ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Автоматизована система контролю доступу на основі біометричних даних і технологій штучного інтелекту»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ _____

(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувачка вищої освіти гр. ІСД-41
Аліса ЛУНЬОВА

Ім'я, ПРІЗВИЩЕ

Керівник: Каміла СТОРЧАК, д. т. н.,
науковий ступінь, вчене звання професор

Ім'я, ПРІЗВИЩЕ

Рецензент:
науковий ступінь, вчене звання

Ім'я, ПРІЗВИЩЕ

Київ - 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Інформаційних систем та технологій
Ступінь вищої освіти бакалавр
Спеціальність 126 Інформаційні системи та технології
Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ
_____Каміла СТОРЧАК
«___» _____20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Луньова Аліса Ігорівна

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Автоматизована система контролю доступу на основі біометричних даних і технологій штучного інтелекту

керівник кваліфікаційної роботи Каміла СТОРЧАК, д. т. н., професор,

(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025 р. № 56

2. Строк подання кваліфікаційної роботи «30» травня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: офіційна технічна документація моделей машинного навчання та інструментів розробки, відкриті результати наукових досліджень, кейси застосування машинного навчання та штучного інтелекту для біометричної ідентифікації

3. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження сучасного стану, технологій та різносторонніх аспектів застосування технологій біометричної ідентифікації у інформаційних системах
2. Проєктування апаратної частини системи біометричного контролю
3. Тестування моделей машинного навчання та розробка програмного забезпечення

4. Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання «24» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	01.03.2025 р.	
2	Дослідження існуючих систем керування транспортним трафіком у розумних містах	15.03.2025 р.	
3	Формулювання технічного завдання, функціональних та нефункціональних вимог на розробку системи управління транспортною інфраструктурою	17.03.2025 р.	
4	Вибір технологічного стеку та проєктування архітектури і монтажної схеми системи керування трафіком дорожнього руху	4.04.2025 р.	
5	Реалізація та тестування інформаційної системи управління транспортною інфраструктурою розумного міста	16.05.2025 р.	
6	Розробка демонстраційних матеріалів	26.05.2025 р.	
7	Попередній захист дипломної роботи	27.05.2025 р.	
8	Подання роботи в деканат	30.05.2025 р.	

Здобувач(ка) вищої освіти _____ _____

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ _____

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 85 стор., 70 рис., 2 табл., 37 джерел.

Мета роботи - розробити автоматизовану систему контролю доступу на основі біометричних даних та технологій штучного інтелекту, що забезпечує високу точність ідентифікації, безпеку даних та зручність використання.
Об'єкт дослідження - біометричні системи контролю доступу та їх інтеграція з технологіями штучного інтелекту.
Предмет дослідження - методи та алгоритми обробки біометричних даних, апаратні та програмні рішення для реалізації системи контролю доступу.

Короткий зміст роботи:
У роботі досліджено сучасні біометричні технології: розпізнавання обличчя, відбитків пальців, голосу та сітківки ока, а також їх застосування у системах контролю доступу. Проаналізовано можливості використання штучного інтелекту та машинного навчання для підвищення точності та ефективності ідентифікації. Розроблено апаратну частину системи на базі мікроконтролера ESP32 та біометричного сенсора, а також програмне забезпечення з використанням алгоритмів обробки зображень і глибокого навчання. Запропоновано веб-інтерфейс для управління системою та забезпечення безпеки даних відповідно до вимог GDPR.

КЛЮЧОВІ СЛОВА: біометрична система, контроль доступу, штучний інтелект, машинне навчання, ESP32, IoT, безпека даних.

ABSTRACT

The text part of the qualifying work for obtaining a bachelor's degree: 85 pages, 70 figures, 2 tables, 37 sources.

The purpose of the work - to develop an automated access control system based on biometric data and artificial intelligence technologies, which ensures high identification accuracy, data security and ease of use.
Object of research - biometric access control systems and their integration with artificial intelligence technologies.
The subject of research - biometric data processing methods and algorithms, hardware and software solutions for the implementation of the access control system.

Summary of the work:
The work examines modern biometric technologies: facial, fingerprint, voice, and retina recognition, as well as their application in access control systems. The possibilities of using artificial intelligence and machine learning to increase the accuracy and efficiency of identification are analyzed. The hardware part of the system is developed based on the ESP32 microcontroller and biometric sensor, as well as software using image processing and deep learning algorithms. A web interface is offered for managing the system and ensuring data security in accordance with GDPR requirements.

KEYWORDS: biometric system, access control, artificial intelligence, machine learning, ESP32, IoT, data security.

ЗМІСТ

ВСТУП

У сучасному світі питання безпеки та ефективності контролю доступу до об’єктів набуває все більшої актуальності. Використання ключів, паролів, магнітних карток або PIN-кодів та інших методів ідентифікації часто виявляються недостатньо надійними та зручними. Їх вразливість до втрати, підробки або несанкціонованого використання створює серйозні загрози для інформаційної та фізичної безпеки. У зв’язку з цим значно зростає інтерес до біометричних технологій, які грунтуються на унікальних фізіологічних або поведінкових характеристиках людини, наприклад, відбитки пальців, форма обличчя або голос.

Особливу увагу в цьому контексті заслуговує інтеграція біометричних методів з алгоритмами штучного інтелекту, зокрема машинного навчання, що дозволяє підвищити точність ідентифікації, забезпечити адаптивність до змін користувача та реалізувати високий рівень безпеки. Поєднання таких технологій відкриває нові можливості у створенні інтелектуальних систем контролю доступу, які здатні працювати автономно, з високою ефективністю та у режимі реального часу.

Метою даної роботи є розробка прототипу автоматизованої системи контролю доступу на основі біометричних даних з використанням технологій штучного інтелекту, що забезпечує високу точність ідентифікації, безпеку даних та зручність використання.

Об’єктом дослідження є автоматизовані системи контролю доступу. Предметом дослідження є технології біометричної ідентифікації та алгоритми штучного інтелекту, які використовуються для розробки інтелектуальних систем доступу.

Для досягнення поставленої мети в роботі передбачено вирішення завдань, описаних далі. По-перше, провести аналіз сучасних біометричних технологій та методів штучного інтелекту в контексті систем контролю доступу. По-друге, дослідити апаратні компоненти, що можуть використовуватись для реалізації прототипу. Наступним, розробити архітектуру системи контролю доступу з

біометричною аутентифікацією. Далі реалізувати програмну частину системи, забезпечивши зручний та захищений інтерфейс користувача. Відповідно, провести тестування системи на відповідність вимогам точності, швидкодії та безпеки, а також сформулювати практичні рекомендації щодо вдосконалення системи та можливості впровадження додаткових функцій, таких як розпізнавання обличчя або багатофакторна аутентифікація.

У роботі використано такі методи дослідження: аналіз літературних джерел і технічної документації, порівняльний аналіз апаратних засобів, моделювання, прототипування, експериментальне тестування та оцінювання ефективності запропонованої системи.

Практичне значення роботи полягає у можливості впровадження запропонованої системи в реальні умови - у навчальних закладах, офісах, житлових комплексах або інших об’єктах з підвищеними вимогами до безпеки. Система відрізняється низькою вартістю, гнучкістю налаштувань і можливістю подальшої масштабованості.

Апробація дослідження здійснювалась у формі участі в фахових конференціях:

1. ІІ всеукраїнська науково-технічна конференція «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» з поданням тези на тему «Штучний інтелект та машинне навчання у побуті та промисловості».

