Вона дає змогу постійно перевіряти, чи користувач, який працює із системою, залишається тим самим, а не був підмінений. Цей підхід особливо ефективний для мобільних пристроїв і корпоративних систем із високими вимогами до безпеки.

Біометричні системи поєднують точність наукового аналізу фізичних характеристик із зручністю користування [6]. Їхня основна перевага - унікальність і складність фальсифікації, що робить їх ефективними в системах високого рівня безпеки - від банківських додатків до державних реєстрів. Кожна

біометрична система, незалежно від типу використовуваних характеристик, включає п’ять базових етапів роботи які зображені на рисунку 1.1.

Рисунок 1.1 - Етапи роботи біометричної системи

1. Збір біометричних даних. Здійснюється за допомогою сенсорів або камер. Наприклад, сканер відбитків пальців, камера смартфона, мікрофон тощо.

2. Попередня обробка. Система усуває шуми, нормалізує зображення чи сигнал, виділяє зони інтересу. Для цього використовуються алгоритми фільтрації, згладжування, контрастного підсилення.

3. Виділення ознак. Відбувається перетворення біометричних даних у цифровий вектор ознак - набір числових характеристик, що описують унікальні

риси користувача. Наприклад, для зображення обличчя можуть використовуватись точки симетрії, відстані між очима, форма підборіддя тощо.

4. Порівняння ознак. Отримані дані зіставляються з еталонним шаблоном у базі. Для цього застосовуються математичні метрики подібності або алгоритми машинного навчання.

5. Прийняття рішення. Якщо ступінь схожості перевищує певний поріг, користувач вважається автентичним. У протилежному випадку доступ забороняється.

1.2. Типи біометричних характеристик та їх застосування

Біометричні характеристики поділяються на кілька основних груп залежно від природи походження та способу вимірювання. Головним чином вони класифікуються на фізіологічні, поведінкові та допоміжні характеристики. Кожен із цих типів має власні переваги, недоліки, а також різний рівень надійності, точності й зручності використання [7].

Фізіологічні біометричні характеристики пов’язані з анатомічними властивостями людини, які залишаються стабільними протягом усього життя.

До фізіологічних характеристик належать:

1. Відбитки пальців. Один із найстаріших і найпоширеніших методів ідентифікації. Кожна людина має унікальний малюнок папілярних ліній, який практично неможливо підробити. Технологія використовується в смартфонах, банківських системах, державних базах даних.

2. Райдужна оболонка ока. Цей метод забезпечує надзвичайно високу точність, адже структура райдужки унікальна навіть для близнюків. Використовується в аеропортах, урядових установах і в високозахищених об’єктах.

3. Обличчя. Один із найзручніших методів, адже користувачеві не потрібно нічого робити, крім як подивитися в камеру. Сучасні алгоритми можуть ідентифікувати особу навіть у русі або при зміні освітлення.

4. Геометрія долоні та пальців. Вимірюються пропорції та відстані між пальцями, форма долоні. Метод зручний, але поступається точністю іншим фізіологічним характеристикам.

5. Голосові характеристики. Кожна людина має індивідуальний тембр, частотний спектр і манеру мовлення. Хоча цей метод менш стабільний (через хвороби чи шумове середовище), він широко використовується у віртуальних асистентах і системах дистанційної ідентифікації.

6. Структура вен. Сканування розташування вен на долоні або пальці, яке відбувається за допомогою інфрачервоного випромінювання. Цей метод майже неможливо підробити, але потребує дорогого обладнання.

Фізіологічні ознаки мають спільну перевагу - вони сталі у часі й майже не змінюються протягом життя. Це робить їх ідеальними для точних систем ідентифікації. Проте їхнім недоліком є висока вартість сенсорів і ризики компрометації . Якщо зловмисник отримає біометричний шаблон (наприклад, зображення відбитка пальця), його неможливо “змінити”, як пароль [8], що і представлено в таблиці 1.1.

Таблиця 1.1

Фізіологічні біометричні характеристики

№	Біометрична характеристика	Опис	Переваги	Недоліки	Застосування
1	Відбитки пальців	Унікальний малюнок папілярних ліній	Висока точність, складно підробити	Вартість сенсорів, ризик компрометації	Смартфони, банківські системи, держбази
2	Райдужна оболонка ока	Унікальна структура райдужки	Надзвичайна точність, навіть у близнюків	Дороге обладнання	Аеропорти, урядові установи, захищені об’єкти
3	Обличчя	Аналіз рис обличчя	Зручно для користувача, можна ідентифікувати в русі	Може помилятися при зміні освітлення	Смартфони, системи безпеки

Прод. табл. 1.1

4	Геометрія долоні та пальців	Вимірювання пропорцій пальців і долоні	Простий метод	Менш точний, ніж інші фізіологічні методи	Системи контролю доступу
5	Голосові характеристики	Тембр, частотний спектр, манера мовлення	Можливість дистанційної ідентифікації	Менш стабільний, чутливий до шуму і хвороб	Віртуальні асистенти, телефонна ідентифікація
6	Судинний малюнок	Сканування вен на долоні або пальці	Важко підробити	Дороге обладнання	Високозахищені системи доступу

Поведінкові біометричні характеристики відображають індивідуальні особливості руху, дій або звичок користувача. На відміну від фізіологічних, вони не є абсолютно сталими, але забезпечують можливість безперервної і непомітної для користувача аутентифікації. Переваги, недоліки та застосування поведінкових біометричних характеристик описані в таблиці 1.2.

Таблиця 1.2

Поведінкові біометричні характеристики

№	Характеристика	Опис	Переваги	Недоліки	Застосування
1	Динаміка набору тексту	Ритм натискання клавіш, паузи, сила натискання	Можливість перевірки особи без додаткових пристроїв	Може змінюватися під впливом настрою або втоми	Системи контролю доступу, онлайн-аутентифікація
2	Манера ходьби	Аналіз пересування людини (швидкість, нахил, ритм)	Непомітна ідентифікація	Залежить від стану здоров'я, поверхні тощо	Відеоспостереження, смартфони
3	Почерк і підпис	Натиск, швидкість і напрямок руху пера	Довга історія використання, зручний для документів	Може змінюватися під час стресу	Фінансові та правові документи
4	Поведінка при використанні пристрою	Патерни тримання телефону, специфічні жести	Непомітна ідентифікація	Змінюється залежно від настрою або пристрою	Смартфони, персоналізовані системи

Як зрозуміло з таблиці 1.2 виділяють наступні найпоширеніших поведінкових характеристики:

1. Динаміка набору тексту. Вимірюється ритм натискання клавіш, паузи між ними, сила натискання. Кожна людина друкує унікально, і це можна використати для перевірки особи навіть без додаткових пристроїв.

2. Манера ходьби. За допомогою камер або сенсорів смартфона аналізується спосіб пересування людини. Алгоритм може відрізнити користувача за швидкістю кроку, нахилом тіла чи ритмом руху.

3. Почерк і підпис. Використовується для ідентифікації у фінансових і правових документах. Цей метод має давню історію, але сьогодні реалізується цифровими сенсорами, що вимірюють натиск, швидкість і напрямок руху пера.

4. Поведінка при використанні пристрою. Наприклад, користувач може тримати телефон під певним кутом або виконувати жести специфічним чином. Ці патерни використовуються для непомітної ідентифікації у смартфонах.

Головна перевага поведінкових характеристик - зручність і непомітність, коли користувач не відчуває жодних додаткових дій. Проте мінус полягає в тому, що поведінкові ознаки можуть змінюватися під впливом настрою, стану здоров’я чи зовнішніх факторів (стрес, втома, шум).

Окрім фізіологічних та поведінкових, у сучасній біометрії виділяють ще допоміжні біометричні характеристики, які не є унікальними, але підвищують точність системи, коли поєднуються з іншими даними. Сюди належать стать, колір шкіри, зріст, вік, колір очей, наявність шрамів, татуювань, окулярів тощо. Такі ознаки допомагають у мультимодальних системах, коли кілька параметрів комбінуються для зменшення похибок.

Біометричні системи можна поділити за кількістю використовуваних характеристик на:

1. Унімодальні - використовують лише одну характеристику (наприклад, тільки відбиток пальця). Вони прості у реалізації, але схильні до помилок через шум або спроби підробки.

2. Мультимодальні - поєднують кілька незалежних характеристик, наприклад, обличчя + голос або відбиток + динаміка набору тексту. Вони мають кращу точність, стійкість до збоїв і вищу безпеку.

У систематичних оглядах показано, що мультимодальні системи мають значно нижчі показники помилкового прийняття та помилкового відхилення порівняно з унімодальними. Це пов’язано з тим, що поєднання кількох джерел даних дає змогу компенсувати недоліки кожного окремого методу.

Сьогодні біометричні технології застосовуються практично у всіх сферах суспільства. У банківській і фінансовій сфері біометричні технології використовуються для підвищення безпеки, швидкості обслуговування та зручності клієнтів. Користувачі можуть входити до систем онлайн-банкінгу, підтверджувати транзакції або відкривати рахунки за допомогою розпізнавання обличчя чи відбитка пальця, що значно знижує ризик шахрайства. У деяких країнах, зокрема в Іспанії та Японії, банки вже впровадили банкомати, які ідентифікують особу за біометричними ознаками без використання картки чи PIN-коду. Крім того, поведінкова біометрія дозволяє розпізнавати підозрілі дії користувача, аналізуючи його рухи, швидкість набору тексту або стиль користування пристроєм, що допомагає запобігати крадіжці особистих даних [9].

У сфері державного управління біометрія стала ключовим інструментом цифрової ідентифікації громадян. Електронні паспорти та ID-картки містять чіп із біометричними даними, такими як відбитки пальців або фото високої точності, що унеможливлює підробку документів. Під час перетину кордону системи автоматичного контролю зчитують обличчя або відбитки, прискорюючи перевірку особи та підвищуючи безпеку. У багатьох країнах також впроваджуються виборчі системи з біометричною перевіркою особи, що запобігає фальсифікаціям і забезпечує прозорість виборів. Такі технології допомагають створювати національні бази ідентифікації, як, наприклад, система Aadhaar в Індії, де кожен громадянин має унікальний біометричний запис.

У медичній сфері біометричні системи забезпечують точну ідентифікацію пацієнтів і захищають конфіденційні дані. Медичні працівники можуть отримувати доступ до електронних карток пацієнтів за допомогою розпізнавання

обличчя або відбитка пальця, що знижує ризик помилок у лікуванні. Біометрія також використовується для контролю доступу до медичних баз даних, лабораторій і приміщень із підвищеним рівнем безпеки. У деяких клініках запроваджено систему ідентифікації за відбитками або райдужкою ока, яка гарантує, що медична інформація потрапить лише до уповноважених осіб.

Біометричні технології активно впроваджуються і в освітніх установах. Вони використовуються для контролю відвідуваності, ідентифікації студентів під час віддаленого навчання або складання онлайн-іспитів, що дозволяє уникати шахрайства. У деяких університетах системи розпізнавання обличчя допомагають автоматично фіксувати присутність студентів на заняттях, а також надавати доступ до навчальних ресурсів. Це робить навчальний процес прозорішим і спрощує адміністрування закладів освіти [10].

У повсякденному житті біометрія стала невід'ємною частиною сучасних технологій. Вона використовується у смартфонах для розблокування пристроїв, авторизації покупок і входу до застосунків. У системах «розумного дому» біометричні дані дозволяють персоналізувати налаштування або забезпечувати доступ лише для членів родини. Біометрія також активно застосовується в роздрібній торгівлі, де розпізнавання обличчя допомагає визначати постійних клієнтів і створювати персоналізовані пропозиції. Таким чином, комерційні компанії використовують ці технології не лише для безпеки, а й для підвищення рівня комфорту споживачів.

1.3. Основні принципи біометричних систем і вимоги до них

Біометричні системи - це складні багаторівневі комплекси, що поєднують сенсорні пристрої, математичні алгоритми, бази даних і засоби прийняття рішень. Їх головна мета - надійно підтвердити особу користувача на основі його біологічних або поведінкових характеристик.

Фундамент будь-якої біометричної системи складають кілька ключових принципів: унікальність, стабільність, універсальність, вимірюваність, надійність та захищеність. Ці принципи визначають якість і ефективність

аутентифікації, а також можливість інтеграції таких систем у реальні прикладні середовища [11]. Основні принципи побудови біометричних систем представлено на рисунку 1.2.

Рисунок 1.2 - Основні принципи побудови біометричних систем

Дивлячись на рисунок 1.2 кожна біометрична ознака повинна бути унікальною для конкретної особи. Наприклад, навіть у однояйцевих близнюків структура райдужної оболонки або відбитки пальців відрізняються. Чим вища унікальність, тим менша ймовірність помилкової ідентифікації. Кожен користувач повинен володіти певною біометричною характеристикою. Наприклад, відбитки пальців мають усі люди, але не кожен має придатні для сканування райдужні оболонки або голосовий зразок (через хвороби голосових зв’язок тощо). Ознака має залишатися відносно незмінною впродовж часу. Наприклад, відбитки пальців стабільні протягом життя, тоді як голос чи почерк

можуть змінюватися з віком або через емоційний стан. Біометрична характеристика повинна бути придатною для вимірювання за допомогою технічних засобів. Наприклад, для розпізнавання обличчя необхідна камера з певною роздільною здатністю, а для сканування вен - інфрачервоний сенсор. Система має стабільно працювати незалежно від умов середовища, освітлення, положення користувача тощо.

Високонадійні системи здатні до самоадаптації й корекції похибок під час роботи. Біометричні дані повинні бути захищені від несанкціонованого доступу, копіювання чи підробки. Зберігання сирих біометричних даних (наприклад, фотографій обличчя чи райдужки) не допускається - замість цього створюються зашифровані шаблони. Успіх біометричної системи визначається не лише технічними показниками, а й готовністю людей її використовувати. Якщо процес аутентифікації надто складний або незручний, користувачі шукатимуть способи його обійти [12].

Біометричні системи зазвичай складаються з таких основних модулів:

1. Модуль збору даних. Першим етапом роботи біометричної системи є збір біометричних даних за допомогою спеціальних сенсорів або пристроїв. Це можуть бути камери, що фіксують обличчя або райдужку ока, сканери відбитків пальців, мікрофони для запису голосу чи навіть сенсори, які зчитують малюнок вен. Якість і точність цього етапу мають вирішальне значення, адже від правильності збору даних залежить ефективність усієї системи. Наприклад, недостатнє освітлення або шумове середовище можуть ускладнити ідентифікацію.

2. Модуль попередньої обробки. Після збору даних система переходить до етапу попередньої обробки. Тут інформація очищається від перешкод, нормалізується та готується до аналізу. Наприклад, програма може покращити контрастність зображення обличчя, видалити фонові шуми з аудіозапису або вирівняти положення пальця на сканері. Метою цього етапу є отримання максимально якісного біометричного зразка, придатного для подальшої обробки.

3. Модуль виділення ознак. На цьому етапі система перетворює зібрані дані у набір цифрових характеристик - так званий вектор ознак. Для кожного типу

біометрії характеристики різняться, оскільки у відбитках пальців враховують мінутії (лінії, вигини, розгалуження), у зображенні обличчя вимірюють відстані між ключовими точками (очі, ніс, рот), а у голосі аналізують спектральні параметри звучання. Цей вектор є своєрідним «біометричним відбитком» людини, який система зберігає або використовує для порівняння.

4. Модуль зіставлення. Отриманий вектор ознак порівнюється з уже наявними шаблонами у базі даних. Цей процес відбувається за допомогою алгоритмів порівняння, які визначають ступінь схожості між поточними даними та збереженими зразками. Якщо рівень збігу перевищує встановлений поріг, система вважає, що особу успішно ідентифіковано або автентифіковано. В іншому випадку доступ не надається.

5. Модуль прийняття рішення. Після етапу зіставлення система ухвалює остаточне рішення - дозволити або заборонити доступ. Це може бути як автоматичне рішення системи, так і комбіноване (наприклад, коли результат перевіряє оператор). Важливо, щоб система враховувала можливі похибки - хибні спрацювання чи відмови, та мала гнучкий механізм налаштування порогів точності.

6. Модуль керування безпекою. Останній, але надзвичайно важливий етап - це забезпечення конфіденційності та захисту біометричних даних. У цьому модулі здійснюється шифрування шаблонів, контроль доступу до бази даних, моніторинг несанкціонованих спроб входу та ведення журналів подій. Оскільки біометричні дані неможливо змінити, як пароль, система безпеки повинна гарантувати, що вони не будуть викрадені або підроблені. Саме цей модуль відповідає за довіру до всієї біометричної системи.

Структура системи біометричної аутентифікації включає в себе наступні модулі: модуль збору даних, модуль попередньої обробки, модуль виділення ознак, модуль зіставлення, модуль прийняття рішення та модуль керування безпекою (рис. 1.3) [13].

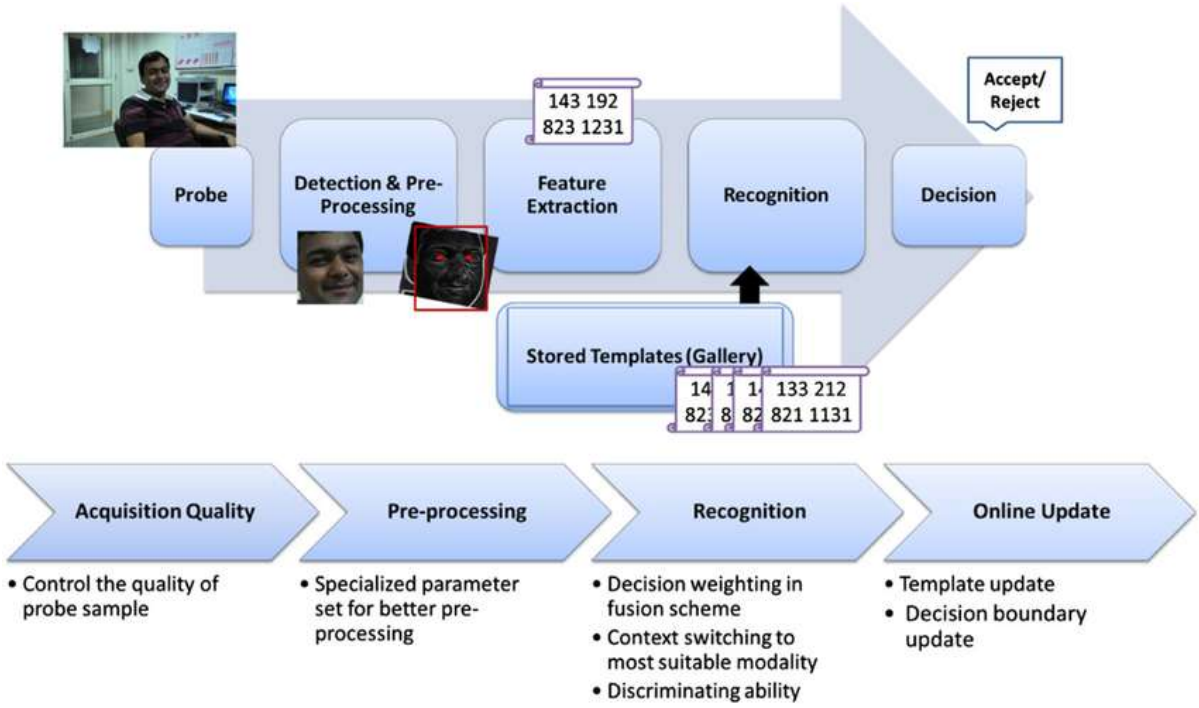


Рисунок 1.3 - Основні модулі біометричної системи

Кожен модуль є критичним для загальної точності системи. Помилка навіть на одному етапі може призвести до хибного результату.

Для оцінки ефективності біометричних систем використовують кількісні показники:

1. Коефіцієнт помилкових прийомів (FAR) - ймовірність того, що система помилково прийме неавторизованого користувача як справжнього.

2. Коефіцієнт помилкових відхилень (FRR) - ймовірність того, що система відхилить справжнього користувача.

3. Рівний рівень помилок (EER) - точка, у якій FAR і FRR рівні. Чим нижчий EER, тим краща точність системи.

4. Робоча характеристика приймача (ROC) - графік, що показує залежність FAR і FRR для оцінки загальної продуктивності системи (рис. 2.4)

Для практичного використання вважається прийнятним, якщо FAR < 0.001% та FRR < 1%. У військових і фінансових системах ці показники мають бути ще нижчими [14].

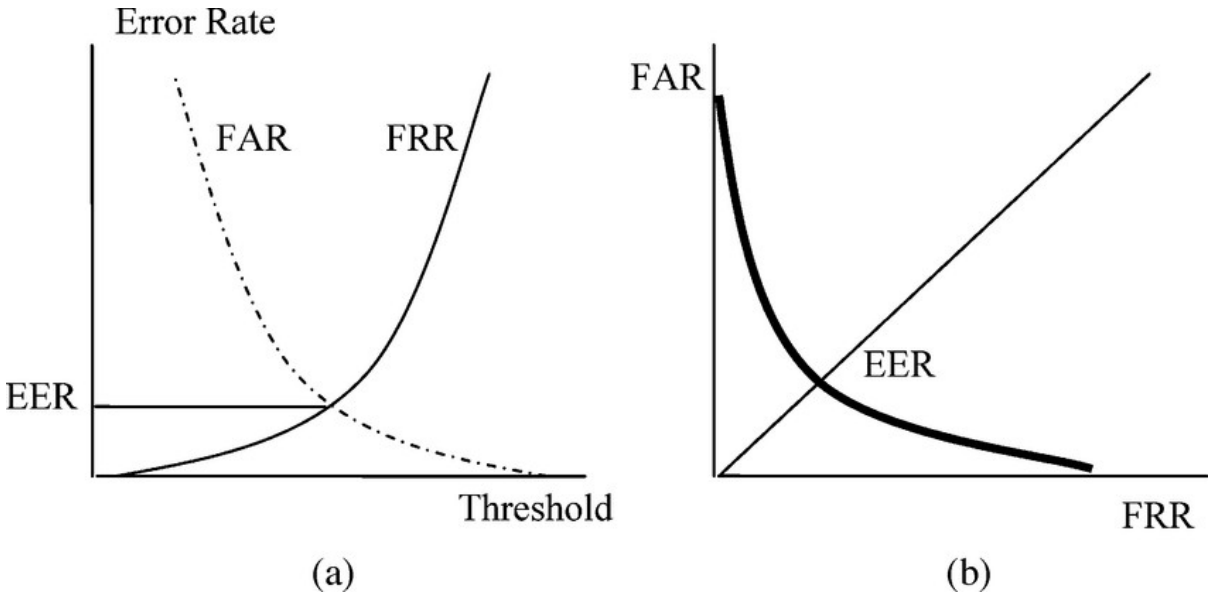


Рисунок 1.4 Крива ROC

Щоб зменшити похибки, сучасні системи використовують такі підходи:

1. Мультимодальні біометричні системи підвищують точність розпізнавання, використовуючи одночасно кілька типів біометричних ознак, наприклад обличчя і голос або відбиток пальця і малюнок вен. Такий підхід дозволяє компенсувати можливі помилки однієї модальності іншою, знижуючи рівень помилкового прийняття та відхилення, а також підвищує надійність системи в складних умовах, наприклад при слабкому освітленні або наявності шуму, і ускладнює спроби підробки даних.