2. XV міжнародна наукова конференція студентів та молодих вчених «Сучасні інформаційні технології 2025» з поданням тези на тему «Розробка системи багатофакторної аутентифікації з використанням біометричних даних і штучного інтелекту».

РОЗДІЛ 1 МОЖЛИВОСТІ ТА ТЕХНОЛОГІЧНІ ОСОБЛИВОСТІ БІОМЕТРИЧНИХ СИСТЕМ І ШТУЧНОГО ІНТЕЛЕКТУ

1.1. Ключові особливості біометричних технологій та сфера їх застосування у сучасному світі

Штучний інтелект (ШІ) демонструє стрімкий розвиток у здатності до розпізнавання зображень та звуків, що має значний вплив на сучасні технології. За останні два десятиліття, як показано на рис. 1.1, продуктивність ШІ у сферах ідентифікування мови та ілюстрацій, зросла до рівня, який перевищує людські можливості у деяких тестах. Ці досягнення є визначальним кроком у розвитку технологій, що застосовуються в багатьох галузях, зокрема біометрію.

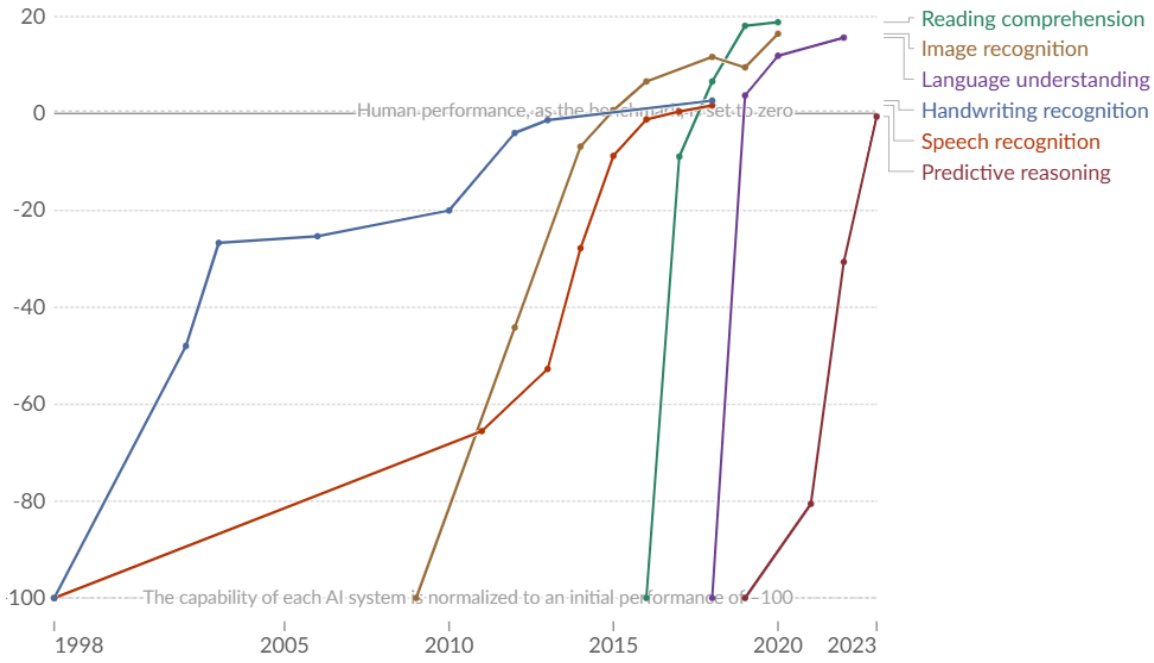


Рис. 1.1 Ріст продуктивності ШІ 1998-2023 рр. у різних задачах порівняно з людиною (0) [8]

Біометричні технології ґрунтуються на зборі та аналізі фізичних або поведінкових характеристик людини. Різні типи біометрії застосовуються для ідентифікації як у державному, так і в приватному секторах. На рис. 1.2 показані

пропорції використання кожного типу біометрії у різних сферах, з них: відбитки пальців, впізнання обличчя, сітківка ока, особливості голосу, тощо.

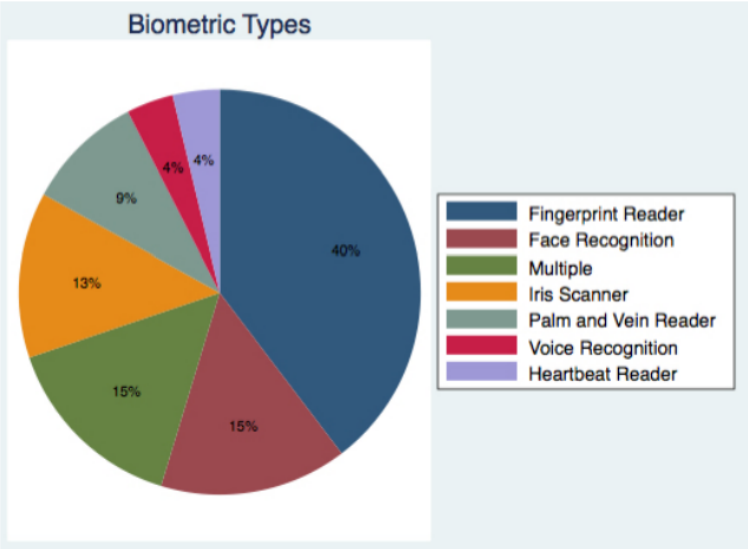


Рис. 1.2 Типи біометрії та їх процентне співвідношення [1]

Особливе місце серед даних технологій займають системи розпізнавання відбитків пальців. Вони популяризувалися завдяки їхній надійності, доступності та зручності інтеграції в різні пристрої та системи. Світовий ринок біометричних систем розпізнавання відбитків пальців у 2022 році оцінювався в $21,6 мільярда і, за прогнозами, до 2032 року досягне $74,1 мільярда з середньорічним темпом зростання (CAGR) у 13,4% [2]. Такі результати зумовлені нарощуванням використання пристроїв для детекції споживачів та зростанням інвестицій у секторі оборони. Однак питання конфіденційності, безпеки та рентабельності є стримуючими факторами розвитку цієї сфери, рис. 1.3.

Report Coverage	Details
Forecast Period	2023–2032
Base Year	2022
Market Size in 2022	$21.6 Billion
Market Size in 2032	$74.1 Billion
CAGR	13.4%
No. of Pages in Report	345
Segments covered	Offering, Type, End User, and Region.
Drivers	Surge in penetration of user identification devices. Increased spending in the defence sector.
Opportunities	Key technological developments leading to the commodification of biometrics
Restraints	Operational concerns related to privacy, security, and ROI

Рис. 1.3 Прогноз динаміки ринку біометричних систем розпізнавання відбитків пальців 2022-2032 рр. [2]

Ринок технологій розпізнавання обличчя також стрімко розвивається, і до 2028 року, за прогнозами Technavio, його обсяг збільшиться на 11,82 млрд доларів США із щорічним темпом приросту понад 22,2% [9]. Попри такі показники, високі витрати на впровадження таких технологій сповільнюють їх поширення. Системи з інтегруванням розпізнавання обличчя активно застосовуються у контролі відвідуваності, ідентифікації пацієнтів та автоматизації платежів. Вони підвищують операційну ефективність в освіті, охороні здоров’я, роздрібній торгівлі, гарантують безпеку в аеропортах і на критичних об’єктах. Тому відомі компанії NEC, Microsoft та AWS, додають розпізнавання обличчя у свої KYC-системи, цифрові гаманці та мобільні додатки.