2. Сучасні біометричні системи широко використовують алгоритми машинного та глибокого навчання для точного аналізу даних. Наприклад, нейронні мережі, такі як згорточна нейронна мережа CNN (Convolutional Neural Network, CNN), ефективно обробляють зображення обличчя чи відбитків пальців, виявляючи складні патерни, які важко зафіксувати традиційними методами. Алгоритми на кшталт, метод опорних векторів (Support Vector Machine, SVM) чи випадкових лісів допомагають класифікувати дані та приймати рішення навіть при наявності шуму або частково пошкоджених зразків. Глибоке навчання дозволяє системі адаптуватися до нових умов та підвищує її точність з часом.

3. Нормалізація даних є важливим етапом обробки біометричних зразків. Вона включає корекцію освітлення, вирівнювання положення голови,

масштабування або обертання зображень, що дозволяє отримати більш стабільні та порівнювані дані для подальшого аналізу. Без нормалізації навіть невеликі зміни у зовнішніх умовах можуть значно вплинути на результат розпізнавання.

4. Фільтрація за якістю полягає у відбраковуванні неякісних або неповних біометричних зразків ще на ранньому етапі обробки. Це дозволяє уникнути помилок, пов'язаних із розмитими зображеннями, шумним аудіо або поганим контактом зі сканером відбитків пальців. Завдяки фільтрації система працює більш надійно та ефективно, знижуючи ймовірність хибних спрацьовувань.

5. Шифрування шаблонів забезпечує безпеку біометричних даних навіть у випадку компрометації бази даних. Замість зберігання «сирих» зразків система зберігає їх у вигляді гешів або токенів, які неможливо відновити назад у початковий вигляд. Це значно підвищує конфіденційність та захищає користувачів від можливого використання їхніх біометричних даних сторонніми особами [15].

Для впровадження біометричної системи в організації важливо враховувати не лише технічні, але й організаційні та етичні вимоги:

1. Конфіденційність. Біометричні дані належать до чутливої інформації, тому повинні оброблятися відповідно до законів про захист персональних даних.

2. Довіра користувачів. Люди мають бути впевнені, що їхні біометричні шаблони не потраплять у сторонні руки.

3. Сумісність. Система повинна підтримувати інтеграцію з іншими інформаційними платформами.

4. Масштабованість. Важливо, щоб система працювала стабільно навіть при збільшенні кількості користувачів до сотень тисяч.

5. Стійкість до атак. Необхідно враховувати можливість атак через фотографії, 3D-маски або записані голоси.

6. Етичність і законність. Біометричні технології мають застосовуватись лише за згодою користувачів і для визначених цілей.

Майбутнє біометрії пов'язане з використанням нейромережевих моделей, гібридних сенсорів і захищених блокчейн-сховищ. Зокрема, активно досліджуються:

1. Самостійна суверенна ідентичність (Self-sovereign identity, SSI) - концепція, де користувач сам контролює свої біометричні дані.

2. Децентралізовані системи зберігання шаблонів. Дані зберігаються не на сервері, а розподілено, що підвищує безпеку.

3. Безконтактні технології. Наприклад, розпізнавання за ходою або за структурою вен без дотику.

4. Біометрія на основі штучного інтелекту (AI-driven biometrics). Використання штучного інтелекту для самонавчання системи з часом, що підвищує точність при кожній взаємодії користувача.

Попри численні переваги, біометричні технології не позбавлені проблем і ризиків. Їхній розвиток породжує як технічні, так і етичні виклики, що безпосередньо впливають на безпеку користувачів, довіру до систем та правові аспекти їх використання.

Біометричні системи, як і будь-які інші цифрові технології, можуть бути об’єктом хакерських атак. Основні технічні загрози включають атаки типу підробки. Зловмисники можуть спробувати обдурити систему, використовуючи фотографію, 3D-маску або запис голосу. Для протидії цьому сучасні системи впроваджують метод перевірку живості (liveness detection) користувача (наприклад, аналіз моргання очей, мікрорухів або температури шкіри).

Витік біометричних шаблонів. Якщо бази даних із біометричними шаблонами потрапляють до рук зловмисників, це створює серйозну загрозу. На відміну від паролів, біометричні дані не можна змінити - людина не може “поміняти відбиток пальця” чи “оновити райдужку ока”. Зниження точності в несприятливих умовах. Зміна освітлення, шум, хвороби, поранення або старіння можуть впливати на якість зчитування біометричних характеристик. Через це можливі помилки розпізнавання або відхилення справжніх користувачів. Помилки обладнання та алгоритмів. Неточності сенсорів, збої у програмному забезпеченні або неправильне навчання моделей машинного навчання можуть призводити до хибних результатів. Особливо це критично для систем із високим рівнем відповідальності - банківських чи державних.

Біометричні дані - це унікальні маркери особистості, що мають глибокий зв’язок із фізичним і психологічним “я” людини. Тому їх збір і зберігання викликає чимало етичних і правових питань таких як питання приватності, постійне стеження, етична проблема дискримінації, питання власності на дані.

Питання приватності - збір біометричних даних без згоди особи є порушенням права на приватність. В окремих країнах уже зафіксовані випадки, коли компанії незаконно зберігали біометричні зразки користувачів для маркетингових цілей [16].

Постійне стеження - використання систем розпізнавання облич у громадських місцях породжує загрозу “цифрового нагляду”, коли кожен крок людини може бути зафіксований і проаналізований. Це суперечить принципам свободи та анонімності. Етична проблема дискримінації - алгоритми розпізнавання можуть мати упередженість до певних груп користувачів (за кольором шкіри, віком або статтю). Причиною є недосконалі набори даних, якими тренують системи. Такі помилки можуть призводити до несправедливих відмов або помилкових ідентифікацій. Питання власності на дані - незрозуміло, хто саме є “власником” біометричних шаблонів - користувач, компанія чи держава. Це ускладнює визначення відповідальності у випадку витоку даних.

У світі активно формуються правові стандарти для захисту біометричної інформації. В Європейському Союзі ключову роль відіграє регламент про захист персональних даних (General Data Protection Regulation, GDPR), який класифікує біометричні дані як “спеціальну категорію персональної інформації”. Їхня обробка можлива лише за згодою користувача або в межах чітко визначених законних цілей.

В Україні питання захисту біометричних даних регулюється Законом “Про захист персональних даних”, проте законодавча база ще розвивається. Для повного захисту біометричних технологій необхідно прийняти стандарти, сумісні з європейськими нормами, а також впровадити незалежні органи контролю за дотриманням правил зберігання й використання таких даних [17].

Окрім технічних і юридичних проблем, існують соціальні ризики, пов’язані з довірою населення до біометричних систем:

1. Психологічний бар’єр. Деякі користувачі відчувають дискомфорт від самої думки, що їх “сканують”. Особливо це стосується технологій розпізнавання облич або голосу.

2. Залежність від технологій. Надмірне використання біометрії може призвести до втрати альтернативних способів ідентифікації. Якщо система вийде з ладу, користувач залишиться “відрізаним” від доступу.

3. Недовіра через попередні інциденти. Після публічних витоків біометричних баз даних (як це траплялося в Китаї, Індії, США) суспільна довіра до таких систем суттєво знизилася. Без прозорих механізмів контролю ситуація може повторитися і в інших країнах.

Для мінімізації ризиків та забезпечення надійності, етичності біометричних систем пропонуються такі напрями вдосконалення:

1. Шифрування шаблонів. Біометричні шаблони мають зберігатися лише у вигляді зашифрованих векторів, без можливості відновлення вихідного зображення.

2. Децентралізоване зберігання. Використання блокчейну для зберігання даних дозволяє уникнути централізованих точок компрометації.

3. Анонімізація даних. Під час обробки шаблони повинні бути від’єднані від особистої інформації користувача.

4. Прозорість і аудит. Компанії, що збирають біометричні дані, мають регулярно проходити незалежну перевірку безпеки.

5. Освітні кампанії. Підвищення обізнаності населення щодо безпечного використання біометричних технологій.

Ключові, загрози та шляхи мінімізації у біометричних системах проаналізовані в додатку А.

Біометричні технології є важливою частиною сучасних систем ідентифікації та автентифікації. Вони дозволяють визначати особу за її унікальними фізіологічними та поведінковими ознаками, які зазвичай не змінюються протягом життя. До фізіологічних модальностей належать відбитки пальців, риси обличчя, геометрія руки, райдужка та сітківка ока, а також ДНК.

Поведінкові модальності включають голос, почерк, динаміку натискання клавіш, особливості ходи та інші характерні патерни поведінки [18].

Процес біометричної аутентифікації проходить кілька етапів. Спочатку дані збираються за допомогою спеціальних сенсорів. Потім вони проходять передобробку, з них виділяються потрібні ознаки, формується біометричний шаблон і виконується порівняння з базою даних. Сучасні методи, що працюють на основі глибокого навчання та нейронних мереж, дозволяють створювати стійкі та надійні вектори ознак. Вони добре компенсують зміни освітлення, різні кути зйомки, шум і інші зовнішні фактори, які можуть впливати на якість даних.

Мультимодальні системи, які поєднують кілька різних видів біометрії, забезпечують більш високу точність і більшу надійність. Важливо уважно ставитися до безпеки біометричних даних, оскільки вони унікальні й незмінні, тому їх неможливо замінити, якщо вони були викрадені чи скомпрометовані. Для цього використовуються скасовані шаблони, криптографічні методи, такі як гомоморфне шифрування та багатосторонні обчислення, а також принципи диференційованої конфіденційності.

Велику роль відіграють стандарти та міжнародні регуляції, такі як NIST, ISO/IEC та GDPR. Вони визначають правила оцінювання точності алгоритмів, встановлюють формати обміну даними та вимагають дотримання приватності користувачів.

У майбутньому розвиток біометричних технологій, поєднаний із вдосконаленням алгоритмів штучного інтелекту та підвищенням стандартів безпеки, дозволить створювати ще більш точні, швидкі та надійні системи ідентифікації. Водночас важливим залишатиметься баланс між зручністю користувачів і захистом їхньої приватності, що робить етичні та правові аспекти невід’ємною частиною впровадження біометрії у різних сферах життя. Завдяки дотриманню міжнародних стандартів і застосуванню сучасних методів захисту даних, біометричні системи стають більш безпечними та надійними для користувачів. Крім того, постійне вдосконалення технологій сприятиме підвищенню довіри до біометрії та її широкому впровадженню у державних і комерційних сферах [19].

2. АНАЛІЗ СУЧАСНИХ БІОМЕТРИЧНИХ СИСТЕМ АУТЕНТИФІКАЦІЇ

2.1. Технології збору та обробки біометричних даних

Біометричні технології базуються на ідентифікації особи за допомогою фізіологічних або поведінкових характеристик людини, які є унікальними та стабільними в часі. Основні фізіологічні модальності включають відбитки пальців, геометрію руки, риси обличчя, райдужну оболонку та сітківку ока, а також ДНК зображені на рисунку 2.1.

Рисунок 2.1 - Основні фізіологічні модальності

Відбитки пальців збираються оптичними, ємнісними або ультразвуковими сенсорами, що зчитують унікальний малюнок гребенів шкіри. Розпізнавання обличчя здійснюється за допомогою RGB або інфрачервоних камер, які формують зображення, аналізуючи просторові співвідношення між ключовими точками (очі, ніс, рот). Для райдужки використовуються спеціальні оптичні сканери, які фіксують мікроструктуру її малюнка. Поведінкові модальності базуються на аналізі особливостей руху, голосу, почерку, натиску при введенні тексту чи підпису. Голосові системи аналізують спектральні параметри та тембр, а системи розпізнавання почерку - динаміку рухів руки на сенсорній поверхні.

Пристрої збору біометричних даних варіюються від стаціонарних сканерів у пунктах контролю до портативних пристроїв і смартфонів із вбудованими сенсорами [20].

Після збору даних система виконує кілька етапів обробки. Спочатку відбувається передобробка у якій усувається шум, вирівнюється освітлення, нормалізується масштаб, здійснюється обрізання непотрібних ділянок. Потім виконується виділення ознак - найважливіших характеристик, які визначають унікальність об’єкта. У традиційних системах для цього застосовували алгоритми хвильового перетворення, а в сучасних системах - глибокі нейронні мережі, що формують числові вектори-ознаки, стійкі до змін освітлення, кута зйомки та шуму. Після цього проводиться зіставлення нових біометричних даних із базою шаблонів. Для обчислення подібності використовуються метрики косинусної схожості або евклідова відстань. Система оцінює, наскільки близький вектор користувача до векторів у базі. Результат порівняння визначається через показники точності, а саме справжній коефіцієнт прийняття TAR, FRR та FAR. Висока якість обробки даних критична, оскільки навіть невеликі викривлення можуть призвести до помилок розпізнавання.

Сучасні біометричні алгоритми базуються переважно на глибокому навчанні. Нейронні мережі типу CNN аналізують мільйони зразків, щоб навчитися розрізняти навіть незначні відмінності між обличчями чи відбитками. У розпізнаванні облич широко застосовуються моделі FaceNet, ArcFace, DeepFace, які використовують спеціальні функції втрат, щоб покращити роздільну здатність простору ознак. Водночас активно розвиваються мультимодальні системи, які поєднують кілька біометричних джерел - наприклад, обличчя та голос або відбитки пальців і геометрію долоні. Це підвищує точність і зменшує ймовірність помилок. Для захисту від атак (наприклад, масок або штучних відбитків) застосовуються системи виявлення «живості», які аналізують мікрорухи очей, коливання голосу або структуру шкіри.

Питання безпеки та приватності є центральними у сфері біометрії. Оскільки біометричні дані неможливо «перезмінити» після витоку, важливо

використовувати механізми захисту шаблонів. Один із методів - біометричні дані, що можна скасувати (cancellable biometrics), коли шаблон зберігається у перетвореному вигляді, і в разі компрометації його можна замінити на новий. Криптографічні методи, такі як гомоморфне шифрування або обчислення з багатьма сторонами , дозволяють проводити порівняння біометричних шаблонів у зашифрованому вигляді, не розкриваючи самих даних. Диференційована конфіденційність використовується для тренування моделей на великих вибірках, щоб зменшити ризик витоку індивідуальної інформації. Такі методи підвищують безпеку, але вимагають великих обчислювальних ресурсів і складного програмного забезпечення [21].

У світі діють міжнародні стандарти й регуляції, які визначають правила використання біометричних систем. Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) розробляє стандарти оцінки продуктивності біометричних алгоритмів та проводить періодичні випробування, такі як тест постачальників систем розпізнавання облич (Face Recognition Vendor Test, FRVT), та обмін мінутіями для забезпечення сумісності (Minutiae Interoperability Exchange, MINEX), результати яких визначають рівень довіри до технологій.. Організація NIST відіграє центральну роль у встановленні стандартів та оцінці продуктивності біометричних систем шляхом серії ретельно спланованих і незалежних випробувань. У її діяльності зосереджено основні програми, такі як тест FRVT і MINEX, які стали міжнародними еталонами оцінки біометричних технологій.

У межах програми FRVT NIST аналізує алгоритми розпізнавання обличчя як у режимі «один-до-одного» (верифікація), так і «один-до-багатьох» (ідентифікація) з використанням великих баз даних. Під час випробувань оцінюються не лише точність і швидкість алгоритмів, а й вплив зовнішніх факторів - освітлення, кута зйомки, віку, статі та етнічної належності особи. Це дозволяє визначити не лише загальну ефективність технології, але й її справедливість та стабільність у реальних умовах.

Програма MINEX зосереджена на аналізі систем розпізнавання відбитків пальців. Її головна мета - перевірити сумісність і точність алгоритмів різних

виробників, що працюють зі стандартами зберігання й обміну біометричних даних. NIST перевіряє, наскільки шаблони відбитків, створені однією системою, можуть бути правильно розпізнані іншими, а також визначає швидкість обробки, обсяг пам’яті та відповідність міжнародним вимогам [22].

Результати таких тестів публікуються у відкритому доступі, що дає змогу компаніям, розробникам і державним структурам об’єктивно оцінювати якість біометричних алгоритмів. Вони також слугують основою для сертифікації технологій і підвищення рівня довіри користувачів до систем ідентифікації. Оцінка продуктивності NIST за допомогою алгоритмів MINEX та FRVT зображені на рисунку 2.2.

Рисунок 2.2. - Оцінка продуктивності біометричних систем NIST

NIST не лише проводить випробування, але й розробляє стандарти та технічні рекомендації для забезпечення інтероперабельності між різними системами. Ці стандарти визначають формати обміну біометричними даними, вимоги до якості зображень та алгоритмів, а також правила оцінки продуктивності. Відомі стандарти, створені за участі NIST, включають

ANSI/NIST-ITL 1 і ISO/IEC 19794-2, які широко застосовуються у міжнародних системах безпеки, паспортному контролі, банківській сфері та мобільній ідентифікації.

Загалом, діяльність цієї організації формує основу глобальної довіри до біометричних технологій. Відкритість результатів тестувань, об'єктивність методології та науковий підхід до оцінки забезпечують прозорість галузі. Технології, що відповідають її вимогам або мають статус сумісності з цими стандартами, визнаються більш надійними, безпечними та придатними для використання у державних і комерційних системах по всьому світу.

У Європейському Союзі обробка біометричних даних регулюється GDPR, який відносить їх до категорії «особливо чутливих». Використання таких даних дозволяється лише за наявності явної згоди або законних підстав. Європейська рада із захисту даних і Європейський наглядовий орган із захисту даних публікують рекомендації щодо етичного та безпечного використання біометрії, особливо в контексті штучного інтелекту та масового відеоспостереження [23].

Серед основних викликів розвитку біометричних технологій варто відзначити проблему упередженості алгоритмів, коли точність розпізнавання може залежати від раси, віку або статі користувача. Для подолання цього необхідно створювати збалансовані датасети та впроваджувати незалежне тестування. Іншою проблемою є приватність і довіра громадськості, адже без зрозумілих механізмів контролю люди не готові погоджуватися на використання біометрії в публічних місцях. Крім того, складність криптографічних обчислень і висока вартість впровадження сучасних методів захисту обмежують широке застосування приватних біометричних систем. Подальший розвиток галузі спрямований на підвищення інтероперабельності стандартів, створення більш енергоефективних алгоритмів і вдосконалення нормативного регулювання. Біометричні технології вже стали невід'ємною частиною цифрової ідентифікації, однак їхня безпечна інтеграція потребує поєднання технічних інновацій, правового контролю та етичної відповідальності.

2.2. Сучасні біометричні системи та протоколи безпеки

Біометричні системи стали одним із найважливіших елементів сучасної цифрової безпеки, оскільки вони забезпечують ідентифікацію особи на основі її унікальних біологічних і поведінкових характеристик. Сьогодні їх використовують у смартфонах, банківських системах, на пунктах пропуску, у правоохоронних структурах і навіть у соціальних мережах. Головна перевага біометрії полягає у тому, що вона не потребує запам'ятовування паролів або носіння фізичних ключів, а ґрунтується на тих ознаках, які притаманні людині від природи. Основними типами біометричних систем є розпізнавання обличчя, відбитків пальців, райдужної оболонки ока, сітківки, геометрії руки, малюнка долоні, голосу, підпису, манера ходьби та навіть динаміки натискання клавіш (рис. 2.3).

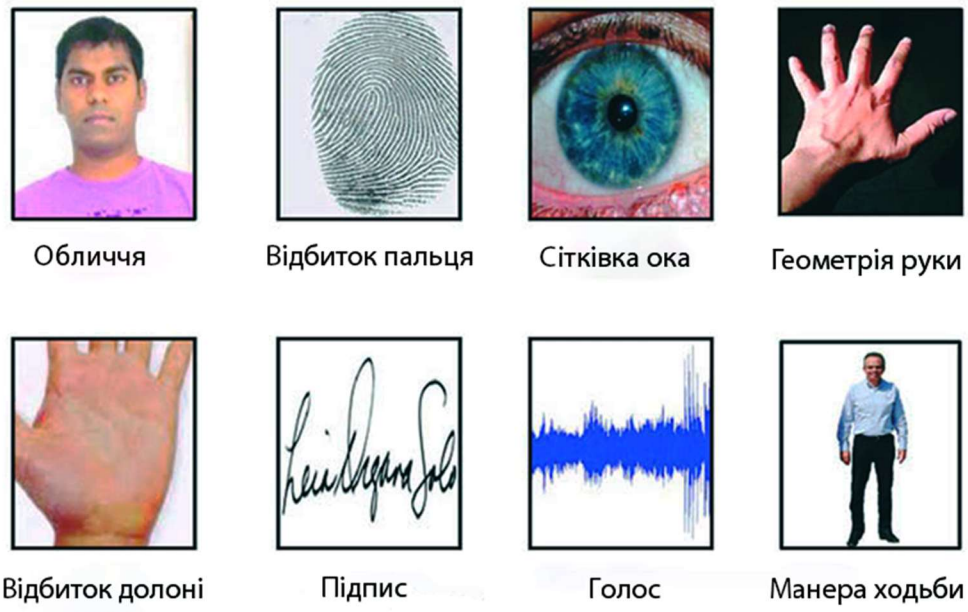


Рисунок 2.3 - Типи біометричних систем

Система розпізнавання обличчя сьогодні є найпоширенішою формою біометрії. Вона складається з кількох етапів, серед яких захоплення зображення за допомогою камери, виявлення обличчя на кадрі, вирівнювання, нормалізація яскравості та кута повороту, а потім виділення ознак. Сучасні системи, як-от (FaceNet (Google), ArcFace (InsightFace) чи DeepFace (Meta), використовують

глибокі згорткові нейронні мережі CNN, які перетворюють обличчя у вектор ознак розмірності 128 512, так званий вбудовуваний (embedding). Під час ідентифікації цей вектор порівнюється з тими, що зберігаються у базі даних, за допомогою косинусної або евклідової метрики. Для підвищення точності застосовуються функції triplet loss і ArcFace loss, що збільшують відстань між різними людьми та зменшують її між зображеннями однієї особи. Сучасні системи також впроваджують модулі виявлення живості (liveness detection) - вони перевіряють, чи є обличчя живим (наприклад, за допомогою аналізу мікрорухів очей, змін освітлення на шкірі або глибини сцени з 3D-камери). Це дозволяє запобігти обману системи за допомогою фотографії або відео [24].