Не зважаючи на конкуренцію типів біометрії, біометрія на основі сітківки ока все ще залишається однією з найбільш стійких та надійних методів ідентифікації особи. Сітківка ока - це тонка тканина, що покриває внутрішню сторону окової ямки та містить унікальний малюнок судин. Він залишається незмінним упродовж життя, що робить його цінним для систем безпеки. Ця технологія демонструє

точність, яка перевищує продуктивність провідних автоматизованих систем відбитків пальців, що вважаються золотим стандартом у сфері ідентифікації. За оцінками уряду США, такі системи досягають точності в межах від 98,1% до 99,9%, тоді як точність біометричних систем на основі сітківки ока коливається від 99% до 99,8% [10]. З економічної точки зору, на рис. 1.4 можна побачити, що попит на ідентифікацію сітківки ока не є таким сильним, як, наприклад, вищерозглянутий принцип розпізнавання обличчя.

Global Iris Recognition Market Value: 2019–2027	In Billion USD
2019	0.68
2021	2.90
2026*	1.85
2027*	8.40

Рис. 1.4 Ринкова вартість розпізнавання райдужної оболонки ока у світі 2019-2027 рр. [11]

Іншим провідним напрямом є розпізнавання голосу, що застосовує алгоритми для аналізу та інтерпретації звуків, створюваних людським голосом, і дозволяє комп'ютерним системам розуміти мову та виконувати команди. Завдяки розвитку ШІ та МН, ця технологія фігурє в багатьох сучасних додатках, зокрема, голосових помічників, автоматизованих систем обслуговування та інтерфейсів для користувачів. Ринок розпізнавання голосу показує вражаючі темпи зростання - прогнозується, що до 2029 року його вартість досягне $49,79 мільярда, що свідчить про великий потенціал цієї технології, рис. 1.5. Одним із головних факторів для цього є адаптація до різних акцентів, мовних стилів і фонових шумів.

Worldwide Market Size of Voice Recognition: 2021–2029	In Billion USD
2021	9.56
2022	11.21
2029*	49.79

Рис. 1.5 Ринкова вартість розпізнавання голосу в світі 2019-2027 рр. [11]

Біометричні технології стають невід'ємною частиною багатьох сфер життя, охоплюючи фінансові послуги, урядову діяльність, робочі середовища, а також освіту, охорону здоров'я, дозвілля та технології, діаграму можна побачити на рис. 1.6.

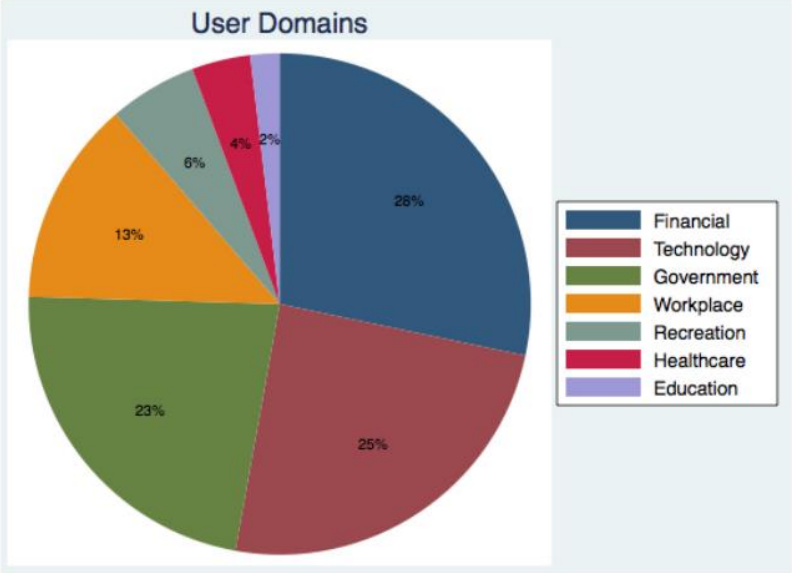


Рис. 1.6 Загальна сфера послуг і діяльності, в якій користувачі використовують біометричні дані для самоідентифікації [1]

Фінансова сфера є одним із найбільш активних доменів впровадження біометрії. Компанії Wells Fargo, Bank of America та Citibank, широко використовують відбитки пальців для ідентифікації клієнтів у банкоматах, під час онлайн-банкінгу та транзакцій у точках продажу. Додатково, інноваційні пристрої, до прикладу, браслети для моніторингу серцебиття, створюють кращі рівні

безпеки. Поширення смартфонів з функцією сканування відбитків пальців від Apple і Samsung, сприяло масовій доступності біометрії відбитка пальця. Згідно з діаграмою на рис. 1.7, відбитки пальців є найпопулярнішим методом у фінансовій сфері та становлять 13,2%. Відповідно, комбіновані технології, наприклад, інтеграція відбитків пальців із розпізнаванням облич (5,7%), забезпечують ще більший захист.

Урядові структури також активно інтегрують біометрію в різні процеси. У багатьох країнах сканування відбитків пальців та долоні стало стандартом для ідентифікації громадян під час голосування, отримання державних послуг або управління кордонами. На рис. 1.7 показано, як біометрія впроваджується в США: сканування райдужної оболонки ока допомагає TSA під час перевірок у аеропортах (3,8%), а розпізнавання облич (5,7%) і відбитки пальців застосовуються для створення кримінальних баз даних та моніторингу ув'язнених.

У робочому середовищі біометрія стає провідним інструментом для спрощення адміністративних процесів. Найпоширенішим методом, як можна побачити на рис. 1.7, є сканування відбитків пальців (5,7%), яке інтегрують для входу до офісів, авторизації працівників при роботі з касовими апаратами та обліку робочого часу. Комбіновані технології (3,8%) також впроваджують для підвищення безпеки в офісах і промислових об'єктах.

Сфери освіти та охорони здоров'я впроваджують біометрію специфічним способом - у цих доменах найбільш поширене сканування райдужної оболонки ока. У навчальних закладах це може використовуватися для контролю відвідуваності або доступу до ресурсів (1,9%). В охороні здоров'я такі технології допомагають уникнути помилок в ідентифікації пацієнтів, гарантуючи їхню конфіденційність (3,8%).

Технологічний сектор пропонує найбільшу різноманітність у використанні біометрії, інтегруючи відбитки пальців (9,4%), розпізнавання облич (5,7%), голосу (1,9%) та комбіновані технології. Такі інновації підвищують рівень безпеки пристроїв і програмного забезпечення.

У секторі дозвілля біометрія використовується для зручного доступу до подій, як спортивні змагання чи концерти. Відбитки пальців (3,8%) і розпізнавання облич (1,9%) є основними методами, що сприяють автоматизації процесів.