Відбитки пальців залишаються класичним і найстарішим видом біометрії, який використовується понад століття. У цифрових системах сенсор зчитує мікрорельєф шкіри, тобто папілярні лінії, які формують характерні точки (мінутії) - розгалуження, закінчення та петлі. Сучасні сканери бувають кількох типів - оптичні, ємнісні, ультразвукові та термальні. Оптичні формують зображення за допомогою світлового відбиття, але є менш стійкими до підробок. Ємнісні вимірюють електричну ємність між гребенями та западинами шкіри, що підвищує точність. Ультразвукові, як у сучасних смартфонах, створюють тривимірну карту поверхні пальця, що майже унеможливлює копіювання. Алгоритми порівняння базуються на співставленні наборів мінутій і їх топологічних взаємовідносин. У більш сучасних підходах використовуються нейронні моделі, які генерують вектори ознак і дозволяють порівнювати відбитки навіть за частковими зображеннями.

Ідентифікація за райдужною оболонкою ока є однією з найточніших методик біометрії. Райдужка має надзвичайно складну структуру з тисячами мікропатернів, які не змінюються протягом життя людини. Для зчитування використовуються камери з інфрачервоним підсвічуванням, які фіксують контраст між зіницею та райдужкою. Потім зображення сегментується, нормалізується у полярній системі координат за алгоритмом Daugman, і з нього генерується бінарний код код райдужки (iris code). Порівняння здійснюється за допомогою метрики Геммінга, яка обчислює відсоток збігу бітів. Ймовірність

помилкового прийняття у таких системах становить менше ніж 1 на мільйон, що робить їх незамінними для державних і військових застосувань.

Системи розпізнавання вен руки чи пальців ґрунтуються на аналізі підшкірної судинної сітки, яку зчитують інфрачервоні сенсори. Оскільки цей малюнок знаходиться під шкірою, його неможливо скопіювати без спеціального обладнання. Такі системи використовуються у банках Японії Hitachi VeinID, Fujitsu PalmSecure та показують високу надійність навіть при фізичних ушкодженнях шкіри [25].

Голосова біометрія базується на унікальних характеристиках голосового тракту, частотних гармоніках, тембрі та манері вимови. Звуковий сигнал аналізується з використанням спектральних коефіцієнтів (Mel-Frequency Cepstral Coefficients, MFCC), на основі яких створюється вектор ознак. Сучасні системи, такі як Google Voice Match чи Nuance VocalPassword, використовують нейронні мережі типу рецидивуючий (recurrent) або трансформер (transformer) для розпізнавання користувачів у реальному часі. У банківських додатках голосові технології поєднуються з фоновим шумозаглушенням та аналізом мовних моделей, що дозволяє відрізняти справжній голос від запису.

Поведінкові біометричні методи, як-от динаміка натискання клавіш, рух миші чи аналіз ходи, стають дедалі популярнішими у кібербезпеці. Вони використовують моделі машинного навчання, які аналізують мікродеталі рухів і звичок людини. Наприклад, системи динаміки натискання клавіш (keystroke dynamics) відстежують час між натисканнями клавіш і силу натиску, що дозволяє ідентифікувати користувача навіть без його участі [26].

Протоколи безпеки у біометричних системах відіграють не меншу роль, ніж самі алгоритми розпізнавання. Біометричні дані є надзвичайно чутливими, тому їх потрібно захищати від крадіжок, підробок і несанкціонованого доступу. Одним із ключових напрямів є скасована біометрія - технологія, яка дозволяє генерувати з біометричних даних реверсивно-незалежні шаблони, тобто у випадку компрометації старий шаблон можна замінити новим без повторного збору даних. Іншим підходом є гомоморфне шифрування, коли операції порівняння виконуються у зашифрованому вигляді без розшифрування самих

біометричних шаблонів. Також активно застосовується безпечні багатосторонні обчислення, де обробка даних розподіляється між кількома серверами, і жоден з них не має повної інформації про користувача. Деякі компанії наприклад, ID R&, NEC, Microsoft розробляють децентралізовані протоколи ідентичності на основі блокчейн - такі системи дозволяють користувачу самостійно контролювати, де і коли використовуються його біометричні дані, без централізованих баз.

Сучасні стандарти безпеки біометрії регулюються міжнародними організаціями, зокрема ISO/IEC JTC1/SC37, які визначають формати шаблонів, протоколи взаємодії та критерії якості сенсорів. У рамках загального регламенту захисту даних GDPR біометричні дані вважаються особливо чутливими, тому їх зберігання потребує згоди користувача і забезпечення принципу мінімізації даних [27].

Таким чином, біометричні системи еволюціонують від простих сенсорних пристроїв до інтелектуальних децентралізованих платформ, які використовують комбінації кількох видів біометрії, машинне навчання і криптографічні протоколи. Їх майбутнє полягає у створенні гібридних систем, що поєднують фізіологічні та поведінкові ознаки, здатних адаптуватися до змін користувача та контексту використання. Біометрія поступово стає не лише засобом автентифікації, а й складовою персоналізованої взаємодії між людиною та цифровим середовищем, забезпечуючи одночасно безпеку, зручність і довіру в епоху інформаційних технологій.

Водночас розвиток біометричних систем стимулює вдосконалення стандартів безпеки та етичних норм, що регулюють використання персональних данихції. В таблиці 2.1 представлено сферу застосування, методи захисту, принципи роботи, рівень точності та стійкості сучасних біометричних систем [28]. Дивлячись на таблицю 2.1 можна сказати, що сучасні біометричні системи охоплюють широкий спектр технологій - від фізіологічних (обличчя, відбитки пальців, райдужна оболонка, венозний малюнок) до поведінкових (динаміка натискання клавіш, хода), забезпечуючи різний рівень точності, зручності та стійкості до підробок.

Таблиця 2.1

Сучасні біометричні системи та методи їх захисту

Тип біометрії	Принцип роботи	Приклади систем / технологій	Рівень точності / стійкість	Сфера застосування
Розпізнавання обличчя	Аналіз просторових співвідношень між рисами обличчя (очі, ніс, рот); формування вектора ознак (embedding) за допомогою CNN	FaceNet (Google), ArcFace InsightFace, DeepFace (Meta)	Висока точність, залежить від освітлення та кута зйомки; наявність (liveness detection) підвищує надійність	Смартфони, відеоспостереження, контроль доступу, прикордонний контроль
Відбитки пальців	Зчитування папілярних ліній і мінутій; порівняння їх топологічних зв'язків	Оптичні, ємнісні, ультразвукові сенсори (Qualcomm 3D Sonic) та (Apple Touch ID)	Дуже висока точність; середня стійкість до підробок (залежно від типу сенсора)	Смартфони, банківські системи, правоохоронні бази, офісні замки
Райдужна оболонка ока (Iris)	Сканування інфрачервоною камерою; створення бінарного коду ((iris code) за алгоритмом Daugman	IrisGuard, IriTech, LG Iris Recognition	Надзвичайно висока точність ФАР < 1×10^{-6} (FAR < 1×10^{-6})	Державні системи, військові об'єкти, прикордонний контроль
Венозна біометрія	Аналіз підшкірної судинної сітки за допомогою ІЧ-сенсорів	Hitachi VeinID, Fujitsu PalmSecure	Висока точність і стійкість до підробок	Банки, медичні установи, корпоративна безпека
Голосова біометрія	Аналіз тембру, частотних гармонік, (MFCC)-коефіцієнтів; побудова вектора ознак	Google Voice Match, Nuance VocalPassword	Середня точність; залежить від шуму та стану голосу	Кол-центри, банківські служби підтримки, віртуальні асистенти
Поведінкова біометрія	Аналіз динаміки натискання клавіш, руху миші, ходи, жестів	TypingDNA, BehavioSec, Keystroke Dynamics	Залежить від кількості спостережень; хороша для постійної ідентифікації	Кібербезпека, аутентифікація користувачів онлайн
Протоколи безпеки	Захист шаблонів за допомогою шифрування, гомоморфних обчислень, розподіленої обробки або blockchain	Cancelable biometrics, Homomorphic Encryption, Secure Multi-Party Computation, Blockchain ID	Забезпечують конфіденційність і стійкість до компрометації	Усі біометричні системи, зокрема державні та банківські

Найвищу точність демонструють системи розпізнавання райдужної оболонки та венозної сітки, тоді як розпізнавання обличчя та голосу більш

уразливе до умов зовнішнього середовища. Поведінкова біометрія має перевагу в можливості безперервної аутентифікації, однак її надійність значною мірою залежить від кількості накопичених даних. Загалом, для підвищення захисту біометричних даних активно застосовуються криптографічні технології - шифрування, гомоморфні обчислення, розподілена обробка та концепції скасованих шаблонів, що дозволяє мінімізувати ризики компрометації та зловживань. Отже, розвиток біометрії рухається у напрямку поєднання різних типів ідентифікаційних ознак та впровадження потужних протоколів безпеки, що забезпечує високий рівень надійності й робить такі системи перспективними для державного, корпоративного та масового використання.

2.3. Проблеми та виклики застосунків біометричної аутентифікації

Біометрична аутентифікація має численні переваги, зокрема унікальність ознак, зручність користування та можливість безперервної перевірки користувача, але водночас вона стикається з низкою складних проблем і викликів, які впливають на ефективність і безпеку систем [29].

Однією з головних проблем є точність. Біометричні системи працюють на основі сенсорів та алгоритмів обробки даних, і навіть невелика помилка у зчитуванні або обробці може призвести до хибного прийняття або відхилення користувача. Показники хибного прийняття FAR і хибного відхилення FRR залежать від якості сенсорів, умов зчитування, стану користувача (наприклад, поранення пальця, зміна голосу через хворобу, втома або стрес), освітлення і шуму. Щоб зменшити ці помилки, застосовують мультимодальні системи, які поєднують кілька біометричних ознак, наприклад, відбиток пальця і розпізнавання обличчя, або голос і динаміку натискання клавіш. Також використовують алгоритми машинного навчання для адаптивної обробки даних і компенсації змін у фізичних характеристиках користувача.

Другим викликом є вразливість до атак. Сучасні зловмисники можуть спробувати обійти систему за допомогою фотографій, відеозаписів, 3D-масок, підроблених відбитків пальців або записаного голосу. Для захисту

впроваджують технології виявлення живості, які перевіряють живість користувача через аналіз мікрорухів очей, змін шкірного кольору, температури, глибини сцени або інших фізіологічних показників. Крім того, для захисту від підробок застосовують спеціальні сенсори високої роздільної здатності, ультразвукові або інфрачервоні, а також алгоритми перевірки узгодженості сигналів з декількох джерел.

Третім серйозним викликом є захист біометричних даних, адже біометричні шаблони є незмінними і користувач не може змінити відбиток пальця або райдужку ока у разі компрометації. Це робить їх особливо цінними для хакерів і одночасно дуже вразливими. Щоби знизити ризики, впроваджують методи скасована біометрія, де з оригінальних даних створюють трансформовані шаблони, які можна змінити у разі витоку. Також використовують шифрування шаблонів, зберігаючи їх як хеші або токени, а обробку виконують у зашифрованому вигляді без розшифровки даних [30].

Четверта група проблем пов’язана з упередженістю та дискримінацією. Біометричні алгоритми можуть демонструвати нижчу точність для окремих демографічних груп через неповноту навчальних наборів даних або неправильне тренування моделей. Це стосується віку, раси, статі та фізичних особливостей. Щоби мінімізувати ці ризики, системи навчають на різноманітних і збалансованих наборах даних, а також проводять періодичну оцінку алгоритмів для виявлення упередженості і корекцію моделей.

П’ятою проблемою є приватність та контроль над даними. Використання біометрії без згоди користувача або в умовах масового спостереження створює ризик порушення конфіденційності та психологічного дискомфорту. Для вирішення цього впроваджують принцип самоконтрольованої ідентичності (self-sovereign identity), де користувач сам визначає, які дані і кому надає. Також застосовують децентралізовані сховища на базі блокчейн і анонімізацію шаблонів, щоб дані не були пов’язані з персональною інформацією [31].

Шостою проблемою є масштабування і інтеграція. У великих організаціях або державних системах велика кількість користувачів і різнорідне обладнання створюють труднощі у стандартизації та сумісності сенсорів і протоколів. Для

цього використовують уніфіковані стандарти, модульні архітектури та протоколи взаємодії між системами, що дозволяє легко додавати нові сенсори чи оновлювати алгоритми.

Сьомою проблемою є безперервна аутентифікація. Вона потребує постійного збору даних про користувача у фоновому режимі, що створює додаткові навантаження на систему, підвищує вимоги до обробки даних і зберігання, а також посилює ризики приватності. Вирішенням є використання оптимізованих алгоритмів обробки, відправка лише агрегованих або анонімізованих даних на сервери і обмеження часу зберігання.

Усі ці проблеми (рис.2.4) можна подолати комплексним підходом, який передбачає поєднання мультимодальних систем, використання адаптивних алгоритмів машинного навчання, захищене зберігання та обробку даних, впровадження правових і етичних стандартів, проведення регулярного аудиту систем і навчання користувачів [32].

Рисунок 2.4 - Виклики біометричних систем та їх рішення

Лише такий підхід дозволяє зробити біометричну аутентифікацію ефективною, безпечною та прийнятною для суспільства, мінімізуючи ризики технічні, соціальні та етичні.

Відбитки пальців є одним із найпоширеніших методів біометричної аутентифікації завдяки простоті збору даних і високому рівню унікальності, проте вони мають ряд проблем і викликів, зокрема знос і пошкодження шкіри, порізи, мозолі або інші зміни на пальцях, що можуть призвести до хибного відхилення користувача, атаки типу (spoofing), коли підроблені відбитки пальців із силікону або гелю дозволяють обійти систему, а також витік шаблонів, оскільки у разі компрометації дані не можна змінити як пароль. Для вирішення цих проблем використовують сенсори з ультразвуковою технологією, які оцінюють структуру під шкірою і визначають живий палець, створюють скасовані відбитки пальців, де з шаблонів формуються трансформовані цифрові вектори, які можна змінити при витоку, а також застосовують мультимодальні системи, поєднуючи відбитки пальців з іншими ознаками, наприклад голосом або обличчям, для підвищення надійності.

Розпізнавання обличчя популярне у смартфонах, банкоматах і системах відеоспостереження, проте воно стикається з проблемами освітлення і ракурсу, коли зміни освітлення, положення голови або часткове закриття обличчя, наприклад окулярами чи масками, можуть вплинути на точність, атаками типу (spoofing), що передбачають використання фотографій, відео або 3D-масок, а також упередженістю алгоритмів, коли точність розпізнавання нижча для людей певних рас, віку або статі через неповні навчальні набори. Для підвищення ефективності застосовують алгоритми глибокого навчання для адаптивного розпізнавання облич у різних умовах, впроваджують технології (liveness detection) для підтвердження живого користувача, а також інтегрують мультимодальні системи, наприклад поєднання розпізнавання обличчя та голосу [33].

Розпізнавання голосу використовується у телефонних банках, віртуальних асистентах та системах дистанційної аутентифікації, проте воно чутливе до змін голосу через хвороби, стрес, старіння або шумове середовище, а також вразливе до атак через відтворення голосу з записів Для підвищення надійності застосовують спектральні і поведінкові ознаки голосу, які важко підробити,

алгоритми адаптивного навчання, що враховують зміни голосу, і поєднання голосу з іншими ознаками, наприклад з динамікою набору тексту

Розпізнавання райдужної оболонки ока забезпечує високоточну ідентифікацію для контролю доступу до високозахищених об’єктів, проте технологія стикається з проблемами високої вартості сенсорів і критичної компрометації шаблонів, оскільки змінити райдужку неможливо Для вирішення цих проблем використовують зашифровані шаблони і захищені протоколи зберігання даних, а також інтегрують цю технологію у мультимодальні системи для підвищення надійності

Поведінкові системи, такі як розпізнавання ходьби, динаміки набору тексту та поведінки користувача при роботі з пристроєм, дозволяють здійснювати непомітну і безперервну аутентифікацію, проте вони мають високу варіативність через настрій, стан здоров’я або стрес і підвищену ймовірність хибного відхилення Для підвищення стабільності застосовують адаптивні алгоритми для постійного навчання системи та комбінацію з фізіологічними ознаками, щоб забезпечити надійну і точну аутентифікацію [34]. Виклики біометричних систем та способи їх вирішення розписані в таблиці 2.2.

Таблиця 2.2

Виклики біометричних систем та способи їх вирішення

Метод біометричної аутентифікації	Основні проблеми та виклики	Приклади загроз	Методи мінімізації / рішення
Відбитки пальців	Технічна точність (FAR/FRR), знос і пошкодження шкіри	Порізи, мозолі, зміни шкіри, хибне відхилення	Сенсори з ультразвуком, cancelable fingerprints, мультимодальні системи (відбиток + голос/обличчя)
Розпізнавання обличчя	Освітлення, ракурс, часткове закриття, упередженість алгоритмів	Фотографії, відео, 3D-маски, нижча точність для певних рас/статей	Алгоритми глибокого навчання, liveness detection, мультимодальні системи (обличчя + голос)
Розпізнавання голосу	Зміни голосу через хвороби, стрес, старіння, шум	Відтворення голосу з записів	Спектральні і поведінкові ознаки, адаптивне навчання, комбінування з іншими ознаками (динаміка набору)

Прод. табл. 2.2

Розпізнавання райдужної оболонки	Висока вартість сенсорів, критична компрометація шаблонів	Незмінність шаблону - неможливо відновити при витоку	Шифрування шаблонів, захищене зберігання, інтеграція у мультимодальні системи
Поведінкові ознаки (ходьба, динаміка набору тексту, поведінка користувача)	Висока варіативність через стан здоров'я, стрес, настрій	Хибне відхилення, нестабільність	Адаптивні алгоритми, постійне навчання, комбінування з фізіологічними ознаками
Загальні проблеми біометричної системи	Технічна точність, атаки spoofing, захист даних, bias, приватність, масштабування, безперервна аутентифікація	Фотографії, маски, відео, підроблені відбитки, витік шаблонів, дискримінація, психологічний дискомфорт	Мультимодальні системи, машинне навчання, liveness detection, cancelable biometrics, шифрування, стандарти, аудит, навчання користувачів, децентралізоване зберігання, self-sovereign identity

У другому розділі було детально розглянуто сучасні методи біометричної аутентифікації та їхні переваги й недоліки. До таких способів належать шифрування інформації, зберігання ембедінгів без доступу до зовнішніх серверів, а також механізми перевірки «живості», що дозволяють системі визначати справжню людину. Приділялася увага точності алгоритмів, а також міжнародним стандартам (ISO/IEC 30107) і законодавчим нормам (GDPR), що регулюють обробку та захист біометричних даних.

Проведений аналіз існуючих технологій показав, що серед усіх методів біометричної ідентифікації саме розпізнавання обличчя виділяється як один із найзручніших і найбільш надійних. Воно поєднує високу точність, швидку роботу та здатність підтримувати механізми перевірки «живості», завдяки чому система стає стійкішою до спроб обману. Зважаючи на всі ці переваги, мною було прийнято рішення створити програму для біометричної аутентифікації користувачів, яка працює саме на основі розпізнавання обличчя.

3. РОЗРОБКА ЗАХИЩЕНОГО МОДУЛЯ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

3.1. Методи захисту біометричних даних та забезпечення конфіденційності

Аутентифікація користувача за допомогою розпізнавання обличчя є однією з найпопулярніших сучасних технологій біометричної ідентифікації. Вона забезпечує швидкий і зручний вхід у систему без необхідності запам’ятовування паролів, але водночас вимагає особливої уваги до питань безпеки, конфіденційності та етичного використання. На рисунку 3.1 зображено структурна схему того як проходить аунтентифікація користувача в додатку за допомогою розпізнавання обличчя.

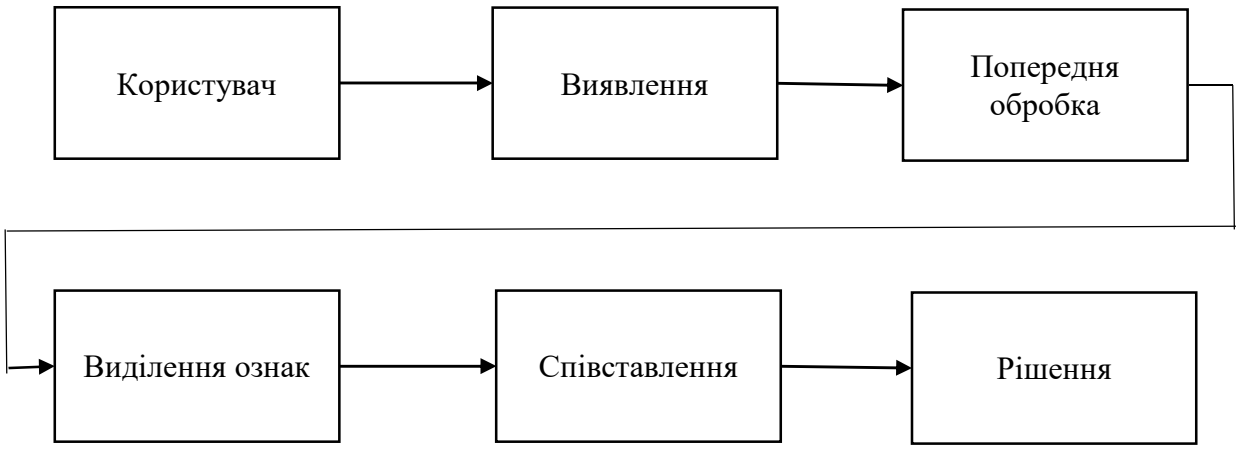


Рисунок 3.1 - Схема розпізнавання обличчя

Коли користувач запускає програму, відкривається графічне вікно, камера активується, і система починає безперервно зчитувати та оновлювати зображення в реальному часі. Саме взаємодія користувача з інтерфейсом визначає подальші дії - реєстрація, авторизація чи видалення. У цей момент система працює у фоновому режимі, постійно оновлюючи останній кадр із вебкамери, щоб мати актуальне зображення для аналізу.

Після того як користувач обирає дію, система переходить до виявлення обличчя. Вона бере останній отриманий кадр з камери, конвертує його з BGR у

RGB, оскільки бібліотека *face_recognition* працює лише з таким форматом. Далі алгоритм шукає на зображенні обличчя - визначає, чи є на кадрі характерні контури, очі, ніс, рот і пропорції, що відповідають людському обличчю. Якщо жодного обличчя не знайдено, процес зупиняється, і користувач отримує повідомлення про помилку.

Коли обличчя знайдено, система продовжує до попередньої обробки. На цьому етапі зображення готується до роботи з алгоритмами глибинного аналізу: вирівнюються кольори, визначаються області обличчя, формується структурований масив пікселів, який далі буде перетворено у числове представлення. Для реєстрації система також зберігає зображення користувача у файл, а для входу та видалення - використовує його лише для подальшого аналізу.

Після підготовки відбувається виділення ознак - найважливіший етап, у якому штучний інтелект будує унікальний вектор чисел, що описує обличчя. Він включає у себе просторові відстані між ключовими точками, симетрію, геометрію і багато інших параметрів. Такий вектор (encoding) фактично є цифровим «відбитком» обличчя. Для реєстрації кожен новий користувач отримує власний набір таких ознак, які зберігаються у вигляді знімка, що потім аналізується при вході. Для авторизації або видалення ознаки порівнюються з тими, що вже є в базі.

Коли ознаки сформовані, система переходить до співставлення. Вона завантажує збережене фото користувача з диска, повторно виділяє ознаки для цього зображення й порівнює їх із поточним вектором. Алгоритм визначає, чи є обидва набори ознак достатньо близькими. Якщо різниця мінімальна - обличчя вважається тим самим, якщо ні - система відмовляє в доступі. Перед цим, звичайно, обов’язково перевіряється логін і хешований пароль, тож фотографія сама по собі не дає доступу без правильних облікових даних.

На завершальному етапі система приймає рішення: чи дозволити дію. Якщо паролі збігаються, а обличчя впізнане - користувача впускають у систему, відкривають для нього потрібну папку, записують факт входу у файл логу або видаляють його обліковий запис. Якщо ж будь-який етап не підтверджено -

система відмовляє в операції, повідомляє користувача й повертається до початкового стану, продовжуючи знімати зображення з камери.

Процес розпізнавання обличчя починається з етапу реєстрації, коли система зберігає зразок обличчя користувача. Зображення обробляється спеціальними алгоритмами, які виділяють основні риси та створюють цифрове представлення обличчя у вигляді векторного шаблону, або так званого ембедінгу. Під час подальших спроб входу програма знову зчитує обличчя користувача, порівнює його ембедінг із уже збереженим і на основі схожості визначає, чи це той самий користувач. У сучасних системах для цього найчастіше використовуються згорткові нейронні мережі, такі як FaceNet або ArcFace, які забезпечують високу точність завдяки вмінню виділяти стійкі ознаки навіть за змін освітлення, положення голови чи віку.

Одним із головних викликів для таких систем є протидія підробкам, коли зловмисник намагається обдурити систему за допомогою фотографії, відео або маски. Для цього впроваджуються методи перевірки живості, які можуть бути активними або пасивними. Активні методи передбачають, що користувач виконує певну дію - наприклад, моргає або повертає голову, - щоб довести, що він справжній. Пасивні методи базуються на аналізі текстур, відблисків, глибини або інших фізичних характеристик обличчя. Визнаним міжнародним стандартом у цій галузі є ISO/IEC 30107, який визначає вимоги до виявлення спроб обману та методологію тестування систем біометричного захисту.

Питання безпеки шаблонів є особливо важливим, оскільки біометричні дані не можна змінити так, як пароль. Замість збереження зображень системи зберігають лише ембедінги, які не дозволяють відтворити первинне фото користувача. Дані шифруються як під час передавання, так і під час зберігання. У деяких рішеннях, наприклад у Face ID від Apple, усі обчислення виконуються безпосередньо на пристрої, і біометричні дані ніколи не залишають його меж. Це значно підвищує рівень конфіденційності, але ускладнює централізоване керування даними у великих системах.

Оцінка точності та справедливості таких систем є ще одним важливим аспектом. Згідно з дослідженнями Національного інституту стандартів і

технологій США (NIST), ефективність алгоритмів розпізнавання може суттєво відрізнятися залежно від раси, статі, віку чи умов освітлення. Тому перед використанням технології в реальному середовищі необхідно проводити ретельне тестування на власних даних користувачів, щоб виявити можливі похибки та упередження.

Юридичний бік питання також відіграє ключову роль. У Європейському Союзі розпізнавання обличчя підпадає під дію Загального регламенту про захист даних (GDPR), який вважає біометричну інформацію особливо чутливою категорією персональних даних. Для її обробки потрібна чітка правова підстава, проведення оцінки впливу на приватність (Data Protection Impact Assessment) та надання користувачам прозорої інформації про те, як саме використовуються їхні обличчя. Крім того, користувачеві повинна бути надана можливість відмовитися від біометричної аутентифікації та скористатися альтернативним способом входу.

На практиці розробникам варто дотримуватися кількох принципів. Перш за все, впроваджувати розпізнавання обличчя лише тоді, коли це дійсно необхідно з погляду безпеки чи зручності. Бажано реалізувати обробку даних безпосередньо на пристрої користувача, використовуючи стандартні засоби операційної системи, такі як Face ID на iOS або BiometricPrompt на Android. Обов’язковим є впровадження механізмів виявлення спуфінгу відповідно до міжнародних стандартів, надійне шифрування шаблонів та обмеження їх зберігання. Важливо також вести аудит спроб входу та виявлених атак, не накопичуючи при цьому зайвих біометричних даних.

Таким чином, технологія аутентифікації за обличчям поєднує у собі зручність для користувача, високу швидкість та сучасні підходи штучного інтелекту, проте потребує глибокого розуміння технічних, юридичних та етичних аспектів. Її успішна реалізація можлива лише тоді, коли розробник одночасно враховує вимоги безпеки, конфіденційності, надійності й справедливості, спираючись на міжнародні дослідження, такі як FaceNet, NIST FRVT і стандарти ISO/IEC 30107, а також дотримання законодавства на кшталт GDPR.

3.2 Програмна реалізація застосунку біометричної аутентифікації

Запропонована програмна реалізації застосунку біометричної аутентифікації застосовується для аутентифікації користувача за допомогою розпізнавання обличчя.

Код програми написаний на мові програмування Python із використанням таких основних репозиторіїв (бібліотек) *Tkinter*, *OpenCV, Face_recognition, Pillow, Json, subprocess,* їх взаємодія показана на рисунку 3.16.

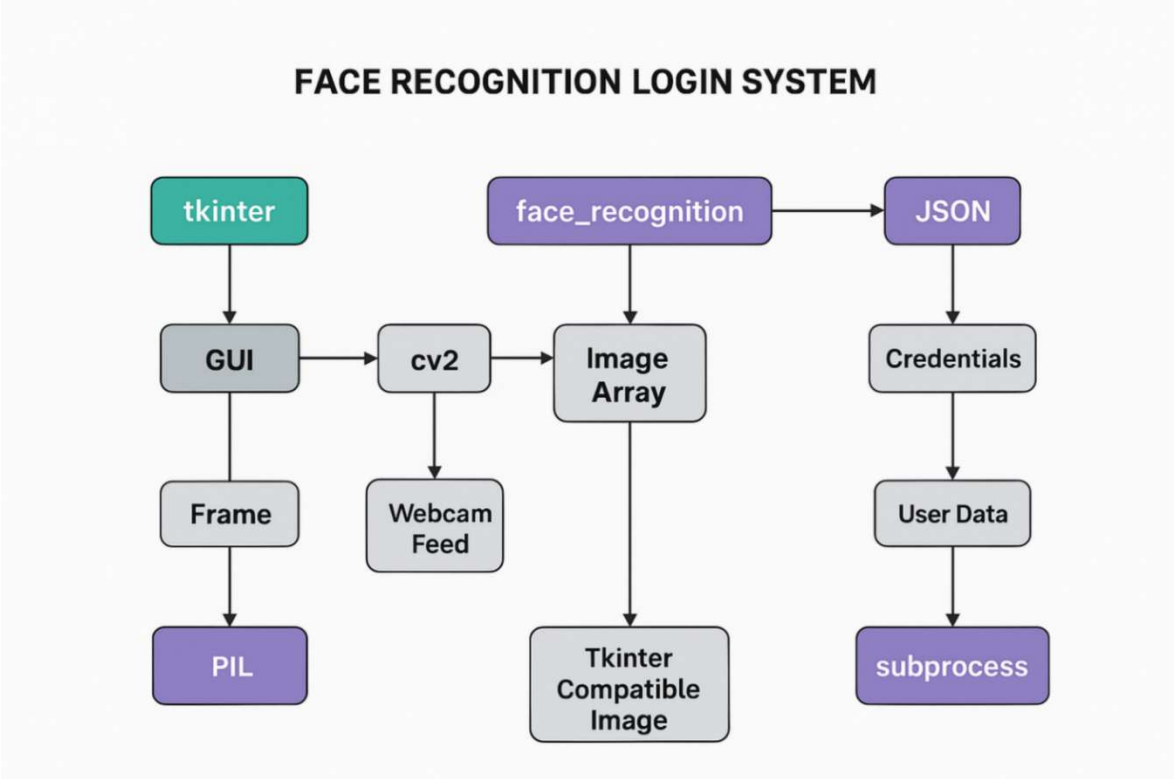


Рисунок 3.2 - Модулі та їх взаємодія в програмі розпізнавання обличчя

Tkinter я обрав тому, що це вбудована бібліотека Python, яка не потребує додаткових установок і дозволяє швидко створювати прості графічні інтерфейси. Завдяки цьому можна зосередитися на функціоналі програми, не витрачаючи час на налаштування середовища чи встановлення важких фреймворків. Інтерфейси, створені за допомогою *tkinter,* достатньо легкі, працюють практично на будь-якій системі та ідеально підходять для невеликих утиліт і прототипів.

OpenCV я обрав через те, що це одна з найефективніших та найоптимізованіших бібліотек для роботи з відеопотоками та зображеннями. Вона забезпечує високу продуктивність, оскільки написана на C/C++ і має широкі можливості - від захоплення відео з камери до комплексної обробки кадрів. У проєктах, де потрібне швидке отримання та обробка зображення в реальному часі, *OpenCV* є практично стандартом, тому він чудово підходить для задач, пов'язаних із розпізнаванням облич або іншими елементами комп'ютерного зору.

Бібліотеку *face_recognition* я обрав тому, що вона має надзвичайно простий і зрозумілий API, при цьому всередині використовує потужні моделі глибокого навчання. Її головна перевага - відсутність необхідності тренувати власну нейромережу. Це дозволяє буквально кількома рядками коду отримувати координати облич на зображенні та векторні представлення (encodings), які дають змогу ідентифікувати людей із високою точністю. Для невеликих локальних систем або навчальних проєктів ця бібліотека є оптимальним рішенням, оскільки поєднує в собі ефективність і легкість використання.

Pillow я обрав як основний інструмент для роботи із зображеннями, тому що вона є стандартом у Python для відкриття, обробки та конвертації графічних файлів. Вона чудово інтегрується з *tkinter* і дозволяє легко відображати кадри чи фотографії у вікні програми. Окрім цього, *Pillow* дає можливість виконувати базову обробку - зміну розміру, обрізання, конвертацію форматів - що важливо, коли потрібно підготувати зображення для подальшої обробки алгоритмами розпізнавання.

Json я обрав тому, що це простий і легкий формат для зберігання даних. Він ідеально підходить для невеликих баз користувачів, де потрібно зберегти параметри профілю, ім'я або набір числових векторів - таких як *face encodings*. Python нативно працює з форматом *JSON*, що робить процес запису і зчитування даних дуже зручним. До того ж *JSON* залишається людиночитним, тому у разі потреби файл можна легко переглянути і відредагувати вручну.

Бібліотеки *subprocess* та *os* я обрав для взаємодії з операційною системою та файловою структурою. Їхнє використання дозволяє зчитувати файли,

створювати каталоги, виконувати системні команди або запускати зовнішні процеси. Це необхідно, коли програма повинна працювати з файлами користувача, організовувати збереження фотографій, перевіряти наявність каталогів або виконувати будь-які інші технічні операції на рівні ОС. Завдяки цим модулям програма отримує можливість гнучко працювати зі структурою файлів, автоматизувати дії та розширювати свою функціональність без зайвих обмежень.

Отже, я обрав саме ці бібліотеки тому, що вони утворюють оптимальне поєднання, при якому *tkinter* забезпечує простий графічний інтерфейс, *OpenCV* працює з відео та зображеннями, *face_recognition* відповідає за ідентифікацію облич, *Pillow* дозволяє обробляти фото, *JSON* зручно зберігає дані користувачів, а *subprocess* і *os* забезпечують повноцінну взаємодію з системою. Разом вони дають змогу реалізувати компактний, ефективний і функціональний застосунок без зайвих залежностей або складних налаштувань.

Запропонована програмна реалізація поєднує інтерфейс користувача (GUI) на базі *tkinter*, обробку зображень і відео за допомогою *OpenCV* та *Pillow*, а також біометричну перевірку особи за допомогою бібліотеки *face_recognition*.

Застосовуючи розроблене програмне рішення користувач може:

1. Зареєструвати цифровий ембедінг для користувача;
2. Аутентифікуватися в системі;
3. Видалити непотрібний обліковий запис.

Під час реєстрації система створює цифровий ембедінг - унікальне числове представлення обличчя. Коли користувач натискає кнопку реєстрації, програма зчитує останній кадр із вебкамери, виконує виявлення обличчя та перетворює зображення у формат, придатний для аналізу. Після цього алгоритм виділяє набір ознак (encoding), що описують геометрію та структуру обличчя. Знімок зберігається у базі даних у вигляді файлу, а пароль - у вигляді хешу. Таким чином, формується особистий шаблон, на основі якого надалі буде здійснюватись ідентифікація користувача.

Під час аутентифікації система одночасно перевіряє і пароль, і відповідність обличчя. Користувач вводить логін та пароль, після чого програма порівнює введений пароль з хешем, що збережений у базі. Одночасно камера

зчитує новий кадр, система повторно виявляє обличчя, виконує його попередню обробку та формує новий ембедінг. Далі він співставляється з тим, що був збережений при реєстрації. Якщо обидві умови - правильний пароль і збіг обличчя - виконані, система визнає користувача справжнім та дає йому доступ до функціоналу.

Видалення облікового запису також відбувається із додатковим рівнем захисту - перевіркою обличчя. Після введення логіна і пароля система валідує пароль, а потім, подібно до авторизації, аналізує поточне обличчя користувача. Алгоритм створює ембедінг із кадру камери та співставляє його з збереженим шаблоном. Якщо підтвердження успішне, система видаляє файл із зображенням та запис у базі користувачів. Таким чином, можливість видалення доступна лише власнику обличчя, а не тому, хто знає пароль.

Репозиторії та модулі, що використовуються в коді:

1. *os*, призначений для роботи з файловою системою операційної системи. Потрібен для створення папок, перевірки існування файлів, видалення зображень користувачів тощо.

Програмна реалізація застосунку біометричної аутентифікації передбачає використання кількох ключових бібліотек Python, кожна з яких виконує певну функціональну роль і взаємодіє з іншими компонентами для забезпечення повноцінного процесу реєстрації, авторизації та видалення користувача. Для роботи з файловою системою використовується бібліотека *os*, яка дозволяє створювати необхідні папки для збереження зображень користувачів, перевіряти наявність файлів та видаляти їх при необхідності. Наприклад, функція *os.makedirs(DB_DIR, exist_ok=True)* автоматично створює каталог для зберігання фотографій, якщо його ще немає (рис. 3.3). Також бібліотека os дозволяє програмі динамічно реагувати на зміни у файловій структурі, що особливо важливо під час обробки великої кількості користувачів. Завдяки цьому застосунок може коректно оновлювати дані, уникати помилок, пов'язаних із відсутніми файлами чи каталогами, та забезпечувати надійне зберігання біометричної інформації.

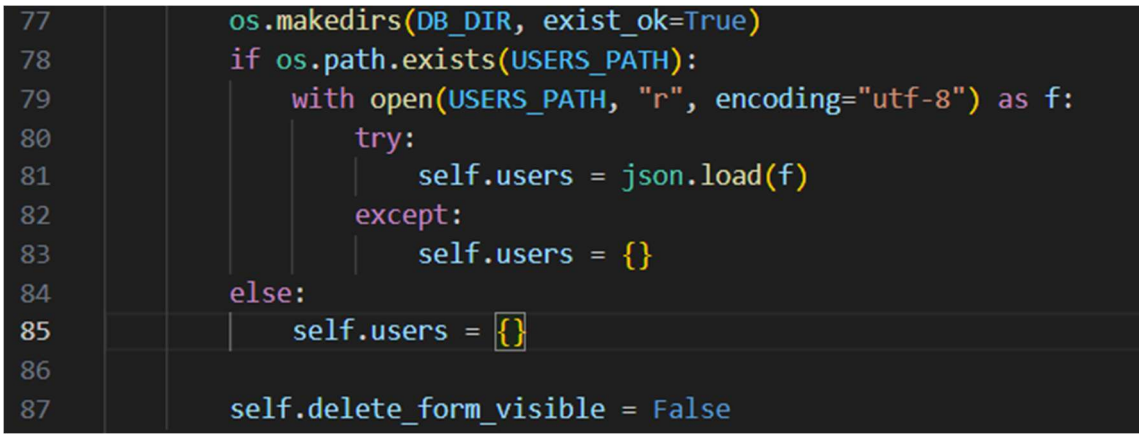


Рисунок 3.3 - Створення каталогу для фото

Функція *os.path.exists(path)* перевіряє, чи існує файл з даними користувача (рис. 3.4).

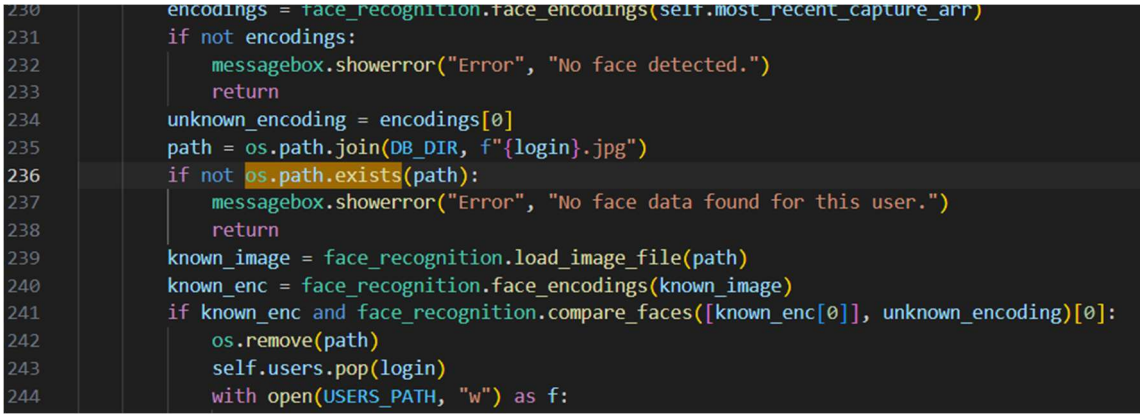


Рисунок 3.4 - Перевірення файла з даними користувача

У випадку видалення облікового запису використовується *os.remove(path)*, яка гарантує, що файли користувача повністю видаляються з системи (рис. 3.5).

Рисунок 3.5 - Видалення користувача з системи

Бібліотека *JSON* у Python використовується для зберігання та обробки даних користувачів у системі біометричної аутентифікації. Вона дозволяє зберігати інформацію у структурованому форматі ключ-значення, що робить її легкою для читання людиною та простою для обробки програмою. У нашому застосунку JSON застосовується для збереження логінів, паролів і шляхів до зображень облич користувачів, необхідних для реєстрації та авторизації.

Під час запуску програми файл *users.json* завантажується у словник Python, що дає змогу швидко отримувати доступ до даних користувачів та перевіряти їхню відповідність під час входу. Структура *JSON* дозволяє зручно додавати нових користувачів, змінювати існуючі записи або видаляти їх, без необхідності використовувати складні бази даних. Наприклад, для кожного користувача зберігаються його логін, пароль і шлях до фотографії обличчя, яка використовується для порівняння з живим зображенням під час аутентифікації.

Коли користувач реєструється, новий запис додається у словник, після чого оновлений словник записується назад у файл за допомогою функції *json.dump()*. Такий підхід забезпечує збереження актуальної бази даних користувачів і дозволяє підтримувати її у структурованому та зрозумілому вигляді. Під час видалення облікового запису відповідний запис видаляється зі словника, а оновлений словник знову записується у файл, що гарантує синхронізацію бази даних із файлами зображень користувачів.