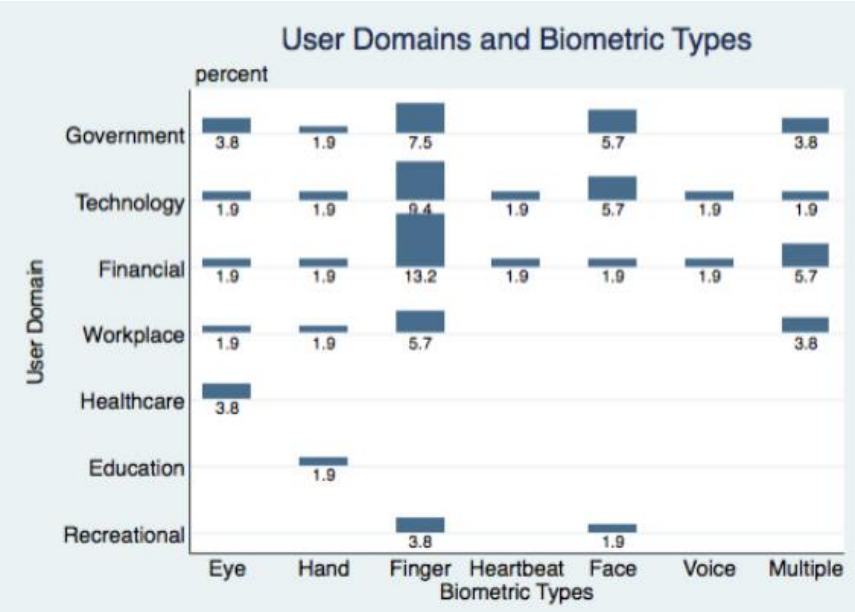


Рис. 1.7 Розподіл біометричних технологій за сферами застосування [1]

За допомогою аналізу платформ, на яких використовуються біометричні системи, можна виявити ключові тенденції в застосуванні та адаптації до потреб користувачів, як наведено на рис. 1.8, рис. 1.9 та рис. 1.10. Станом на 2025 рік, стаціонарні системи залишаються лідерами у впровадженні біометричних технологій, охоплюючи 55% ринку. Ці системи застосовуються для ідентифікації користувачів у фінансових установах, на робочих місцях та в урядових органах.

Мобільні пристрої, що займають 30% ринку, поширюються з новими моделями смартфонів із вбудованими біометричними функціями. Розпізнавання облич і сканування відбитків пальців стали звичайною практикою для мобільних додатків у вищезгаданій фінансовій сфері. Персональні комп’ютери, які становлять 9% ринку, поступово впроваджують біометричні технології, зокрема сканери відбитків пальців та функції розпізнавання облич.

Носимі пристрої, які займають 6% ринку, представляють новий етап у розвитку біометричних систем. Завдяки компактності та портативності, носимі

гаджети типу смарт-годинників або біометричних браслетів, відкривають нові можливості для ідентифікації користувачів. Наприклад, браслет Nymi, який аналізує серцевий ритм, дозволяє здійснювати безпечні фінансові транзакції та отримувати доступ до захищених об'єктів.

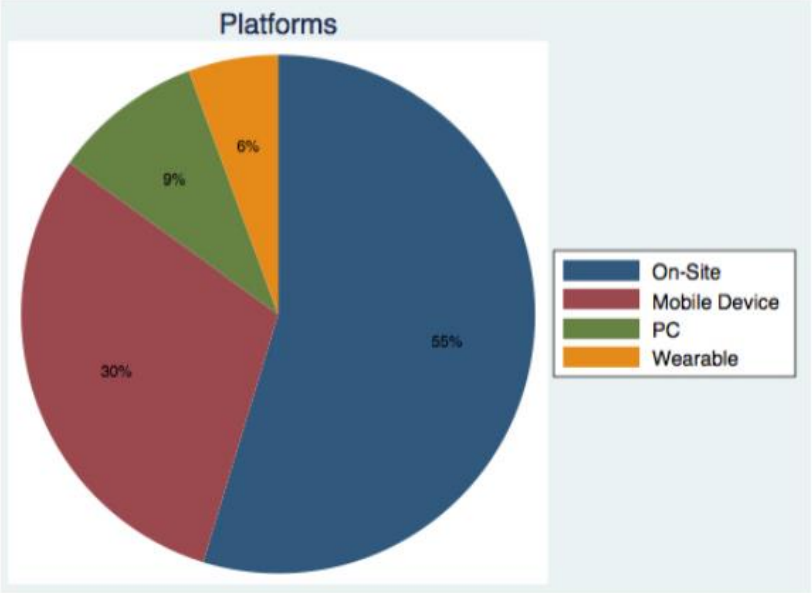


Рис. 1.8 Відмінності між різними платформами, які використовуються для ідентифікації осіб [1]

Дані діаграм - рис. 1.9, 1.10 поглиблюють аспекти відмінності у використанні біометричних технологій на різних платформах. На стаціонарних системах спостерігається домінування сканування відбитків пальців (22,6%) та розпізнавання очей (11,3%), у той час як у мобільних пристроях найбільш поширені сканування відбитків пальців (11,3%) і розпізнавання облич (7,5%).

До того ж, стаціонарні системи найбільш активно використовуються в урядовій сфері (20,8%) і на робочих місцях (13,2%). Це пов’язано з необхідністю високого рівня захисту та можливістю інтеграції складних рішень, зокрема комбінованих систем. Наприклад, сканування облич або очей у поєднанні з іншими методами забезпечує надійний доступ до конфіденційної інформації або захищених зон.

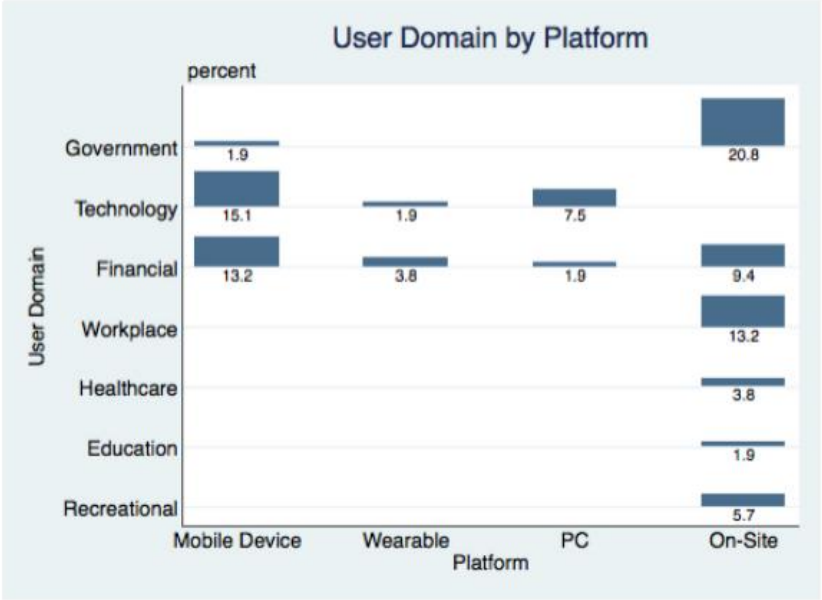


Рис. 1.9 Розподіл сфер використання біометрики за типами платформ [1]

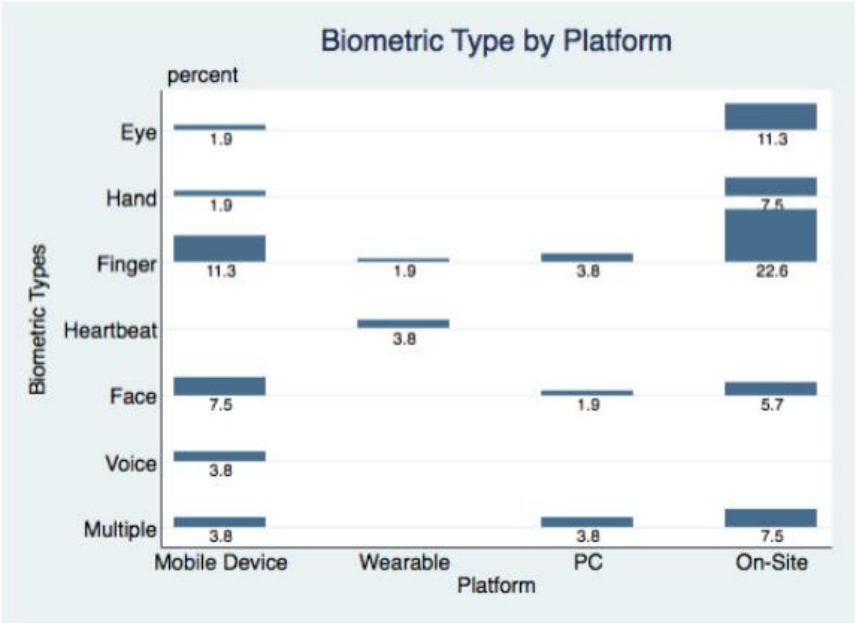


Рис. 1.10 Варіації платформ для кожного з досліджуваних біометричних типів [1]