Завдяки використанню *JSON* програма залишається простою у підтримці, легко масштабується для невеликих і середніх систем, забезпечує зручність резервного копіювання та можливість ручного редагування даних. У результаті *JSON* виступає зручним, легким і надійним інструментом для роботи з даними користувачів у біометричній системі, що ілюструє рисунок 3.6.

```
183         filename = os.path.join(DB_DIR, f"{login}.jpg")
184         cv2.imwrite(filename, self.most_recent_capture_arr)
185         self.users[login] = {"password": password}
186         with open(USERS_PATH, "w") as f:
187             json.dump(self.users, f, indent=4)
188         messagebox.showinfo("Success", f"User '{login}' registered successfully!")
189         self.hide_all_frames()
190
```

Рисунок 3.6 - Робота з даними

Бібліотека *datetime* у Python використовується для роботи з датою та часом, що є важливим елементом у біометричній системі аутентифікації для ведення журналу подій та контролю активності користувачів. У нашому застосунку *datetime* дозволяє фіксувати точний момент входу користувача у систему, що підвищує безпеку та дозволяє відстежувати історію дій. Під час авторизації, після успішного входу, програма зчитує логін користувача та поточний час за допомогою функції *datetime.datetime.now()*. Ця інформація записується у файл *log.txt* у вигляді рядка, що містить ім'я користувача, дату та час входу, а також тип дії, наприклад, вхід у систему. Такий журнал дозволяє відстежувати, коли і хто входив до системи, що важливо для аудиту безпеки та контролю доступу. Крім фіксації часу входу, *datetime* може використовуватися для порівняння дат та визначення термінів дії сесій або обмежень доступу. Важливо, що завдяки стандартному формату запису часу, дані з *datetime* легко обробляти, сортувати та аналізувати. Таким чином, використання *datetime* у нашій системі забезпечує надійний контроль активності користувачів та ведення журналу подій у зручному і зрозумілому форматі (рис. 3.7).

```
209         known_image = face_recognition.load_image_file(path)
210         known_enc = face_recognition.face_encodings(known_image)
211         if known_enc and face_recognition.compare_faces([known_enc[0]], unknown_encoding)[0]:
212             messagebox.showinfo("Welcome", f"Welcome, {login}!")
213             with open(LOG_PATH, "a", encoding="utf-8") as f:
214                 f.write(f"{login},{datetime.datetime.now()},in\n")
215             if os.path.exists(OPEN_FOLDER_PATH):
216                 subprocess.Popen(f'cmd /c start "" "{OPEN_FOLDER_PATH}"', shell=True)
217             self.hide_all_frames()
218         else:
219             messagebox.showerror("Error", "Face does not match registered user.")
```

Рисунок 3.7 - Запис логіна та час користувача

Бібліотека *tkinter* у Python використовується для створення графічного інтерфейсу користувача (GUI), що є основою взаємодії людини з біометричною системою аутентифікації. Вона дозволяє створювати вікна, кнопки, поля введення, текстові повідомлення та інші елементи інтерфейсу без необхідності встановлювати додаткові пакети, оскільки *tkinter* є стандартною бібліотекою Python. У нашому застосунку *tkinter* формує головне вікно програми, де користувач бачить назву системи, відеопотік з вебкамери та кнопки для

виконання основних дій - LOGIN, REGISTER і DELETE ACCOUNT. Кожна кнопка пов'язана з певною функцією, яка обробляє відповідну дію користувача. Наприклад, кнопка REGISTER відкриває форму для введення логіну та паролю, а також активує процес зйомки фотографії обличчя користувача, яка буде збережена для подальшої аутентифікації. *tk.Label* і *tk.Entry* дозволяють відображати текст і приймати введення користувача, а *tk.messagebox* використовується для відображення інформаційних повідомлень про успішну або невдалу реєстрацію, авторизацію чи видалення облікового запису. Завдяки інтеграції з іншими бібліотеками, такими як OpenCV та Pillow, tkinter дозволяє відображати відеопотік з камери в реальному часі всередині вікна програми, забезпечуючи зручний і наочний інтерфейс для користувача. Таким чином, *tkinter* виконує роль основного інтерфейсного модуля, забезпечуючи інтуїтивну взаємодію користувача із системою, наочне відображення відеопотоку та повідомлень, а також керування всіма основними функціями програми (рис. 3.8).

```
        # Права колонка
        self.form_card = tk.Frame(self.main_frame, bg="#2B2B2B", bd=3, relief="ridge", padx=30, pady=25)
        self.form_card.pack(side="right", fill="y", padx=15, pady=15)

        # Кнопки зверху
        self.button_frame = tk.Frame(self.form_card, bg="#2B2B2B")
        self.button_frame.pack(pady=(5, 15))

        btn_style = {"font": ("Segoe UI", 13, "bold"), "width": 16, "height": 1, "bd": 0,
                     "relief": "flat", "cursor": "hand2", "fg": "white"}

        self.login_button = tk.Button(self.button_frame, text="LOGIN", bg="#00ADB5",
                                      activebackground="#00CED1", command=self.show_login_form, **btn_style)
        self.login_button.grid(row=0, column=0, padx=10)

        self.register_button = tk.Button(self.button_frame, text="REGISTER", bg="#393E46",
                                         activebackground="#50555C", command=self.show_register_form, **btn_style)
        self.register_button.grid(row=0, column=1, padx=10)

        self.delete_button = tk.Button(self.button_frame, text="DELETE ACCOUNT", bg="#FF4444", fg="white",
                                       font=("Segoe UI", 13, "bold"), width=36, height=2,
                                       command=self.toggle_delete_form)
        self.delete_button.grid(row=1, column=0, columnspan=2, pady=(15,0))
```

Рисунок 3.8 - Генерація користувацького інтерфейсу

Бібліотека *cv2 (OpenCV)* є ключовим інструментом для роботи з відеопотоками та обробки зображень у нашій біометричній системі аутентифікації. Вона дозволяє підключатися до вебкамери, отримувати кадри в реальному часі та обробляти їх для подальшого аналізу. В нашому застосунку *cv2.VideoCapture(0)* відкриває основну вебкамеру (рис. 3.9).

```
37          self.cap = cv2.VideoCapture(0)
38          if not self.cap.isOpened():
39              messagebox.showerror("Camera Error", "Cannot open camera.")
40          self.most_recent_capture_arr = None
41          self.most_recent_capture_pil = None
42          self._start_main_camera_loop()
```

Рисунок 3.9 - Відкриття вебкамери

Після відкриття вебкамери за допомогою *cap.read()* з кожного кадру зчитується зображення, яке можна аналізувати або відображати користувачу (рис. 3.10).

```
89      # Камера
90      def _start_main_camera_loop(self):
91          ret, frame = self.cap.read()
92          if ret:
93              self.most_recent_capture_arr = frame
94              rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
95              self.most_recent_capture_pil = Image.fromarray(rgb)
96              imgtk = ImageTk.PhotoImage(image=self.most_recent_capture_pil)
97              self.webcam_label.imgtk = imgtk
98              self.webcam_label.configure(image=imgtk)
99          self.webcam_label.after(30, self._start_main_camera_loop)
```

Рисунок 3.10 - Зчитування зображення

Кожен кадр конвертується з формату BGR у RGB за допомогою *cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)*, оскільки бібліотека *Pillow*, яка використовується для показу зображень у *tkinter*, працює саме з RGB. Під час реєстрації користувача *cv2.imwrite()* зберігає фото обличчя у папку бази даних, що дозволяє формувати локальний набір зображень для подальшої біометричної обробки (рис. 3.11).

```
183         filename = os.path.join(DB_DIR, f"{login}.jpg")
184         cv2.imwrite(filename, self.most_recent_capture_arr)
185         self.users[login] = {"password": password}
186         with open(USERS_PATH, "w") as f:
187             json.dump(self.users, f, indent=4)
188         messagebox.showinfo("Success", f"User '{login}' registered successfully!")
189         self.hide_all_frames()
190
```

Рисунок 3.11 - Реєстрація користувача

OpenCV також забезпечує гнучкість і високу продуктивність завдяки оптимізації на *C/C++*, що робить обробку відеопотоку швидкою та ефективною навіть у реальному часі. Це дозволяє системі оперативно передавати кадри для аналізу бібліотекою *face_recognition*, перевіряти наявність обличчя на зображенні, а також візуально відображати користувачу результат у вікні програми. Таким чином, *cv2* є основним компонентом для роботи з камерою, обробки та конвертації зображень, забезпечуючи безперебійну передачу відеопотоку і підготовку кадрів для біометричної ідентифікації.

Бібліотека *Pillow (PIL)* використовується в програмі для конвертації та відображення зображень з *OpenCV* у формат, сумісний з *tkinter. Tkinter* не може напряму показати масиви з *OpenCV*, тому *Pillow* слугує своєрідним «мостом» між обробкою зображень і графічним інтерфейсом користувача.

Після того, як *OpenCV* отримує кадр з вебкамери і конвертує його у формат *RGB (cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)),* цей масив передається в *Image.fromarray(rgb)* (рис. 3.12), що перетворює масив (numpy) на об’єкт зображення *PIL*.

```
89      # Камера
90      def _start_main_camera_loop(self):
91          ret, frame = self.cap.read()
92          if ret:
93              self.most_recent_capture_arr = frame
94              rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
95              self.most_recent_capture_pil = Image.fromarray(rgb)
96              imgtk = ImageTk.PhotoImage(image=self.most_recent_capture_pil)
97              self.webcam_label.imgtk = imgtk
98              self.webcam_label.configure(image=imgtk)
99          self.webcam_label.after(30, self._start_main_camera_loop)
100
```

Рисунок 3.12 - Перетворення масиву на об’єкт зображення для *PIL*

Далі для відображення в *tkinter* використовується *ImageTk.PhotoImage(image=...)* (рис. 3.13), який створює сумісний формат, який можна вставити у Label чи інший графічний віджет.

```
89      # Камера
90      def _start_main_camera_loop(self):
91          ret, frame = self.cap.read()
92          if ret:
93              self.most_recent_capture_arr = frame
94              rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
95              self.most_recent_capture_pil = Image.fromarray(rgb)
96              imgtk = ImageTk.PhotoImage(image=self.most_recent_capture_pil)
97              self.webcam_label.imgtk = imgtk
98              self.webcam_label.configure(image=imgtk)
99          self.webcam_label.after(30, self._start_main_camera_loop)
```

Рисунок 3.13 - Створення сумісного формату

Pillow також дозволяє виконувати базові операції з зображеннями, такі як зміна розміру, обрізка, обертання та конвертація форматів, що необхідно для підготовки кадрів перед обробкою бібліотекою *face_recognition*. Завдяки цьому користувач бачить у вікні програми реальне відео з вебкамери в оптимальному розмірі та форматі, а система одночасно може виконувати біометричний аналіз.

Таким чином, *Pillow* забезпечує плавне відображення кадрів з камери в інтерфейсі та дає можливість коректно обробляти і підготовлювати зображення для розпізнавання облич у реальному часі.

Бібліотека *face_recognition* є центральним компонентом біометричної системи аутентифікації, оскільки відповідає за ідентифікацію користувачів за обличчям. Вона побудована на основі потужної бібліотеки *dlib* та використовує нейронні мережі для виявлення і аналізу облич, що значно спрощує роботу розробника, оскільки не потрібно тренувати власні моделі.

Після того, як кадр з вебкамери оброблений через *OpenCV* і перетворений у формат RGB для сумісності з *tkinter* і *Pillow*, *face_recognition* знаходить на зображенні всі обличчя і створює для кожного числовий вектор - так званий «ембедінг», який унікально описує риси обличчя користувача.

Для цього використовується функція *face_recognition. face_encodings(image)* (рис. 3.14), яка повертає 128-елементний вектор.

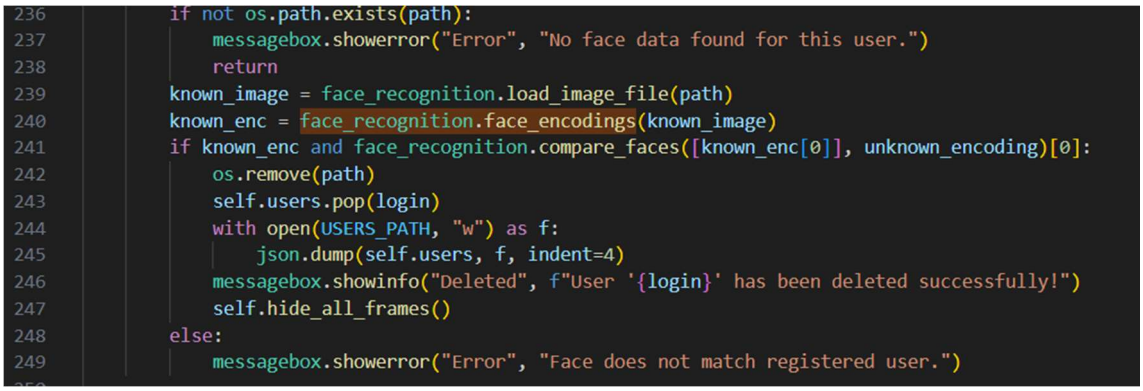


Рисунок 3.14 - Створення ембендінгу

Після створення ембедінгу програма порівнює його з вже збереженими шаблонами користувачів у базі даних за допомогою *face_recognition.compare_faces([known_enc[0]], unknown_encoding* (рис. 3.15). Якщо збіг знайдено, користувач допускається до системи. При реєстрації бібліотека не зберігає векторні представлення напряму, а використовується зображення, яке потім при вході перетворюється на ембедінг для порівняння з поточним кадром.

Рисунок 3.15 - Порівняння ембедінгу з збереженими шаблонами

Цей підхід забезпечує високий рівень безпеки, оскільки ембедінг не дозволяє відновити первинне фото, і водночас дозволяє ефективно перевіряти відповідність облич у реальному часі. Бібліотека *face_recognition* поєднує простоту використання, швидкість і точність розпізнавання, що робить її

оптимальним вибором для локальних біометричних систем та навчальних проєктів.

Бібліотека *subprocess* у нашій біометричній системі використовується для взаємодії програми з операційною системою на більш низькому рівні, зокрема для запуску зовнішніх процесів або відкриття файлів та папок. Вона дозволяє програмі виконувати команди так, якби користувач сам їх вводив у командний рядок, що робить можливим інтегрування функціоналу ОС без додаткових зовнішніх програмних інтерфейсів.

У конкретному застосунку після успішної аутентифікації користувача бібліотека *subprocess* відкриває певну директорію на комп'ютері, яка була задана в налаштуваннях системи, наприклад *D:\PC*. Це реалізується через виклик *subprocess.Popen* (рис. 3.16). Команда *cmd /c start "" "{OPEN_FOLDER_PATH}"* відкриває вікно Провідника Windows у зазначеній папці, а параметр *shell=True* дозволяє виконати команду безпосередньо через оболонку Windows.

```
209         known_image = face_recognition.load_image_file(path)
210         known_enc = face_recognition.face_encodings(known_image)
211         if known_enc and face_recognition.compare_faces([known_enc[0]], unknown_encoding)[0]:
212             messagebox.showinfo("Welcome", f"Welcome, {login}!")
213             with open(LOG_PATH, "a", encoding="utf-8") as f:
214                 f.write(f"{login},{datetime.datetime.now()},in\n")
215             if os.path.exists(OPEN_FOLDER_PATH):
216                 subprocess.Popen(f'cmd /c start "" "{OPEN_FOLDER_PATH}"', shell=True)
217             self.hide_all_frames()
218         else:
219             messagebox.showerror("Error", "Face does not match registered user.")
220
```

Рисунок 3.16 - Відкриття дерикторії

Таким чином, *subprocess* забезпечує плавну інтеграцію біометричної системи з операційною системою користувача, дозволяючи автоматично відкривати потрібні ресурси після успішного входу. Використання цієї бібліотеки робить роботу програми більш гнучкою і зручною для кінцевого користувача, оскільки дії після аутентифікації виконуються автоматично і без додаткових ручних дій. Повний код програмної реалізації запропонованої системи біометричної ідентифікації представлено в додатку Б.

3.3 Практична реалізація біометричної системи ідентифікації користувачів

Після запуску програми відбувається ініціалізація графічного інтерфейсу і на екрані відкривається головне вікно, у якому розташовано назву системи, область для відображення відеопотоку з вебкамери та три основні кнопки керування: LOGIN, REGISTER і DELETE ACCOUNT. Одразу під час запуску програми активується вебкамера, яка починає зчитувати відеокадри у режимі реального часу. Отримані зображення проходять конвертацію в зручний формат та безперервно відображаються в інтерфейсі, що створює ефект живого відео (рис. 3.17).

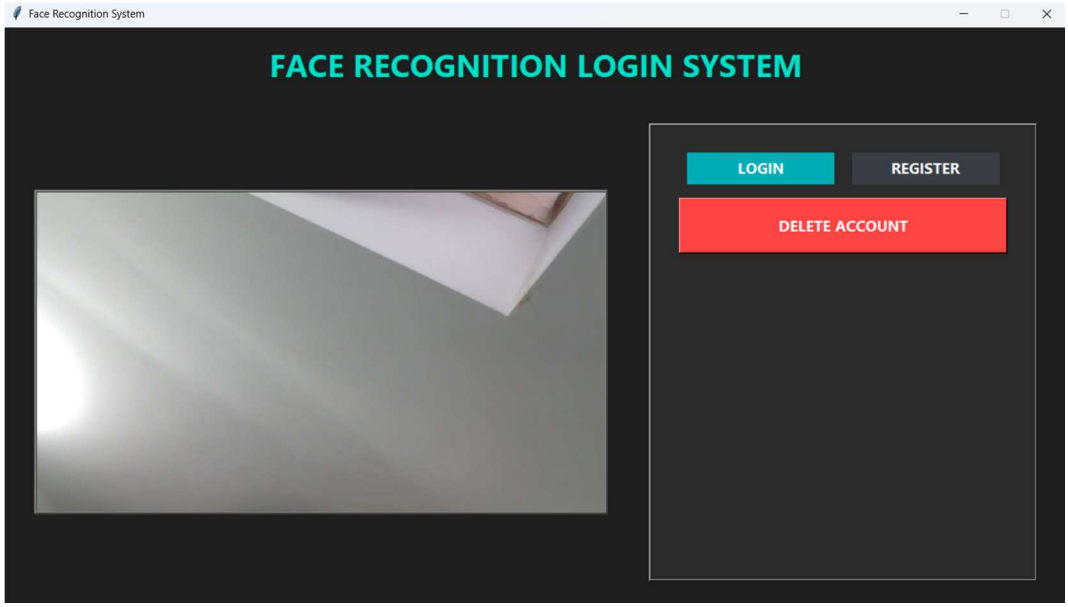


Рисунок 3.17 - Головне вікно програми

Реєстрація нового користувача є першим і критично важливим етапом функціонування біометричної системи. Вона дозволяє сформувати базу даних облікових записів, включно з біометричними даними, та забезпечує подальшу безпечну авторизацію.

Процес реєстрації починається після натискання кнопки REGISTER у головному вікні програми. Після цього відкривається форма для введення нового облікового запису, де користувач вводить свій логін та пароль. Ця перевірка необхідна для того, щоб ідентифікувати користувача у майбутньому та забезпечити можливість відновлення доступу, якщо це буде потрібно.

Після введення облікових даних система активує камеру за допомогою бібліотеки *OpenCV (cv2),* яка забезпечує захоплення відеопотоку в реальному часі. Користувачеві пропонується розташувати своє обличчя перед камерою, і програма робить один або декілька кадрів, щоб зберегти зображення обличчя (рис. 3.18).

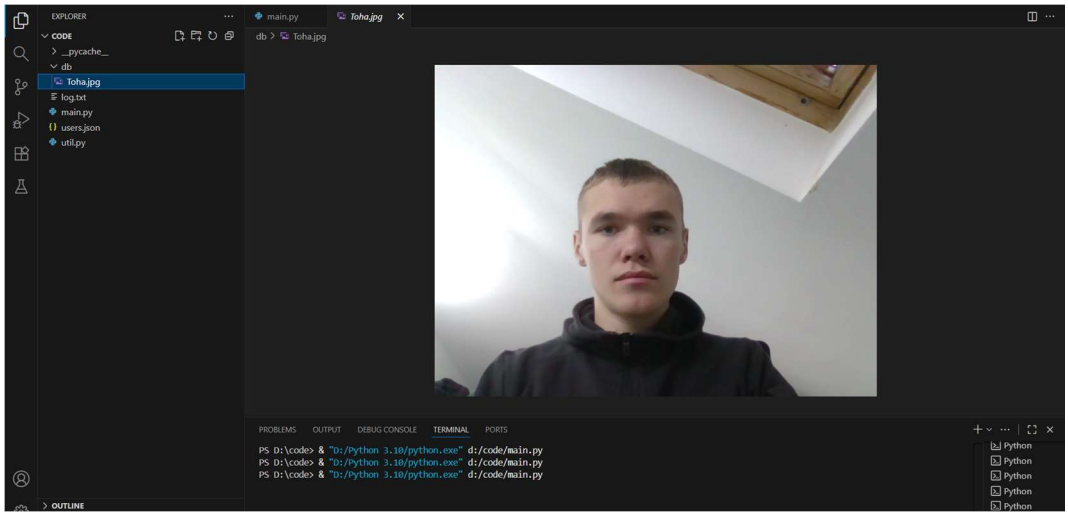


Рисунок 3.18 - Зберігання зображення обличчя

Збережене зображення програма конвертує у формат RGB для сумісності з бібліотекою face_recognition, після чого може бути створений цифровий вектор (encoding) у майбутніх етапах аутентифікації. На цьому етапі саме зображення зберігається у спеціальній папці db, наприклад, у даній програмній реалізації використовується файл *db/Toha.jpg*.

Після успішного збереження фотографії система додає запис користувача у файл *users.json*, де зберігаються всі логіни та паролі зареєстрованих користувачів (рис. 3.19). Зберігання паролю в хеші дозволяє не тримати його у відкритому вигляді, тому навіть у разі витоку бази даних зловмисник не побачить справжній пароль, а лише результат одностороннього перетворення. Хеш неможливо повернути назад у пароль, тому це значно ускладнює крадіжку даних. Я використав алгоритм SHA-256, він має високу криптографічну стійкість, не дозволяє відновити початкові дані з хешу й забезпечує стабільний, унікальний результат для кожного вхідного значення. Алгоритм добре захищений від колізій, працює швидко, широко підтримується в різних системах і вважається надійним для перевірки цілісності даних та цифрових підписів.

Рисунок 3.19 - Зберігання даних користувача в файлі

Це дозволяє створити централізовану базу для подальшої авторизації та ведення журналу активності користувачів. При записі даних програма забезпечує збереження структури *JSON* у зручному для читання форматі з відступами, що полегшує перегляд або редагування файлу вручну при необхідності.

Після успішного завершення усіх дій інформація про користувача додається у базу даних

Водночас після успішного завершення усіх дій користувачеві виводиться повідомлення про успішну реєстрацію в користувацькому інтерфейсі, наприклад “User ‘Toha’ registered successfully” (рис. 3.20).

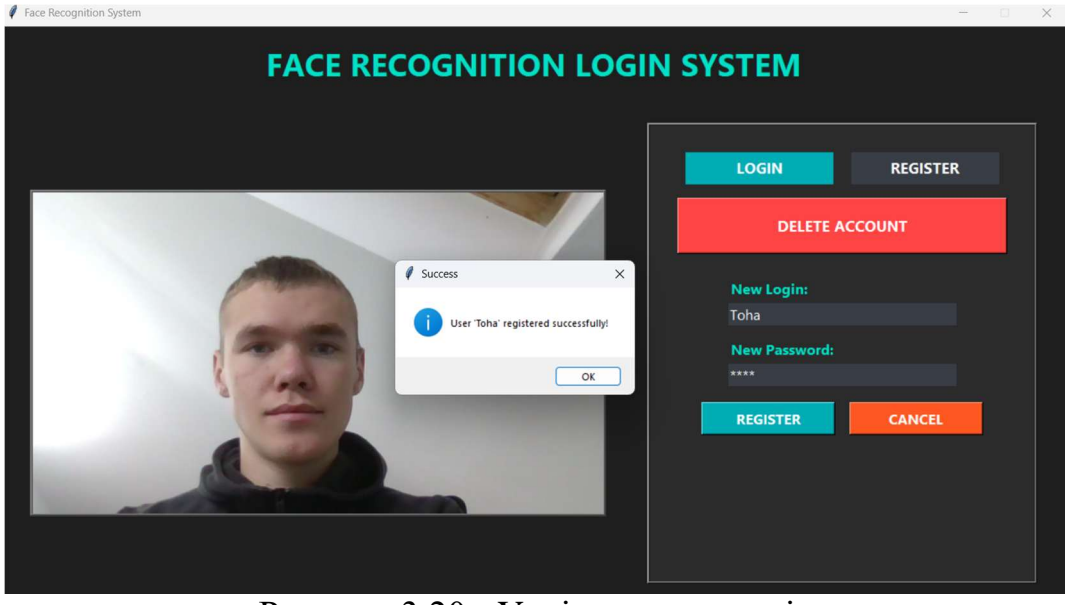


Рисунок 3.20 - Успішна реєстрація

Це підтверджує, що система успішно зберегла всі необхідні дані для подальшої аутентифікації, а також сигналізує користувачу, що обліковий запис готовий до використання.

Додатково варто відзначити, що на цьому етапі система також може проводити перевірку якості зображення, наприклад визначати, чи обличчя знаходиться повністю у кадрі, чи достатньо освітлення та чи немає перешкод, що закривають обличчя. Такі перевірки підвищують точність майбутньої аутентифікації і запобігають помилкам при вході.

Таким чином, процес реєстрації нового користувача поєднує в собі класичну створення облікового запису через логін і пароль із сучасним підходом біометричної фіксації обличчя. Це дозволяє системі забезпечити високий рівень безпеки і точності при подальшій авторизації, а також надає користувачу зручний і зрозумілий спосіб створення облікового запису.

Авторизація є ключовим етапом роботи біометричної системи, оскільки саме на цьому етапі визначається, чи має конкретний користувач доступ до системи. У створеній програмі процес авторизації включає кілька взаємопов’язаних кроків, що поєднують традиційну перевірку облікових даних і біометричну перевірку обличчя.

Після натискання кнопки LOGIN у головному вікні користувачеві відкривається форма введення логіну та пароля. Перший крок авторизації полягає у перевірці цих даних. Програма зчитує файл *users.json*, де зберігаються всі зареєстровані облікові записи, і порівнює введені значення з наявними. Ця перевірка дозволяє відсікти випадки спроб входу сторонніми особами, які могли дізнатися пароль, але не є власниками облікового запису. Якщо логін або пароль не збігаються, система негайно повідомляє про помилку і припиняє процес авторизації.

Після успішної перевірки облікових даних програма переходить до другого рівня безпеки - біометричної перевірки обличчя. Камера активується, і програмне забезпечення отримує поточний кадр користувача. Зображення конвертується з формату BGR у RGB за допомогою *OpenCV*, щоб його можна було передати у функції бібліотеки *face_recognition*. Бібліотека створює цифровий вектор (encoding), який описує унікальні риси обличчя користувача. Потім цей вектор порівнюється зі збереженим зображенням, яке було отримано під час реєстрації. Алгоритм порівняння враховує всі ключові точки обличчя,

включаючи очі, ніс, рот, контур обличчя та просторові співвідношення між ними. У разі успішного збігу система підтверджує особу користувача і надає доступ до програми. На екран виводиться повідомлення “Welcome, [ім’я користувача]” (рис. 3.21).

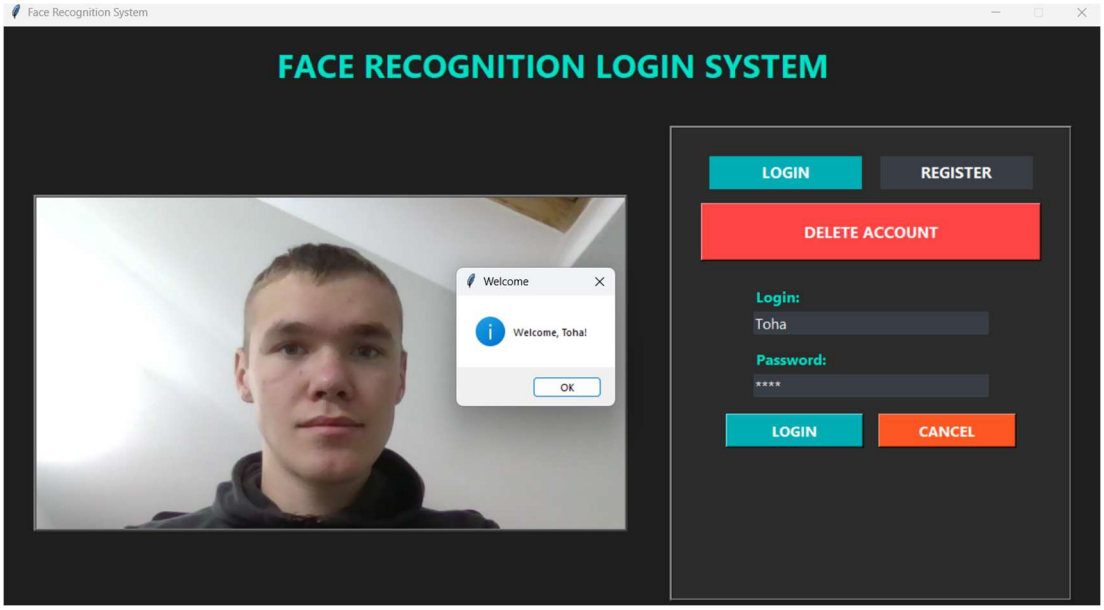


Рисунок 3.21 - Успішна аутентифікація

Факт входу фіксується у файлі *log.txt* із зазначенням дати та часу (рис. 3.22).

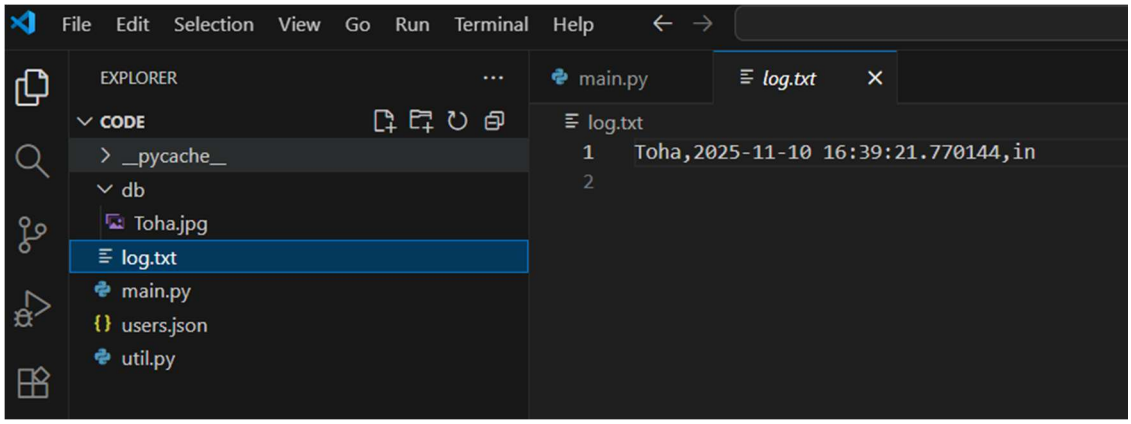


Рисунок 3.22 - Фіксація входу

Ця функція дозволяє вести журнал активності, що важливо для безпеки та аудиту. Такий двоетапний підхід - спершу перевірка облікових даних, потім біометрична ідентифікація - дозволяє значно підвищити надійність системи,

оскільки для доступу недостатньо знати тільки пароль, необхідне фізичне підтвердження особи. Крім того, він зменшує ризик шахрайства, що включає використання фотографій, відео чи масок, оскільки реальний користувач має бути присутнім перед камерою. Успішна авторизація також може запускати додаткові дії, наприклад відкривати конкретні папки або програми на комп'ютері користувача, що демонструє ефективну інтеграцію біометричного контролю з робочим середовищем (рис. 3.23).

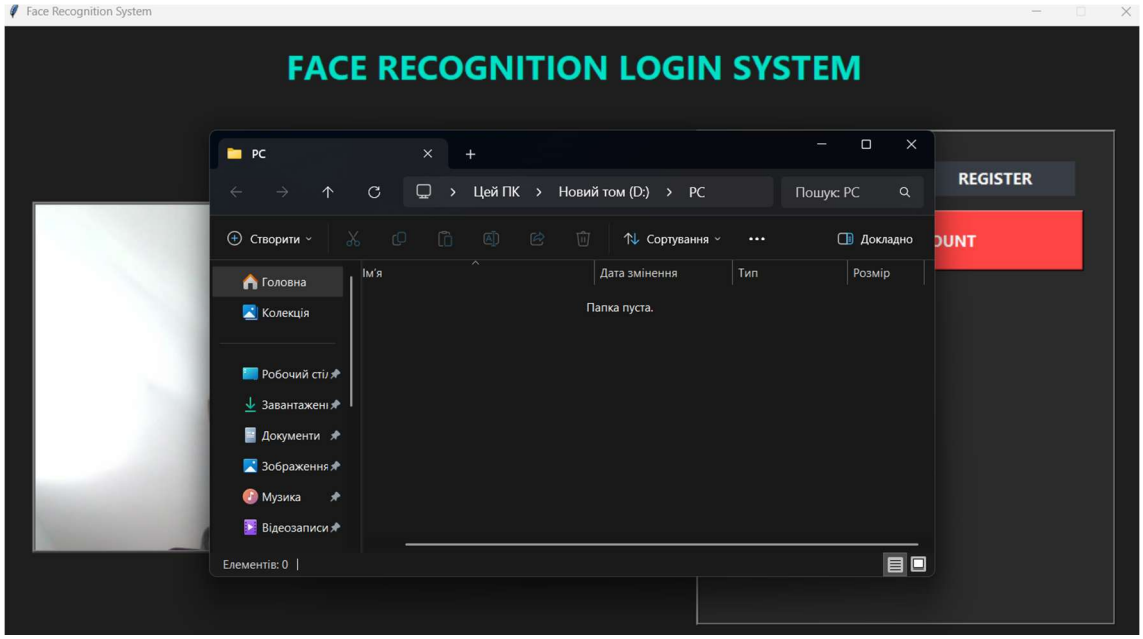


Рисунок 3.23 - Відкриття папки після успішного входу

Таким чином, авторизація користувача у розробленій системі є багаторівневою, поєднує класичну перевірку облікових даних і сучасну біометричну ідентифікацію, забезпечуючи високий рівень безпеки та зручність використання.

Перевірка наявності та видимості обличчя Одним із ключових етапів біометричної аутентифікації є перевірка того, чи присутнє обличчя користувача у кадрі та наскільки воно чітко видно. Цей процес є критично важливим для забезпечення точності і безпеки системи, оскільки будь-які помилки на цьому етапі можуть призвести до невірної аутентифікації або до спроб обману системи. Після введення облікових даних і натискання кнопки LOGIN, програма активує камеру та зчитує кадр у реальному часі за допомогою бібліотеки *OpenCV (cv2)*.

Отримане зображення спочатку конвертується з формату BGR у RGB, оскільки бібліотека *face_recognition*, яка відповідає за біометричне розпізнавання, працює саме з RGB.

На наступному етапі кадр передається до функції *face_recognition.face_encodings(),* яка аналізує зображення і шукає ключові точки обличчя користувача. Ця функція визначає такі критично важливі особливості, як положення очей, носа, рота та контури обличчя, після чого формує унікальний цифровий вектор (encoding). Якщо система не знаходить жодного обличчя, функція повертає порожній результат. Це може трапитися якщо обличчя користувача закрите рукою, маскою або іншими предметами, обличчя знаходиться поза кадром або частково зникло через неправильне положення камери, недостатнє освітлення або тінь на обличчі ускладнює виявлення ключових точок, дуже низька якість кадру (розмиття, шум) або обличчя користувача повернене під екстремальним кутом. У випадку відсутності або часткової видимості обличчя система відразу виводить повідомлення “No face detected” і блокує доступ до подальшої аутентифікації (рис. 3.24).

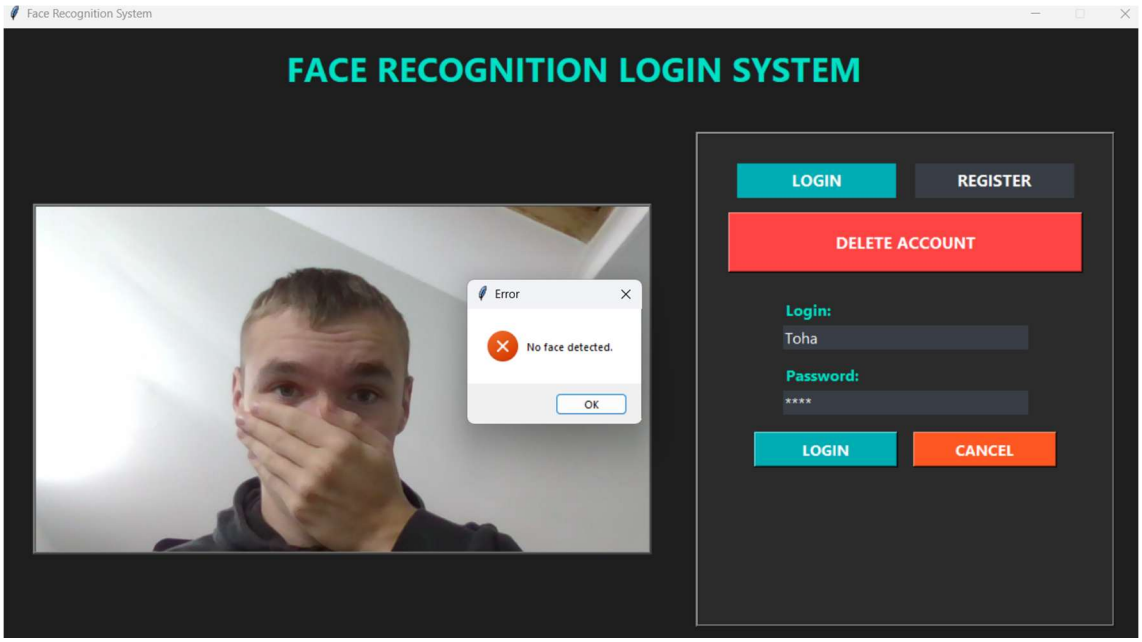


Рисунок 3.24 - Невдала аутентифікація

Це забезпечує високий рівень безпеки, оскільки підтвердження особи можливе лише тоді, коли камера чітко бачить обличчя користувача. Якщо ж

обличчя визначене правильно, програма порівнює отриманий вектор з ембедінгом, збереженим під час реєстрації. Тільки після успішного збігу користувач допускається до системи, а факт входу фіксується у лог-файлі. Додатково, перевірка наявності обличчя дозволяє попереджати користувача про потенційні проблеми, такі як неправильно розташована камера, недостатнє освітлення або про предмети, що закривають обличчя. Це підвищує зручність користування та зменшує ризик помилкових відмов при аутентифікації. Таким чином, перевірка наявності та видимості обличчя є критичною для забезпечення надійності системи, оскільки вона є першим етапом біометричного захисту, який гарантує, що подальша обробка даних відбувається тільки при правильних і безпечних умовах.

Функція видалення облікового запису реалізована таким чином, щоб максимально захистити персональні та біометричні дані користувача. Вона складається з кількох етапів перевірки та повного очищення інформації про користувача з системи. Процес починається з того, що користувач у головному вікні програми натискає кнопку DELETE ACCOUNT, після чого на екрані з’являється окрема форма для підтвердження дії.

У цьому вікні користувачеві потрібно ввести свій логін і пароль. Це перший рівень перевірки, який дозволяє переконатися, що запит на видалення надходить від справжнього власника облікового запису. Після введення даних програма порівнює отримані значення з інформацією, збереженою у файлі users.json. Якщо логін або пароль не збігаються з наявними даними, процес негайно припиняється, а користувач отримує повідомлення про помилку. Це запобігає можливості несанкціонованого видалення.

Якщо логін і пароль введено правильно, система переходить до другого, значно важливішого етапу - перевірки обличчя. В цей момент камера активується, знімає поточний кадр, а бібліотека *face_recognition* аналізує його, формуючи біометричний вектор (encoding). Отриманий вектор порівнюється зі збереженим зображенням користувача, яке знаходиться в папці *db.*

Тільки якщо збіг є достовірним, система дозволяє виконати видалення облікового запису. Це гарантовано захищає користувача від ситуацій, у яких

стороння особа могла б дізнатися його пароль, але не має доступу до його обличчя. Якщо обличчя не розпізнано - процес переривається, а система повідомляє про помилку Після успішної ідентифікації програма переходить до безпосереднього видалення даних. На цьому етапі виконуються такі дії:

1. Видалення біометричного зображення користувача. Система знаходить файл із фотографією (наприклад, *db/Toha.jpg*) та видаляє його з диска. Це забезпечує повне очищення біометричної інформації.

2. Оновлення файлу *users.json.* Програма відкриває файл, у якому зберігаються всі зареєстровані користувачі, видаляє відповідний запис та зберігає оновлені дані.

3. Виведення підтвердження на екран. Після завершення всіх операцій користувач отримує повідомлення “User deleted successfully”, яке підтверджує, що обліковий запис було успішно видалено (рисунок 3.25).

Рисунок 3.25 демонструє фінальне повідомлення, яке бачить користувач після успішного виконання операції.

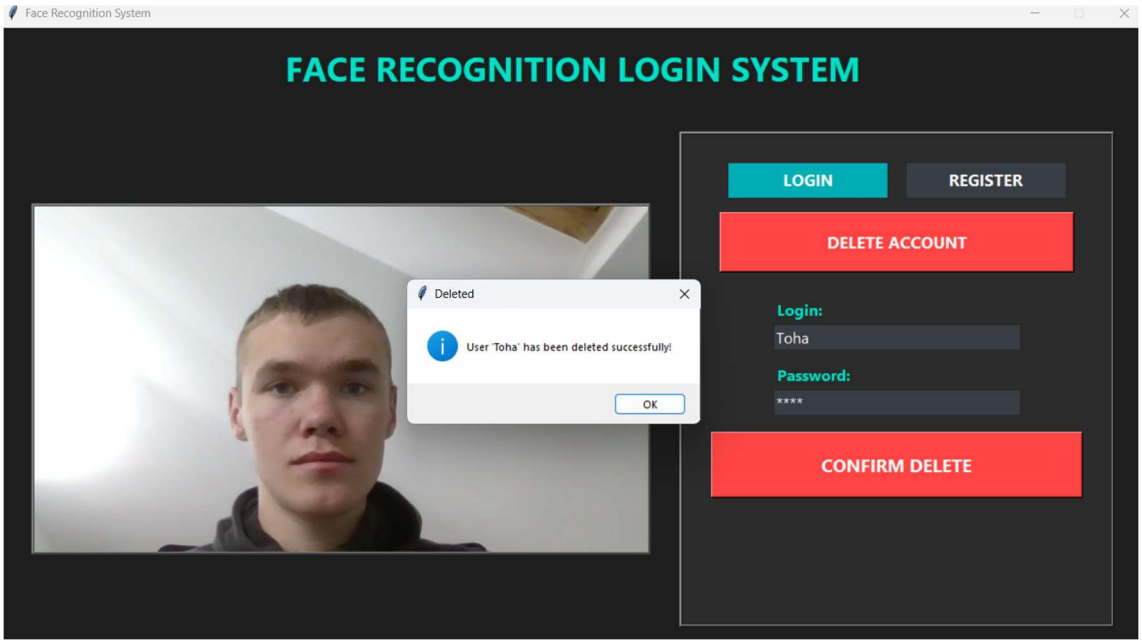


Рисунок 3.25 - Успішне видалення

Одним із ключових елементів біометричної системи є модуль, що забезпечує передачу і відображення відеопотоку від вебкамери в головному вікні програми. Його робота базується на постійному отриманні кадрів з камери, їх

обробці та виведенні на екран з мінімальною затримкою. Завдяки цьому користувач бачить себе у режимі реального часу, що значно підвищує зручність взаємодії та точність виконання біометричних процедур. Робота модуля продемонстрована на рисунку 3.26.

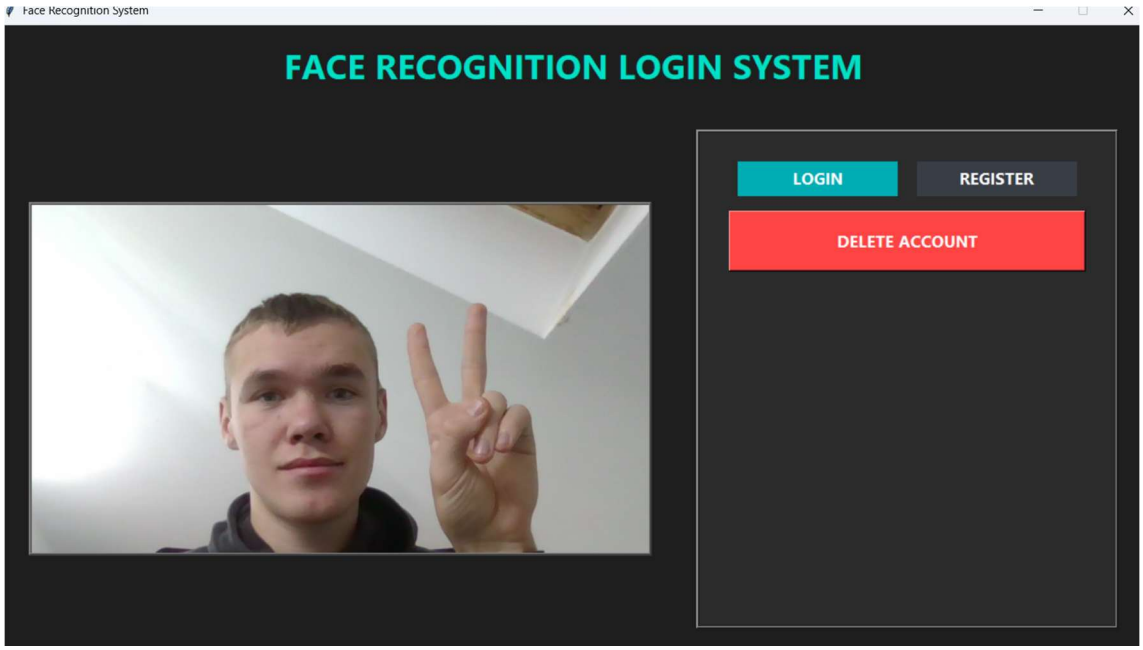


Рисунок 3.26 - Зображення в реальному часі

Після ініціалізації програми бібліотека *OpenCV (cv2)* активує вебкамеру, створюючи вхідний потік зображень. Кожен відеокадр, який надходить із камери, має формат BGR - стандартне внутрішнє представлення кольорів у *OpenCV*. Однак у графічному інтерфейсі tkinter використовується формат RGB, тому кожен кадр проходить попередню конвертацію з BGR у RGB. Ця операція є обов'язковою, оскільки без неї кольори на екрані відображалися б неправильно - із синіми та червоними компонентами, розташованими навпаки.

Після конвертації кадр, завдяки модулю *PIL.ImageTk*, транслюється в інтерфейсі. Кадр вставляється в елемент *Label* або *Canvas*, який і відповідає за відображення потокового відео.

Для забезпечення плавності та безперервності відображення використовується цикл оновлення кадрів, що працює через метод *tkinter after()*. Він виконує функцію, яка відповідає за захоплення і показ нового кадру приблизно кожні 30 мілісекунд, тобто із частотою близько 30 кадрів за секунду.

Така частота є достатньою для комфортного сприйняття руху та для точної роботи алгоритмів розпізнавання обличчя.

У кожному новому циклі виконуються такі дії:

1. Зчитується щойно отриманий кадр із вебкамери;
2. Кадр перетворюється в потрібний колірний формат;
3. Зображення оновлює попередній кадр на екрані;
4. Запускається наступне оновлення через 30 мс.