Значним проривом у сфері біометричних технологій стало введення багатофакторної аутентифікації. Вона поєднує кілька типів біометричних даних, зокрема, відбитки пальців і розпізнавання обличчя, або додає біометричні методи до звичних способів ідентифікації, таких як паролі чи PIN-коди. Це дозволяє створити додатковий рівень безпеки, особливо в умовах зростаючих кіберзагроз. Так, фінансові установи вже активно впроваджують відповідні підходи для

запобігання шахрайству, пов’язаному з доступом до банківських акаунтів чи цифрових гаманців.

До того ж, інтеграція біометричних систем у системи "Розумного дому" є перспективним напрямком розвитку. Ці технології дозволяють ідентифікувати мешканців і надавати їм персоналізований доступ до окремих зон або функцій. Наприклад, системи розпізнавання обличчя можуть автоматично відкривати двері, регулювати освітлення чи температуру в приміщенні відповідно до індивідуальних вподобань користувачів. Подібні рішення активно розвиваються компаніями, які займаються "розумними" технологіями, зокрема Google та Amazon.

Іншим помітним напрямом є впровадження біометрії в транспортній інфраструктурі. Системи автоматичного розпізнавання облич та відбитків пальців застосовуються для підвищення безпеки на вокзалах, в аеропортах та громадському транспорті. Наприклад, у аеропортах США, TSA використовує біометричні технології для прискорення процесу ідентифікації пасажирів під час перевірки безпеки. Аналогічні системи впроваджуються в багатьох інших країнах, наприклад, Велика Британія, Німеччина та Японія. Крім того, транспортні компанії починають експлуатувати біометрію для забезпечення безконтактного доступу до транспортних засобів, що значно спрощує процес купівлі квитків та посадки. Однак одним із головних викликів для впровадження біометрії в транспорті та інших сферах залишається питання конфіденційності даних. Реалізація біометричних систем потребує збирання та обробки чутливих даних, які можуть бути вразливими до кібератак або неправомірного доступу. Законодавство у багатьох країнах намагається вирішити ці проблеми, розробляючи нормативно-правові акти щодо захисту персональних даних. Наприклад, у Європейському Союзі діє Загальний регламент захисту даних GDPR - General Data Protection Regulation, що встановлює жорсткі вимоги до обробки біометричних даних. (буде розглянуто більш детально в розділі 1.4).

Ще одним напрямком, де біометрія має потенціал для розвитку, є медицина - біометричні системи залучають для ідентифікації пацієнтів, запобігання медичним помилкам та збереження конфіденційності медичних записів. До

прикладу, у США біометричні рішення використовуються для доступу до електронних медичних записів та верифікації особистості пацієнтів перед проведенням медичних процедур. У поєднанні зі штучним інтелектом такі системи можуть навіть прогнозувати ризики для здоров’я на основі зібраних біометричних даних, що відкриває нові можливості для профілактичної медицини.

1.2. Технології штучного інтелекту та машинного навчання, що використовуються для ідентифікації особистості

Штучний інтелект та машинне навчання відіграють вирішальну роль у сучасних системах ідентифікації особистості, забезпечуючи високий рівень точності, ефективності та адаптивності. Завдяки використанню цих технологій біометричні системи виходять на новий рівень, що дозволяє зменшити ризики помилкової ідентифікації, підвищити захист даних і розширити сферу застосування таких систем. Аби зрозуміти концепт роботи цих механізмів, варто спочатку розглянути термін "Наука про дані".

"Наука про дані" (Data Science, DS) - це дисципліна, яка вивчає узагальнення методів, підходів та технологій для вирішення таких завдань, як обробка інформації, тобто здатність збирати, аналізувати, прогнозувати й застосовувати дані для ухвалення обґрунтованих рішень. Ця галузь включає кілька ключових напрямів, кожен із яких має своє призначення та особливості.

Інженерія даних (Data Engineering, DE) зосереджується на зборі, управлінні, попередній обробці даних та створенні датасетів, необхідних для подальшого застосування методів машинного навчання.

Машинне навчання (Machine Learning, ML) охоплює методи та технології, що дозволяють створювати моделі, здатні до прогнозування й аналізу на основі попереднього навчання на даних.

Штучний інтелект (Artificial Intelligence, AI), у свою чергу, представляє набір технологій і моделей, що імітують аспекти людського мислення, такі як розв'язання проблем, навчання, прийняття рішень та сприйняття. AI використовує елементи

машинного навчання, але фокусується на відтворенні особливостей людського інтелекту.

Інтелектуальний аналіз даних (Intelligent Data Analysis, IDA) спрямований на вирішення конкретних прикладних задач із залученням інструментів аналізу та вже тренованих моделей.

Вагомим аспектом науки про дані є створення інтелектуальних моделей, які здатні до самонавчання та узагальнення знань. Такі моделі не лише аналізують наявні дані, а й прогнозують майбутні сценарії або події. Наприклад, якщо інформаційна система може лише ідентифікувати об'єкти на основі зразків, вона не є інтелектуальною. Натомість можливість передбачати зміни або генерувати нові знання свідчить про її інтелектуальність.

Штучний інтелект поділяють на два основних типи. Слабкий або вузький AI (narrow AI, weak AI) спеціалізується на розв'язанні конкретних задач, як розпізнавання мовлення чи гри в шахи. Відповідно, сильний або загальний AI (general AI, strong AI) теоретично здатний до мислення, навчання та прийняття рішень на рівні людського інтелекту. Однак цей тип інтелекту наразі існує лише в теорії.

Хоча в багатьох джерелах поняття "Машинне навчання" і "Штучний інтелект" іноді вживають як взаємозамінні, між ними існують фундаментальні відмінності: МН охоплює всі можливі методи створення моделей, коли ШІ фокусується на тих, які імітують людські когнітивні процеси. Інженерія даних, у свою чергу, забезпечує створення якісних датасетів для навчання моделей. Інтелектуальний аналіз даних використовує готові моделі для розв'язання прикладних задач.