Оскільки весь процес відбувається без необхідності повного перезапуску інтерфейсу, відеопотік виглядає плавним і природним. Користувач може легко змінити положення, підійти ближче чи віддалитися від камери, контролюючи те, як програма «бачить» його обличчя. Це особливо важливо під час реєстрації та аутентифікації, коли система повинна мати чіткий та якісний кадр для коректного розпізнавання.

Крім цього, відображення в реальному часі дозволяє побачити й оцінити зовнішні фактори, що можуть впливати на якість розпізнавання - наприклад, недостатнє освітлення, надмірну тінь, неправильний кут зйомки або часткове закриття обличчя. Користувач може відразу виправити такі моменти, не чекаючи повідомлення про помилку.

Таким чином, модуль відображення зображення в реальному часі забезпечує не лише візуальний комфорт користувача, але й стабільну роботу біометричних алгоритмів, створюючи основу для точної та надійної ідентифікації.

У процесі побудови системи біометричної автентифікації було створено програмий додаток з простим графічним інтерфейсом у якому користувач одразу бачить зображення з камери, може взаємодіяти з системою в реальному часі та виконувати основні дії, такі як реєстрацію, вхід або видалення облікового запису.

Під час реєстрації камера автоматично робить фото обличчя, а система створює його цифровий шаблон, який використовується під час перевірки особи. Усі дані зберігаються в локальній базі, тому система працює автономно і не залежить від зовнішніх серверів.

Аутентифікація поєднує пароль та розпізнавання обличчя, що робить систему значно безпечнішою. Вхід дозволяється тільки тоді, коли камера чітко бачить обличчя користувача. Це не дає можливості обманути програму за допомогою спотворених кадрів.

Усі спроби авторизації записуються в журнал подій, що робить роботу системи більш прозорою. Важливою функцією є й можливість видалення облікового запису, яке потребує повторної перевірки обличчя. Це захищає дані від випадкового чи небажаного видалення.

Під час роботи програма постійно оновлює відеопотік з невеликою затримкою, тому зображення в інтерфейсі виглядає плавно і природно. Загалом практична частина показує, що створена система не тільки працює стабільно, але й є зручною для користувача. Вона поєднує сучасні методи комп’ютерного зору та зрозумілі інструменти керування даними. Така система може стати основою для актуальних рішень у сфері контролю доступу і з часом може бути доповнена новими видами біометрії або іншими механізмами безпеки.

ВИСНОВКИ

У кваліфікаційній роботі було розв'язано актуальну задачу підвищення надійності та захищеності систем аутентифікації шляхом впровадження біометричних методів, стійких до спуфінг-атак.

При цьому отримано наступні результати:

1. Проведено аналіз механізмів аутентифікації який показав, що сучасні системи контролю доступу вимагають переходу до багатофакторних рішень та автономної обробки конфіденційних біометричних даних. Було визначено критичні вразливості, пов'язані з компрометацією шаблонів та атаками обману (спуфінг), це зумовило необхідність інтеграції додаткових спеціалізованих захисних механізмів.

2. Проведено дослідження загроз конфіденційності яке виявило, що основною вимогою до захищеної біометричної системи є локальне та зашифроване зберігання шаблонів. Запропонована архітектура забезпечує незалежність від зовнішніх мереж, що мінімізує ризик витоку даних.

3. Розроблено алгоритм аутентифікації який містить надійну двофакторну схему (пароль + розпізнавання обличчя), що значно підвищує поріг відкидання несанкціонованого доступу порівняно з однофакторними рішеннями.

4. Запропоновано механізм виявлення обману, який базується на аналізі чіткості обличчя у відеопотоці, що дозволило ефективно протидіяти спуфінг-атакам із використанням статичних зображень.

5. Проведене експерементальне дослідження багатофакторної аутентифікації підтвердило, що комбінування біометричного фактору з парольним фактором є оптимальним підходом для підвищення безпеки у системах контролю доступу.

6. Розроблена система та її програмний прототип відповідають сучасним вимогам захисту даних, є стабільними, зручними для користувача та забезпечують захист конфіденційності та цілісності біометричних даних, підтверджуючи свою практичну цінність для використання як автономні рішення у критичній інфраструктурі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петренчук, А., Дзівак О. Системи аутентифікацій на основі біометричних данних. Захист інформації: Збірник матеріалів науково-практичного симпозіуму, 30.11.2024. – Тернопіль, 2024. – С. 25–27.
2. Петренчук, А., Кулина С. Системи аутентифікації на основі біометричних даних. Інформаційно-комп'ютерні технології: Матеріали XV Міжнар. наук.-техн. конф., 28–29 березня 2025. – Житомир, 2025. – С. 141–142.
3. Пташенко, О. В., Пастушенко, А. О., Імнадзе, І. Н., & Солдатова, А. А. (2021). Тенденції розвитку глобальних ринків в умовах цифровізації. *Вісник Східноукраїнського національного університету імені Володимира Даля*, (6 (270)), 131-134.
4. Ryu, R., Yeom, S., Kim, S. H., & Herbert, D. (2021). Continuous multimodal biometric authentication schemes: a systematic review. *IEEe Access*, *9*, 34541-34557.
5. Jain, A., Bolle, R., & Pankanti, S. (2011). Introduction to biometrics. In *Biometrics: personal identification in networked society* (pp. 1-41). Boston, MA: Springer US.
6. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, *14*(1), 4-20.
7. Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. *Computers and Electrical Engineering*, *119*, 109485.
8. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. London: Springer London.
9. Marani, M., Soltani, M., Bahadori, M., Soleimani, M., & Moshayedi, A. (2023). The role of biometric in banking: A review. *EAI Endorsed Transactions on AI and Robotics*, *2*(1), 1-15.

10. Muratuly, D., Denissova, N. F., Krak, Y. V., & Apayev, K. S. (2022). Biometric authentication of students to control the learning process in online education. *Scientific Journal of Astana IT University*.
11. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20.
12. Gomez-Barrero, M., Galbally, J., Rathgeb, C., & Busch, C. (2017). General framework to evaluate unlinkability in biometric template protection systems. *IEEE Transactions on Information Forensics and Security*, *13*(6), 1406-1420.
13. Журавель, Ю. І., & Лісовський, Б. В. (2025). Аналіз моделей та алгоритмів автентифікації на основі біометричних даних. *Сучасний захист інформації*, (2), 51-58.
14. Т М, М., Капелюшна, Т. В., Якименко, Ю. М., Будзинський, О. В., & Ніколабай, А. О. (2025). Показники FRR і FAR як критерії оцінювання надійності біометричних методів. *Сучасний захист інформації*, (1), 98-104.
15. Ali, H. S., Elhefnawy, E. I., & Abo-Zahhad, M. (2024). Cancelable palmprint: intelligent framework toward secure and privacy-aware recognition system. *EURASIP Journal on Information Security*, *2024*(1), 31.
16. White, B. (2024). Tailoring Biometric Innovation to Privacy Law in the Retail Industry. *SMU Sci. & Tech. L. Rev.*, *27*, 343.
17. Бойко А. Міжнародне законодавство та принципи у сфері захисту біометричних персональних даних. *EVROPSKÝ POLITICKÝ A PRÁVNÍ DISKURZ* , 52.
18. Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, *143*, 113114.
19. Guo, J., Mu, H., Liu, X., Ren, H., & Han, C. (2024). Federated learning for biometric recognition: a survey. *Artificial Intelligence Review*, *57*(8), 208.

20. Nechyporenko, O., & Korpan, Y. (2017). Analysis of methods and technologies of human face recognition. *Технологический аудит и резервы производства*, *5*(2 (37)), 4-10.
21. Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). A review of homomorphic encryption for privacy-preserving biometrics. *Sensors*, *23*(7), 3566.
22. Jain, A. K., & Kumar, A. (2012). Biometric recognition: an overview. *Second generation biometrics: The ethical, legal and social context*, 49-79.
23. Regulation, P. (2018). General data protection regulation. *Intouch*, *25*, 1-5.
24. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). Facenet: A unified embedding for face recognition and clustering. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 815-823).
25. Lee, J. C. (2012). A novel biometric system based on palm vein image. *Pattern Recognition Letters*, *33*(12), 1520-1528.
26. Kasprowski, P., Borowska, Z., & Harezlak, K. (2022). Biometric identification based on keystroke dynamics. *Sensors*, *22*(9), 3158.
27. Lee, M. W., & Wennblom, P. C. (2025). International standards for the Metaverse. In *Human-Centered Metaverse* (pp. 197-211). Morgan Kaufmann.
28. Utegen, D., & Rakhmetov, B. Z. (2023). Facial recognition technology and ensuring security of biometric data: Comparative analysis of legal regulation models. *Journal of Digital Technologies and Law*, *1*(3).
29. Jain, A., Bolle, R., & Pankanti, S. (2011). Introduction to biometrics. In *Biometrics: personal identification in networked society* (pp. 1-41). Boston, MA: Springer US.
30. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal*, *40*(3), 614-634.
31. Poehn, D., Grabatin, M., & Hommel, W. (2023). Analyzing the threats to blockchain-based self-sovereign identities by conducting a literature survey. *Applied Sciences*, *14*(1), 139.

32. Talreja, V., Valenti, M. C., & Nasrabadi, N. M. (2020). Deep hashing for secure multimodal biometrics. *IEEE Transactions on Information Forensics and Security*, *16*, 1306-1321.
33. Du, H., Shi, H., Zeng, D., Zhang, X. P., & Mei, T. (2022). The elements of end-to-end deep face recognition: A survey of recent advances. *ACM computing surveys (CSUR)*, *54*(10s), 1-42.
34. Gunetti, D., & Picardi, C. (2005). Keystroke analysis of free text. *ACM Transactions on Information and System Security (TISSEC)*, *8*(3), 312-347.

ДОДАТОК А

Таблиця А1

Ризики, загрози та шляхи мінімізації у біометричних системах

Категорія ризику	Проблеми та загрози	Приклади / пояснення	Шляхи мінімізації
Технічні загрози та вразливості	Атаки типу підробка (spoofing) Витік біометричних шаблонів Зниження точності в несприятливих умовах Помилки обладнання та алгоритмів	Імітація відбитка пальця, обличчя або голосу; 3D-маски, записи Бази даних потрапляють до зловмисників; неможливо змінити біометричні дані Погане освітлення, шум, травми, старіння Збої сенсорів, помилки програмного забезпечення, неправильне навчання AI	Виявлення живості (Liveness detection) (аналіз моргання очей, мікрорухів, температури шкіри) Шифрування шаблонів; децентралізоване зберігання; анонімізація даних Поліпшення алгоритмів та сенсорів; регулярне оновлення моделей Регулярний аудит та тестування; використання резервних способів аутентифікації
Проблеми конфіденційності та етики	Питання приватності Постійне стеження (Surveillance) Дискримінація (bias) Власність на дані	Незаконний збір/зберігання без згоди Системи розпізнавання облич у публічних місцях Упереджені алгоритми щодо кольору шкіри, віку, статі Невизначеність, хто відповідає за біометричні шаблони	Чіткі політики збору даних; прозорість Регулювання використання у громадських просторах Використання збалансованих тренувальних наборів; регулярна перевірка алгоритмів Законодавче уточнення власності та відповідальності
Правове регулювання	Недостатнє регулювання	Різні країни мають різні стандарти	Впровадження стандартів GDPR; створення незалежних органів контролю

прод. табл А1

Категорія ризику	Проблеми та загрози	Приклади / пояснення	Шляхи мінімізації
Соціальні ризики	Психологічний бар’єр Залежність від технологій Недовіра через попередні інциденти	Дискомфорт від “сканування” обличчя або голосу Втрата альтернативних способів ідентифікації Витоки даних у різних країнах	Освітні кампанії, пояснення користі та безпеки Наявність резервних методів доступу Прозорі механізми контролю та аудит систем
Шляхи мінімізації ризиків	Технічні Організаційні	Шифрування шаблонів, децентралізоване зберігання, анонімізація Прозорість, аудит, освіта	Зменшення шансів витоку або компрометації даних Підвищення довіри та обізнаності користувачів

ДОДАТОК Б

Код програмної реалізації

```
import os
import json
import datetime
import tkinter as tk
from tkinter import messagebox
import cv2
from PIL import Image, ImageTk
import face_recognition
import subprocess
import hashlib
import sys
OPEN_FOLDER_PATH = r"D:\PC"
DB_DIR = './db'
USERS_PATH = './users.json'
LOG_PATH = './log.txt'
class App:
    def __init__(self):
        self.main_window = tk.Tk()
        self.main_window.title("Face Recognition System")
        self.main_window.geometry("1200x650+300+100")
        self.main_window.configure(bg="#1E1E1E")
        self.main_window.resizable(False, False)
        tk.Label(self.main_window, text="FACE RECOGNITION LOGIN SYSTEM",
                 font=("Segoe UI", 26, "bold"), fg="#00E0C6", bg="#1E1E1E").pack(pady=15)
        self.main_frame = tk.Frame(self.main_window, bg="#1E1E1E")
        self.main_frame.pack(fill="both", expand=True, padx=20, pady=10)
        self.camera_frame = tk.Frame(self.main_frame, bg="#1E1E1E")
        self.camera_frame.pack(side="left", padx=15, pady=10)
        # використовуємо великий Label, але зображення буде підганятися
        self.webcam_label = tk.Label(self.camera_frame, bg="#000000", width=640, height=360,
relief="ridge", bd=3)
        self.webcam_label.pack(pady=15)
        self.cap = cv2.VideoCapture(0)
        if not self.cap.isOpened():
            messagebox.showerror("Camera Error", "Cannot open camera.")
        self.most_recent_capture_arr = None  # BGR numpy array від OpenCV
        self.most_recent_capture_pil = None  # PIL Image (RGB)
        self._start_main_camera_loop()
        self.form_card = tk.Frame(self.main_frame, bg="#2B2B2B", bd=3, relief="ridge", padx=30,
pady=25)
        self.form_card.pack(side="right", fill="y", padx=15, pady=15)
        self.button_frame = tk.Frame(self.form_card, bg="#2B2B2B")
        self.button_frame.pack(pady=(5, 15))
        btn_style = {"font": ("Segoe UI", 13, "bold"), "width": 16, "height": 1, "bd": 0,
                     "relief": "flat", "cursor": "hand2", "fg": "white"}
        self.login_button = tk.Button(self.button_frame, text="LOGIN", bg="#00ADB5",
                                      activebackground="#00CED1", command=self.show_login_form,
**btn_style)
        self.login_button.grid(row=0, column=0, padx=10)
```

```
        self.register_button = tk.Button(self.button_frame, text="REGISTER", bg="#393E46",
                                         activebackground="#50555C", command=self.show_register_form,
**btn_style)
        self.register_button.grid(row=0, column=1, padx=10)
        self.delete_button = tk.Button(self.button_frame, text="DELETE ACCOUNT",
bg="#FF4444", fg="white",
                                       font=("Segoe UI", 13, "bold"), width=36, height=2,
                                       command=self.toggle_delete_form)
        self.delete_button.grid(row=1, column=0, columnspan=2, pady=(15,0))
        # Створюємо фрейми для форм
        self.login_frame = tk.Frame(self.form_card, bg="#2B2B2B")
        self.register_frame = tk.Frame(self.form_card, bg="#2B2B2B")
        self.delete_form_frame = tk.Frame(self.form_card, bg="#2B2B2B")
        self.login_frame.pack_forget()
        self.register_frame.pack_forget()
        self.delete_form_frame.pack_forget()
        # Папки та файл користувачів
        os.makedirs(DB_DIR, exist_ok=True)
        if not os.path.exists(USERS_PATH):
            with open(USERS_PATH, "w", encoding="utf-8") as f:
                json.dump({}, f)
        try:
            with open(USERS_PATH, "r", encoding="utf-8") as f:
                self.users = json.load(f) or {}
        except (json.JSONDecodeError, FileNotFoundError):
            self.users = {}
        self.delete_form_visible = False
        # Обробник закриття вікна: щоб звільнити камеру
        self.main_window.protocol("WM_DELETE_WINDOW", self.on_closing)
    def hash_password(self, password: str) -> str:
        return hashlib.sha256(password.encode("utf-8")).hexdigest()
    def _start_main_camera_loop(self):
        try:
            ret, frame = self.cap.read()
        except Exception:
            ret = False
            frame = None
        if ret and frame is not None:
            # frame — BGR від OpenCV
            self.most_recent_capture_arr = frame.copy()
            rgb = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
            self.most_recent_capture_pil = Image.fromarray(rgb)
            imgtk = ImageTk.PhotoImage(image=self.most_recent_capture_pil)
            self.webcam_label.imgtk = imgtk
            self.webcam_label.configure(image=imgtk)
        if self.webcam_label.winfo_exists():
            self.webcam_label.after(30, self._start_main_camera_loop)
    def hide_all_frames(self):
        self.login_frame.pack_forget()
        self.register_frame.pack_forget()
        self.delete_form_frame.pack_forget()
        self.delete_form_visible = False
    def show_login_form(self):
```

```
        self.hide_all_frames()
        self.login_frame.pack(fill="x", pady=5)
        self._create_login_form()
    def show_register_form(self):
        self.hide_all_frames()
        self.register_frame.pack(fill="x", pady=5)
        self._create_register_form()
    def toggle_delete_form(self):
        if self.delete_form_visible:
            self.delete_form_frame.pack_forget()
            self.delete_form_visible = False
        else:
            self.hide_all_frames()
            self.delete_form_frame.pack(fill="x", pady=5)
            self._create_delete_form()
            self.delete_form_visible = True
    def _create_entry(self, parent, label, attr, show=None):
        f = tk.Frame(parent, bg="#2B2B2B")
        f.pack(pady=5)
        tk.Label(f, text=label, font=("Segoe UI", 12, "bold"), fg="#00E0C6",
bg="#2B2B2B").pack(anchor="w")
        e = tk.Entry(f, font=("Segoe UI", 12), width=28, bg="#393E46", fg="white",
insertbackground="white",
                     relief="flat", show=show)
        e.pack(pady=3)
        setattr(self, attr, e)
    def _create_login_form(self):
        for w in self.login_frame.winfo_children():
            w.destroy()
        self._create_entry(self.login_frame, "Login:", "login_entry")
        self._create_entry(self.login_frame, "Password:", "password_entry", show="*")
        btns = tk.Frame(self.login_frame, bg="#2B2B2B")
        btns.pack(pady=10)
        tk.Button(btns, text="LOGIN", bg="#00ADB5", fg="white",
                  font=("Segoe UI", 12, "bold"), width=14, command=self.login).grid(row=0, column=0,
padx=8)
        tk.Button(btns, text="CANCEL", bg="#FF5722", fg="white",
                  font=("Segoe UI", 12, "bold"), width=14, command=self.hide_all_frames).grid(row=0,
column=1, padx=8)
    def _create_register_form(self):
        for w in self.register_frame.winfo_children():
            w.destroy()
        self._create_entry(self.register_frame, "New Login:", "new_login_entry")
        self._create_entry(self.register_frame, "New Password:", "new_password_entry", show="*")
        btns = tk.Frame(self.register_frame, bg="#2B2B2B")
        btns.pack(pady=10)
        tk.Button(btns, text="REGISTER", bg="#00ADB5", fg="white",
                  font=("Segoe UI", 12, "bold"), width=14, command=self.register_user).grid(row=0,
column=0, padx=8)
        tk.Button(btns, text="CANCEL", bg="#FF5722", fg="white",
                  font=("Segoe UI", 12, "bold"), width=14, command=self.hide_all_frames).grid(row=0,
column=1, padx=8)
    def _create_delete_form(self):
```

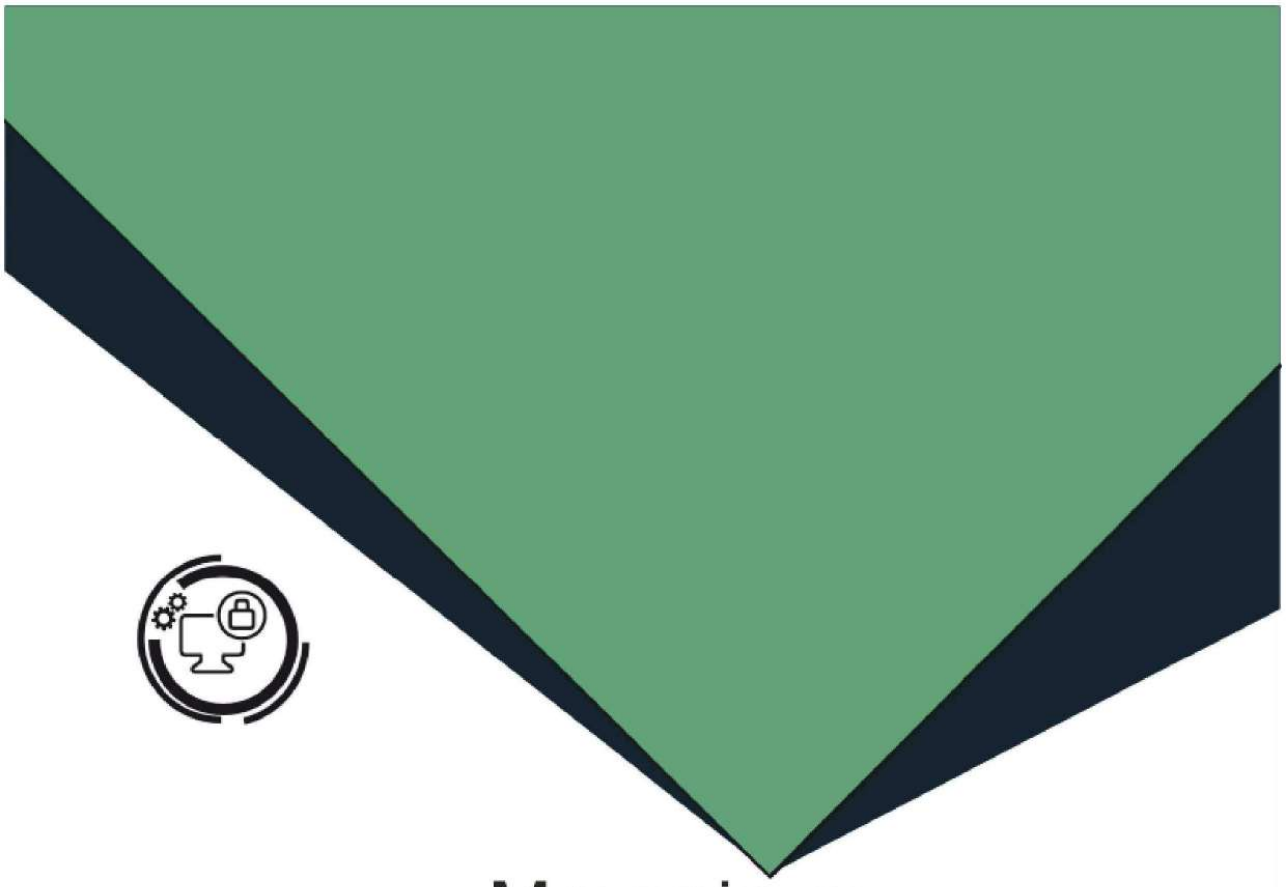
```
        for w in self.delete_form_frame.winfo_children():
            w.destroy()
        self._create_entry(self.delete_form_frame, "Login:", "del_login_entry")
        self._create_entry(self.delete_form_frame, "Password:", "del_password_entry", show="*")
        tk.Button(self.delete_form_frame, text="CONFIRM DELETE", bg="#FF4444", fg="white",
                  font=("Segoe UI", 14, "bold"), width=36, height=2,
command=self.confirm_delete_account).pack(pady=10)
    def register_user(self):
        login = self.new_login_entry.get().strip()
        password = self.new_password_entry.get().strip()
        if not login or not password:
            messagebox.showerror("Error", "Please fill all fields.")
            return
        if login in self.users:
            messagebox.showerror("Error", "User already exists.")
            return
        if self.most_recent_capture_arr is None:
            messagebox.showerror("Error", "No camera frame available.")
            return
        filename = os.path.join(DB_DIR, f"{login}.jpg")
        try:
            cv2.imwrite(filename, self.most_recent_capture_arr)
        except Exception as e:
            messagebox.showerror("Error", f"Failed to save face image: {e}")
            return
        hashed = self.hash_password(password)
        self.users[login] = {"password": hashed}
        try:
            with open(USERS_PATH, "w", encoding="utf-8") as f:
                json.dump(self.users, f, indent=4, ensure_ascii=False)
        except Exception as e:
            messagebox.showerror("Error", f"Failed to write users file: {e}")
            return
        messagebox.showinfo("Success", f"User '{login}' registered successfully!")
        self.hide_all_frames()
    def login(self):
        login = self.login_entry.get().strip()
        password = self.password_entry.get().strip()
        if not login or not password:
            messagebox.showerror("Error", "Please fill all fields.")
            return
        hashed = self.hash_password(password)
        if login not in self.users or self.users[login].get("password") != hashed:
            messagebox.showerror("Error", "Invalid login or password.")
            return
        if self.most_recent_capture_arr is None:
            messagebox.showerror("Error", "No camera frame available.")
            return
        try:
            rgb_image = cv2.cvtColor(self.most_recent_capture_arr, cv2.COLOR_BGR2RGB)
        except Exception:
            messagebox.showerror("Error", "Failed to process camera image.")
            return
```

```
        encodings = face_recognition.face_encodings(rgb_image)
        if not encodings:
            messagebox.showerror("Error", "No face detected.")
            return
        unknown_encoding = encodings[0]
        path = os.path.join(DB_DIR, f"{login}.jpg")
        if not os.path.exists(path):
            messagebox.showerror("Error", "No face data found for this user.")
            return
        try:
            known_image = face_recognition.load_image_file(path)
            known_enc = face_recognition.face_encodings(known_image)
        except Exception as e:
            messagebox.showerror("Error", f"Failed to load known face: {e}")
            return
        if known_enc and face_recognition.compare_faces([known_enc[0]], unknown_encoding)[0]:
            messagebox.showinfo("Welcome", f"Welcome, {login}!")
            try:
                with open(LOG_PATH, "a", encoding="utf-8") as f:
                    f.write(f"{login},{datetime.datetime.now()},in\n")
            except Exception:
                pass
            try:
                if os.path.exists(OPEN_FOLDER_PATH):
                    subprocess.Popen(f'cmd /c start "" "{OPEN_FOLDER_PATH}"', shell=True)
            except Exception:
                pass
            self.hide_all_frames()
        else:
            messagebox.showerror("Error", "Face does not match registered user.")
    def confirm_delete_account(self):
        login = self.del_login_entry.get().strip()
        password = self.del_password_entry.get().strip()
        if not login or not password:
            messagebox.showerror("Error", "Please fill all fields.")
            return
        hashed = self.hash_password(password)
        if login not in self.users or self.users[login].get("password") != hashed:
            messagebox.showerror("Error", "Invalid login or password.")
            return
        if self.most_recent_capture_arr is None:
            messagebox.showerror("Error", "No camera frame available.")
            return
        try:
            rgb_image = cv2.cvtColor(self.most_recent_capture_arr, cv2.COLOR_BGR2RGB)
        except Exception:
            messagebox.showerror("Error", "Failed to process camera image.")
            return
        encodings = face_recognition.face_encodings(rgb_image)
        if not encodings:
            messagebox.showerror("Error", "No face detected.")
            return
        unknown_encoding = encodings[0]
```

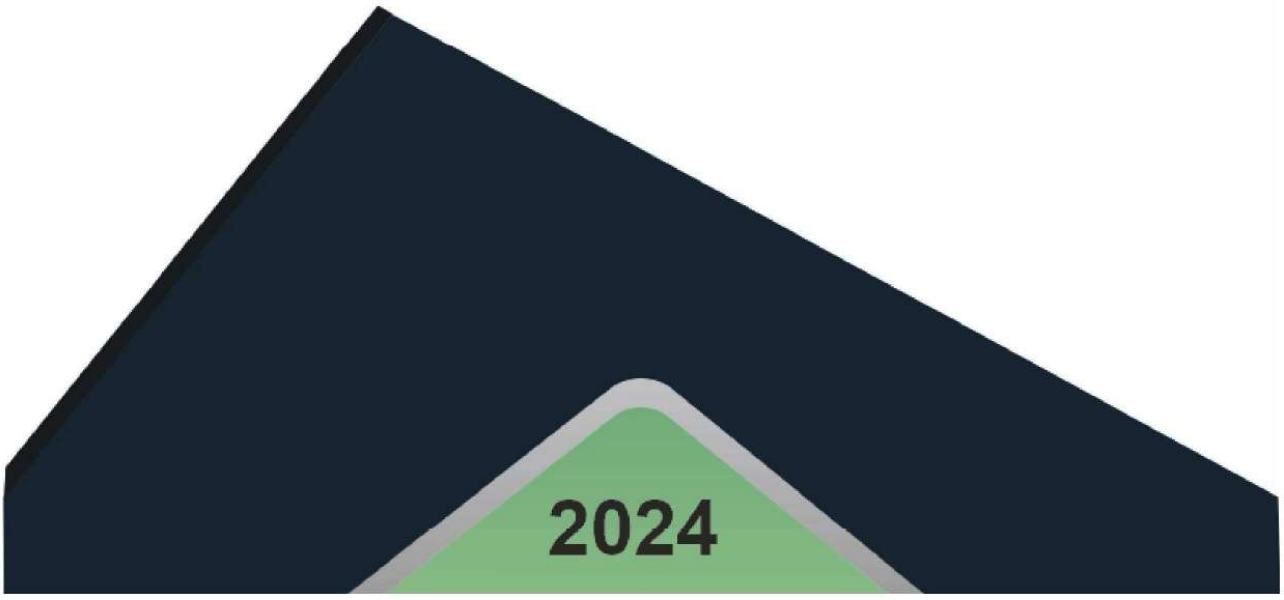
```
            path = os.path.join(DB_DIR, f"{login}.jpg")
            if not os.path.exists(path):
                messagebox.showerror("Error", "No face data found for this user.")
                return
            try:
                known_image = face_recognition.load_image_file(path)
                known_enc = face_recognition.face_encodings(known_image)
            except Exception as e:
                messagebox.showerror("Error", f"Failed to load known face: {e}")
                return
            if known_enc and face_recognition.compare_faces([known_enc[0]], unknown_encoding)[0]:
                try:
                    os.remove(path)
                except Exception:
                    pass
                self.users.pop(login, None)
                try:
                    with open(USERS_PATH, "w", encoding="utf-8") as f:
                        json.dump(self.users, f, indent=4, ensure_ascii=False)
                except Exception as e:
                    messagebox.showerror("Error", f"Failed to update users file: {e}")
                    return
                messagebox.showinfo("Deleted", f"User '{login}' has been deleted successfully!")
                self.hide_all_frames()
            else:
                messagebox.showerror("Error", "Face does not match registered user.")
        def on_closing(self):
            try:
                if self.cap and self.cap.isOpened():
                    self.cap.release()
            except Exception:
                pass
            # закриваємо головне вікно
            try:
                self.main_window.destroy()
            except Exception:
                sys.exit(0)
        def start(self):
            self.main_window.mainloop()
    if __name__ == "__main__":
        app = App()
        app.start()
```

Додаток В

Копії публікацій



Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»



У збірнику опубліковано матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. - 130с.

Технічний редактор: Давлетова А.Я.

Адреса редакції:
Громадська організація «Кібербезпека і автоматизація»
м. Тернопіль
Контактний телефон: (066)043-42-10
e-mail: conferencekb@gmail.com

УДК 004.056

Антон ПЕТРЕНЧУК, Олександр ДЗІВАК

Західноукраїнський національний університет

СИСТЕМИ АУТЕНТИФІКАЦІЙ НА ОСНОВІ БІОМЕТРИЧНИХ ДАННИХ

Вступ. Системи аутентифікації на основі біометричних даних використовують унікальні фізіологічні та поведінкові характеристики, такі як відбитки пальців, риси обличчя або візерунки райдужної оболонки ока, для перевірки особи. Вони забезпечують вищий рівень безпеки порівняно з традиційними методами, як-от паролі, які легко втратити або викрасти. Аналізуючи унікальні маркери, такі системи дозволяють ефективно контролювати доступ у фінансовій, медичній та інших сферах та забезпечуючи надійність і зручність [1].

Мета: забезпечити надійний і зручний спосіб ідентифікації особи, використовуючи унікальні фізіологічні або поведінкові характеристики.

1. Системи біометричної аутентифікації

Біометричні системи автентифікації базуються на унікальних фізичних чи поведінкових характеристиках людини, які використовуються для ідентифікації або підтвердження особи. Різноманіття цих систем дозволяє їх адаптувати під специфічні потреби, підвищуючи безпеку та зручність використання (рисунок 1).

Рисунок 1 - Системи біометричної аутентифікації

Нижче наведено основні типи біометричних систем:

1. Розпізнавання обличчя. Аналізує геометричні особливості обличчя для створення цифрової моделі, широко використовується у смартфонах, системах безпеки та платежах. Попри зручність, є ризики через вплив глибоких фейків.

2. Розпізнавання відбитків пальців. Один із найпоширеніших методів, що застосовується у смартфонах, системах доступу та банківській сфері. Проте якість сенсорів та стан шкіри можуть впливати на точність.

3. Голосова автентифікація. Вивчає тон, частотні характеристики та тембр голосу. Використовується у службах підтримки. Слабкість полягає у впливі шуму та змін голосу.

4. Розпізнання райдужної оболонки ока. Ця технологія має високу точність, оскільки він є унікальним для кожної людини. Застосовується у високобезпекових системах, таких як військові об'єкти. Недоліками є висока вартість обладнання та складність реалізації.

5. Розпізнання вен. Аналізує унікальний малюнок кровоносних судин у руці чи пальці за допомогою інфрачервоного світла. Метод дуже точний і стійкий до підробок, але дорогий.

6. 6.Використання долоні. Використовує відбитки, геометрію долоні та візерунок вен. Завдяки комбінуванню даних забезпечує високу точність. Однак обладнання для цієї системи також є дорогим.

7. Розпізнання підпису. Аналізує характерні особливості рукописного підпису, такі як швидкість та тиск при його виконанні. Використовується переважно у фінансових операціях і підписанні юридичних документів.

2. Технологія розпізнавання обличчя

Одна з найвідоміших і передових біометричних систем аутентифікації - це технологія розпізнавання обличчя. Ця система використовується переважно для перевірки особистості, аналізуючи унікальні риси обличчя, такі як відстань між очима, форма підборіддя, контури щік та інші відмінні особливості. Як зазначено в IEEE Transactions on Information Forensics and Security, технологія розпізнавання обличчя стала популярним методом у різних безпекових застосунках завдяки своїй неінтрузивній природі та здатності забезпечувати швидку та надійну ідентифікацію.

Розпізнавання обличчя зазвичай працює шляхом захоплення зображення або відео обличчя людини за допомогою камери, яке потім порівнюється з базою даних раніше зареєстрованих біометричних даних (рисунок 2).

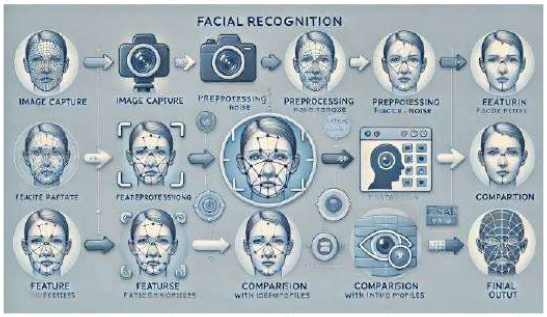


Рисунок 2 - Основні етапи роботи розпізнавання обличчя

Система відображає ключові точки (так звані маркери обличчя) на обличчі та створює цифровий шаблон, унікальний для кожної особи. Цей шаблон зберігається в базі даних, де його можна зіставити з майбутніми запитами для аутентифікації. Згідно з дослідженням, опублікованим у Pattern Recognition Letters, сучасні системи розпізнавання обличчя використовують алгоритми машинного навчання, такі як глибокі нейронні мережі, для покращення точності та зменшення кількості помилок, постійно вивчаючи і адаптуючись до різних умов освітлення, виразів обличчя та кутів огляду [2].

Одним з яскравих прикладів застосування розпізнавання обличчя є його інтеграція в смартфони. Система Face ID від Apple, яка використовує 3D-розпізнавання обличчя, є широко використовуваним прикладом цієї технології. Face ID створює детальну карту глибини обличчя користувача за допомогою інфрачервоних сенсорів, і ці дані зберігаються безпечно на чіпі пристрою, що гарантує захист біометричних даних від зовнішнього доступу.

Цей метод, як зазначено в The Journal of Mobile Technology in Medicine, забезпечує високий рівень безпеки через складність його підробки або обману, на відміну від 2D-розпізнавання обличчя, яке можна обдурити за допомогою фотографій чи відео.

Розпізнавання обличчя також швидко набуває популярності в системах безпеки для контролю доступу та спостереження. Наприклад, аеропорти та урядові установи впровадили ці системи для прискорення процесу перевірки пасажирів та підвищення безпеки шляхом швидкої ідентифікації осіб, які перебувають у списках для перевірки. У доповіді Європейського агентства з кібербезпеки (ENISA) підкреслюється, що системи розпізнавання обличчя можуть підвищити ефективність та точність у процесах перевірки, зменшуючи людські помилки та можливість порушення безпеки.

Однак, незважаючи на численні переваги, технологія розпізнавання обличчя викликає значні побоювання щодо приватності та етики. Як зазначено в Electronic Frontier Foundation (EFF) [3], існують побоювання щодо масового спостереження та потенційного зловживання біометричними даними без належної згоди. Крім того, дослідження, такі як те, що опубліковано в MIT Media Lab, виявили, що деякі системи розпізнавання обличчя мають вищі показники помилок для людей з темною шкірою та жінок, що підкреслює необхідність створення більш рівноправних і точних систем. Отже, хоча технологія розпізнавання обличчя має значні переваги в плані безпеки та ефективності, вона також ставить нові виклики щодо приватності, етики та справедливості. Подальші дослідження, регулювання та розробка більш інклюзивних систем є необхідними для забезпечення відповідального та ефективного використання розпізнавання обличчя в безпекових застосунках.

Висновок. Біометричні системи аутентифікації, зокрема розпізнавання обличчя, демонструють значний потенціал у забезпеченні безпеки та зручності, особливо у сферах мобільних пристроїв, банківських послуг та транспорту. Завдяки унікальним характеристикам, які складно підробити, ці технології забезпечують точну ідентифікацію користувачів. Водночас вони стикаються з викликами щодо приватності, етики та точності, включаючи захист даних і ризики дискримінації. Для ефективності цих систем важливо забезпечити баланс між інноваціями та правами користувачів, вдосконалювати технології та розробляти чіткі стандарти їх застосування.

Перелік використаних джерел.

1. European Union Agency for Cybersecurity (ENISA). (2020). Biometrics and Privacy: An Overview of Security and Privacy Considerations. [Електронний ресурс].- Режим доступу: https://www.enisa.europa.eu/

2. Kaur, Paramjit & Krishan, Kewal & Sharma, Suresh & Kanchan, Tanuj. (2020). Facial-recognition algorithms: A literature review. Medicine, science, and the law. 10.1177/0025802419893168..

3. Electronic Frontier Foundation (EFF). (2021). Privacy and Ethics of Biometric Surveillance: The Case of Facial Recognition. [Електронний ресурс].- Режим доступу: https://www.eff.org/

Міністерство освіти і науки України,
ДНУ «Інститут модернізації змісту освіти»,
Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»,
Інститут кібернетики ім. В.М. Глушкова НАН України,
Інститут телекомунікацій і глобального інформаційного простору НАН України,
Інститут цифровізації освіти НАПН України,
Житомирський державний університет імені Івана Франка,
Житомирський військовий інститут імені С.П. Корольова,
Черкаський державний технологічний університет,
Вінницький національний технічний університет,
Опольська політехніка (Республіка Польща),
Варшавський технологічний університет (Республіка Польща),
Технологічний університет Лулео (Королівство Швеція),
Технічний університет (Чеська Республіка),
Технічний університет (Республіка Болгарія),
Університет країни Басків (Королівство Іспанія),
Віденський технічний університет (Республіка Австрія),
ADA University (Азербайджан)

ТЕЗИ ДОПОВІДЕЙ

XV Міжнародної науково-технічної конференції

Інформаційно-комп'ютерні технології

м. Житомир, 28-29 березня 2025 р.

Житомир
2025

УДК 004
Т11

Рекомендовано до друку Вченою радою Державного університету «Житомирська політехніка» (протокол № 6 від 24.03.2025 р.)

Тези XV Міжнародної науково-технічної конференції
Т11 «Інформаційно-комп'ютерні технології», м. Житомир, 28-29 березня 2025 р. – Житомир: Житомирська політехніка, 2025. – 352 с.
ISBN 978-966-683-698-7

Представлено доповіді учасників XV Міжнародної науково-технічної конференції. Наведено аналіз та результати досліджень сучасних проблем інформаційних технологій, математичного моделювання та розробки програмного забезпечення, інформаційних систем, комп'ютерної інженерії та кібербезпеки, цифрової обробки сигналів та зображень, комп'ютерно-інтегрованих технологій, робототехніки та приладобудування, інформаційних технологій в телекомунікаціях та біомедицині, інформаційно-комунікаційних технологій в освіті.

УДК 004

ISBN 978-966-683-698-7

Наукове видання

Тези XV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології», Житомир, 28-29 березня 2025 р.

Відповідальний за випуск В.В. Болотіна

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи ДК № 7177 ВІД 04.11.2021 р.

Адреса редакції: Державний університет «Житомирська політехніка», вул. Чуднівська, 103, м.Житомир, 10005

УДК 004.056

Петренчук А.В., здобувач
Кулина С.В., к.т.н., доцент
Західноукраїнський національний університет

СИСТЕМИ АУТЕНТИФІКАЦІЇ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

Системи аутентифікації на основі біометричних даних використовують унікальні фізіологічні та поведінкові характеристики, такі як відбитки пальців, риси обличчя або візерунки райдужної оболонки ока, для перевірки особи. Вони забезпечують вищий рівень безпеки порівняно з традиційними методами, як-от паролі, які легко втратити або викрасти. Аналізуючи унікальні маркери, такі системи дозволяють ефективно контролювати доступ у фінансовій, медичній та інших сферах, забезпечуючи надійність і зручність [1].

Сучасні системи аутентифікації – це комплекс технологій та методів, спрямованих на підтвердження особи користувача, який намагається отримати доступ до інформаційних ресурсів. Вони еволюціонували від простих паролів до складних біометричних систем, що враховують унікальні фізіологічні та поведінкові характеристики людини.

Основні типи сучасних систем аутентифікації:

• Парольна аутентифікація – найпоширеніший метод, але має ряд недоліків, таких як вразливість до зламу та необхідність запам'ятовувати складні паролі.

• Багатофакторна аутентифікація вимагає використання двох або більше факторів аутентифікації, що значно підвищує рівень безпеки.

• Біометрична аутентифікація використовує унікальні фізіологічні або поведінкові характеристики людини, такі як відбитки пальців, розпізнавання обличчя тощо.

• Аутентифікація на основі сертифікатів використовує цифрові сертифікати для підтвердження особи користувача.

• Аутентифікація на основі токенів використовує фізичні або програмні токени для генерації одноразових паролів.

Аналіз та порівняння існуючих біометричних систем є важливим етапом для розуміння їхніх можливостей, обмежень та сфери застосування.

Основні типи біометричних систем:

• Фізіологічні: відбитки пальців, розпізнавання обличчя, райдужна оболонка ока, геометрія руки.

• Поведінкові: розпізнавання голосу, динаміка підпису, натискання клавіш.

Критерії порівняння[2]:

• Точність – помилки хибного прийняття і хибного відхилення.
• Швидкість – час, необхідний для аутентифікації.
• Зручність – простота використання.
• Вартість – витрати на обладнання та впровадження.
• Безпека – стійкість до підробки.
• Прийнятність – сприйняття користувачами.

У таблиці 1 представлено порівняння існуючих типів біометричних систем за вище згаданими критеріями.

Таблиця 1

Порівняння існуючих типів біометричних систем

Характеристика	Відбитки пальців	Розпізнання обличчя	Райдужна оболонка ока	Розпізнання голосу
Точність	Висока	Середня	Висока	Середня
Швидкість	Висока	Висока	Висока	Середня
Зручність	Висока	Висока	Середня	Висока
Вартість	Низька	Середня	Висока	Низька
Безпека	Середня	Середня	Висока	Низька

Сучасні системи аутентифікації знаходяться на етапі трансформації, де традиційні методи поступово замінюються більш надійними та зручними рішеннями. Біометрична аутентифікація відіграє ключову роль у підвищенні рівня захисту, а багатофакторна біометрична аутентифікація є перспективним напрямком розвитку. Важливо враховувати етичні та юридичні аспекти використання біометричних даних, а також забезпечувати їхній захист від несанкціонованого доступу.

Список використаних джерел:

1. Tirfe D., Anand V.K. A Survey on Trends of Two-Factor Authentication. In: Sarma H.K.D., Balas V.E., Bhuyan B., Dutta N. (eds) Contemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems, vol 281. Springer, Singapore, 2022.

2. Скорик Ю., Костромицький А., Копиця А. Порівняння видів біометричних пристроїв. Міжнародний науковий журнал інженерії та сільського господарства, 3 (5), 1–7, 2024.