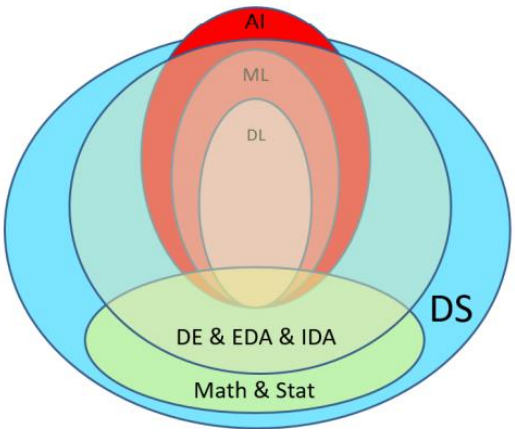


Рис. 1.11 Схема взаємозв'язків між штучним інтелектом (AI), машинним навчанням (ML), глибоким навчанням (DL), аналізом даних (DE, EDA, IDA), математикою та статистикою (Math & Stat) та наукою про дані (DS) [12]

Процес роботи з даними в межах DS зазвичай включає кілька основних етапів. Спершу відбувається збір і попередня обробка даних (Data Engineering). Наступний етап - розвідувальний аналіз даних (Exploratory Data Analysis, EDA), що передбачає застосування математичних і статистичних методів для виявлення закономірностей у даних. Далі здійснюється машинне навчання моделей (ML) для вирішення завдань аналізу даних у межах IDA.

Наука про дані здатна вирішувати задачі, пов’язані зі слабко-структурованими або неструктурованими проблемами. Вони характеризуються наявністю як кількісних, так і якісних елементів із високим рівнем невизначеності. У свою чергу, вживання методів МН, DL (глибокого навчання) та ШІ дозволяє підвищити структурованість даних, що значно полегшує аналіз і прогнозування.

Інформатика, як галузь, поєднує інформаційні технології (IT), комп’ютерні науки, знання предметної області та бізнес-аспекти, формуючи основу для розроблення програмного забезпечення. Суттєву роль у цій сфері відіграє математика, зокрема статистика, та кібернетика, включаючи теорію керування й оптимізації систем, що дає можливість проводити математичне моделювання, прогнозування та оптимізацію процесів і систем. Саме поєднання інформатики з математикою сприяло розвитку МН та ШІ, а інтеграція цих дисциплін створила

науку про дані (Data Science, DS). Діаграму зі зв’язком цих принципів можна побачити на рис. 1.12. Для опанування DS потрібне розуміння математики, програмування (передусім на Python), а також знання предметної області та постановки задачі з урахуванням вимог, обмежень і критеріїв ефективності методів і технологій.

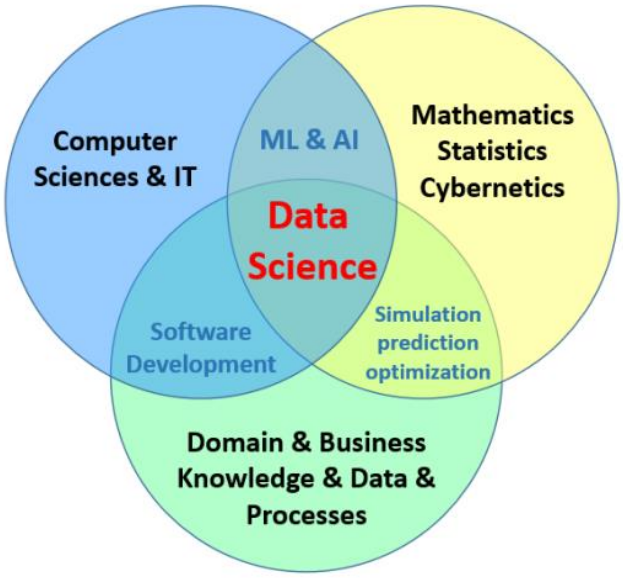


Рис. 1.12 Основні поняття та їх поєднання у сфері Data Science

Машинне навчання, як підгалузь штучного інтелекту, ґрунтується на застосуванні алгоритмів для автоматичного виявлення закономірностей у великих обсягах даних і побудови моделей для прийняття рішень. У машинному навчанні виділяють три основні типи навчання: навчання з учителем (supervised learning), навчання без учителя (unsupervised learning) та навчання з підкріпленням (reinforcement learning), рис. 1.13.

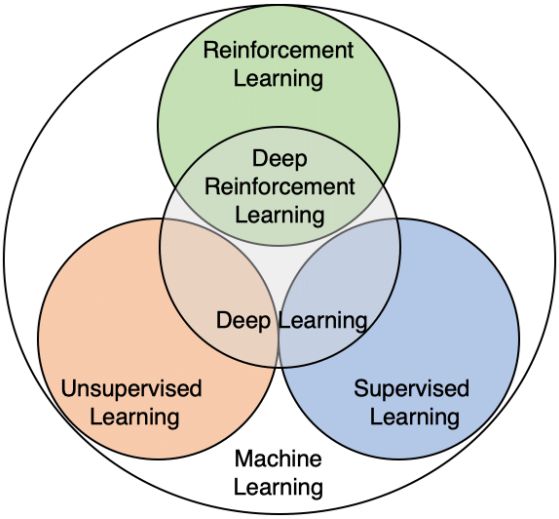


Рис. 1.13 Основні типи Машинного навчання (ML) [13]

У навчанні з учителем модель оперує даними з відповідними мітками для вивчення залежностей між вхідними параметрами та цільовими значеннями. У навчанні без учителя моделі шукають приховані закономірності в даних без наявності міток, як-от у задачах кластеризації текстів. Навчання з підкріпленням, натомість, передбачає взаємодію моделі з динамічним середовищем для прийняття оптимальних рішень, наприклад, у навчанні робота керувати літаком для мінімізації аварій чи максимізації часу польоту. В прикладних дослідженнях основна увага часто приділяється методам навчання з учителем.

У сфері ідентифікації особистості застосовуються як класичні методи МН, так і новітні підходи, наприклад, глибоке навчання. Серед найбільш поширених алгоритмів - кластеризація та класифікація, зокрема, методи Support Vector Machines (SVM) та K-Nearest Neighbors (k-NN), які мають високу точність у розпізнаванні обличчя, голосу чи інших біометричних характеристик. Глибокі нейронні мережі Convolutional Neural Networks (CNN) і Recurrent Neural Networks (RNN), дозволяють аналізувати складні багатовимірні дані, наприклад зображення чи голосові сигнали. Додатково, ефективним інструментом для підвищення точності аналізу є ансамблеве навчання, яке об'єднує результати кількох моделей, як Random Forest або Gradient Boosting. Генеративно-змагальні мережі (GANs)

знаходять широке застосування у створенні синтетичних біометричних даних та боротьбі з підробками.

Архітектура систем ідентифікації зазвичай складає попередню обробку даних, екстракцію ознак і класифікацію, рис. 1.14. На етапі попередньої обробки виконуються очищення, нормалізація та видалення шумів (для зображень також вирівнювання). Екстракція ознак виділяє ключові характеристики - форму обличчя чи тембр голосу, тоді як класифікація базується на порівнянні цих характеристик із базою даних. Завдяки сучасним алгоритмам машинного навчання системи ідентифікації стають дедалі точнішими, відкриваючи нові можливості для їхнього застосування в різних галузях.

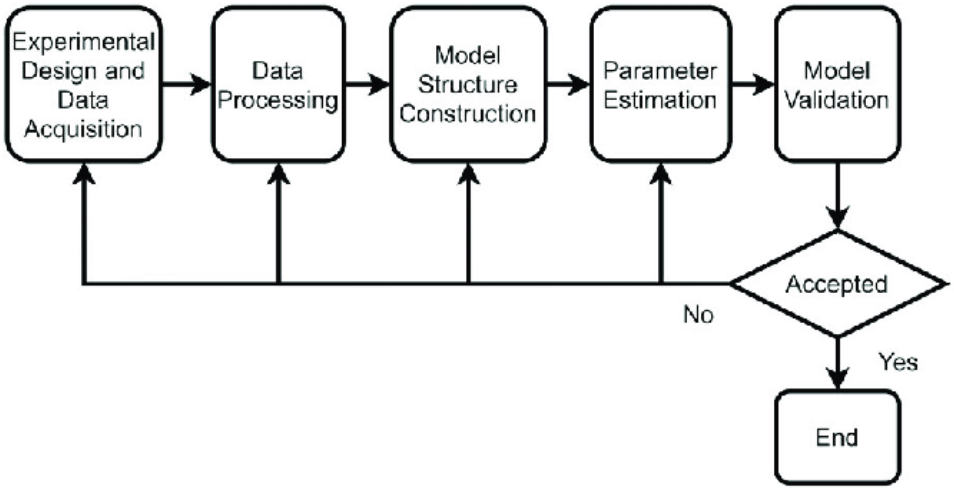


Рис. 1.14 Процес ідентифікації системи [13]

На рис. 1.15 можна побачити прогноз розвитку поширеності біометрії за наступні 5 років, із чого можна зробити висновок про швидкий ріст попиту на технології ШІ, а й, отже, МН.

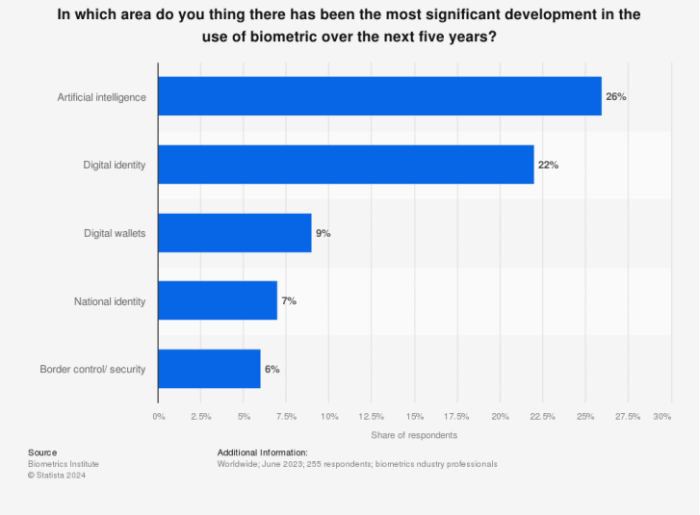


Рис. 1.15 Прогноз розподілу ключових напрямів розвитку біометричних технологій на 2024-2029 рр. [14]

У найближчому майбутньому можна очікувати подальшого вдосконалення ШІ та МН за рахунок впровадження інноваційних алгоритмів і розширення можливостей глибокого навчання. Наприклад, інтеграція блокчейн-технологій для зберігання та обміну біометричними даними дозволяє децентралізований підхід і тому підвищує безпеку даних, знижує ризики зламування систем та сприяє захисту конфіденційності, рис. 1.16. У поєднанні з технологіями машинного навчання блокчейн може сприяти прозорості і відстежуваності процесу ідентифікації, що є особливо важливим у фінансовій сфері, охороні здоров'я та державних установах.

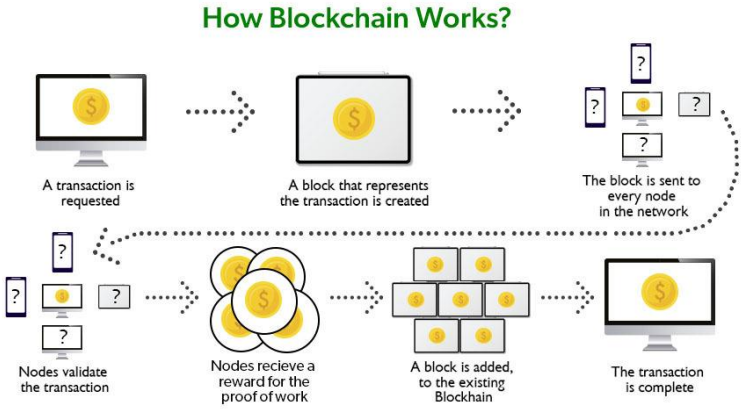


Рис. 1.16 Принцип роботи Blockchain [15]

Значний розвиток отримують також алгоритми адаптивного навчання, які дозволяють системам ідентифікації враховувати зміни в зовнішності користувачів, тобто старіння, зміна зачіски або використання аксесуарів. До того ж, ці алгоритми здатні працювати в умовах обмеженого обсягу даних, що необхідно в роботі з спеціалізованими або малими системи.

Додатково, залучення трансформерів та вже згаданих генеративно-змагальних мереж (GANs), рис. 1.17 та інших генеративних моделей, відкриває нову область для досліджень.

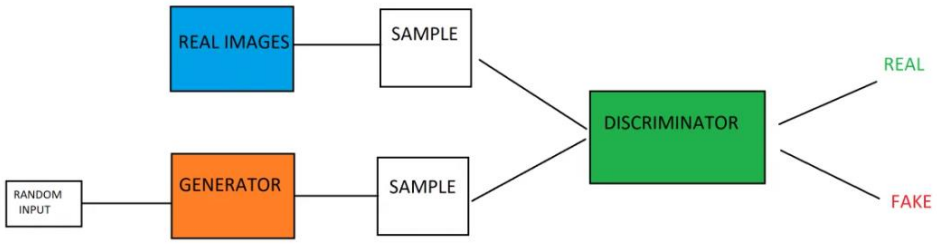


Рис. 1.17 Принцип роботи GANs [15]

У контексті глобального розвитку технологій складним питанням залишається забезпечення етичного використання ШІ та МН у системах ідентифікації. Це передбачає створення таких алгоритмів, що відповідають принципам відсутності дискримінації та захисту конфіденційності. У розділі 1.4 розглянуто різні нормативні акти, що регулюють впровадження біометричних даних, гарантують право на приватність та обмежують можливості зловживань.

1.3. Використання комп'ютерного зору в біометричних системах

Однією з ключових методик, яка забезпечує розвиток біометричних систем для ідентифікації особистості, є комп’ютерний зір. Ця технологія дозволяє автоматично розпізнавати унікальні фізичні характеристики людини: риси обличчя, відбитки пальців, райдужну оболонку ока, рухи тіла або навіть унікальні

особливості ходи. Комп’ютерний зір використовує методи обробки зображень, машинного навчання та глибоких нейронних мереж.

Типовий модуль обробки зображень формується з чотирьох основних компонентів: отримання зображення, сегментації зображення, інтерпретації зображення та вилучення ознак, специфічних для конкретного застосування, рис. 1.18.

Сегментація зображення є багатоступеневим процесом, який охоплює попередній аналіз зображення, основну сегментацію та постобробку сегментованого зображення. Попередня обробка готує дані для основного алгоритму сегментації, який виділяє ключові об'єкти або області. Постобробка спрямована на уточнення та фільтрацію результатів сегментації для досягнення більшої точності.

На етапі інтерпретації зображення виконується ідентифікації об'єктів на сцені, зокрема виявлення людини та визначення її координат. Центральним елементом цього процесу є класифікатор. Він побудований на основі нейронної мережі, який аналізує ознаки сегментованих об'єктів і визначає наявність людини. Інтерпретації критично важлива для коректності ідентифікації об'єктів у різноманітних умовах.

Додатково, можливо вилучати певні ознаки задля підвищення точності та адаптивності системи.

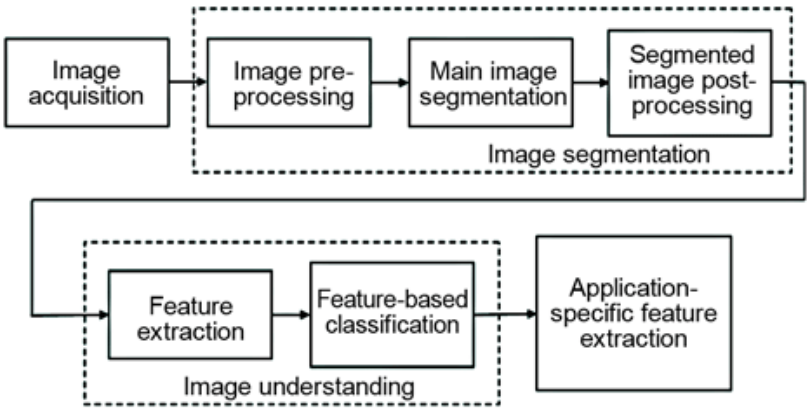


Рис. 1.18 Блок-схема процесу обробки зображень (комп'ютерного зору) [13]

Робота біометричних систем із використанням комп'ютерного зору побудована з декількох стадій. 1.19. Першим кроком є збір зображень, де системи застосовують камери або інші сенсори для отримання біометричних даних, наприклад, обличчя людини чи райдужної оболонки ока. Другий етап - попередня обробка зображень - під час якої дані проходять фільтрацію шумів, нормалізацію яскравості, корекцію контрастності та інші процедури для покращення якості вхідних даних. На третьому етапі виконується екстракція ознак, коли виділяються специфічні характеристики об'єкта, тобто, форма очей чи відстань між рисами обличчя. Для цього часто користуються глибокими нейронними мережами Convolutional Neural Networks (CNN). Четвертим етапом є порівняння з базою даних, де виділені ознаки зіставляються із шаблонами, що зберігаються в базі. На фінальному етапі система приймає рішення щодо ідентифікації та верифікації особи.

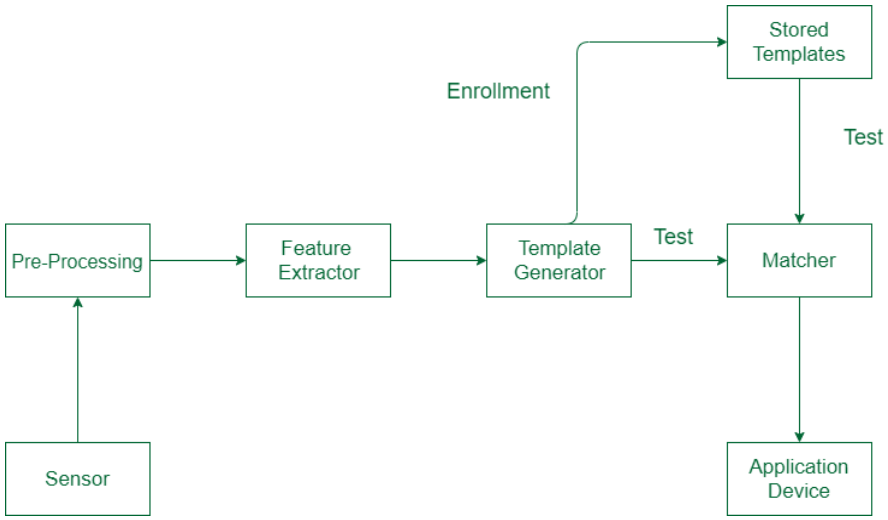


Рис. 1.19 Архітектура біометричної системи [15]

Комп'ютерний зір дозволяє досягти високої акуратності ідентифікації навіть за умов низької якості зображень або складних освітлювальних умов. Сучасні методи на основі глибокого навчання, як FaceNet або DeepFace, забезпечують точність розпізнавання обличчя понад 99% [16]. Крім того, системи з використанням комп'ютерного зору можуть працювати в реальному часі, що є визначальним для застосувань у сфері безпеки.

Найпоширенішою підкатегорією комп’ютерного зору є розпізнавання обличчя. Першим кроком такого процесу, рис. 1.20, є виявлення обличчя, під час якого система знаходить обличчя на зображенні та створює навколо нього обмежувальну рамку (bounding box). Це дозволяє виділити об'єкт для подальшої обробки.

На другому етапі виконується вирівнювання обличчя. Виявлене обличчя нормалізується, що дозволяє усунути варіації, пов’язані з кутом нахилу, освітленням та розміром. Вирівнювання є невід’ємним для підвищення точності системи: дослідження показують, що лише цей етап може збільшити точність розпізнавання обличчя на 1% або більше.

Третім етапом є вилучення ознак, де зображення аналізується для отримання локальних характеристик, як контури, текстури та геометричні властивості. Для цього інтегрують спеціалізовані алгоритми глибоких нейронних мереж або методів комп'ютерного зору. Ці ознаки є принциповими для подальшого етапу.

Останнім кроком є розпізнавання обличчя, яке передбачає зіставлення отриманих ознак з базою даних, що містить попередньо збережені зображення облич. Метою цього етапу є ідентифікація особи, до якої належить вхідне зображення. Для цього можуть бути задіяні Support Vector Machines (SVM), Convolutional Neural Networks (CNN) або інші методи глибокого навчання.

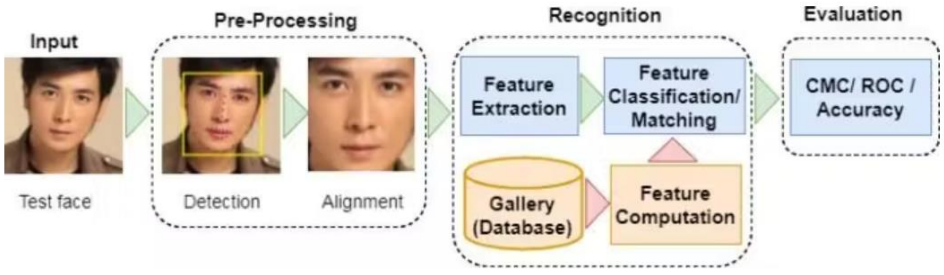


Рис. 1.20 Архітектура біометричної системи [16]

Ранні дослідження розпізнавання облич були зосереджені на методах обробки зображень для підбору простих ознак, що описують геометрію облич.

Незважаючи на те, що ці методи працювали лише за дуже вузьких налаштувань, вони показали, що можна експлуатувати комп'ютери для автоматичного розпізнавання облич. Після цього набули популярності методи статистичних підпросторів, зокрема аналіз головних компонентів (PCA) і лінійний дискримінантний аналіз (LDA). Ці методи називають ахолістичними, оскільки вони впроваджують всю область обличчя як вхідні дані. Одночасно, прогрес в інших областях комп'ютерного зору призвів до розробки локальних екстракторів ознак, які здатні описувати текстуру зображення в різних місцях. У загальному, підходи до розпізнавання обличчя на основі рис полягають у зіставленні цих локальних особливостей на зображеннях обличчя. Цілісні методи та методи, засновані на ознаках, отримали подальший розвиток і об'єднані в гібридні методи. Системи розпізнавання облич, засновані на гібридних методиках, залишалися найсучаснішими донедавна, коли глибоке навчання стало провідним підходом до більшості програм комп'ютерного зору, включно з розпізнаванням облич.

Перші технології, спрямовані на автоматичне розпізнавання облич, користувалися спеціалізованими детекторами контурів і країв для визначення місцеположення набору рис обличчя та вимірювання відносних відстаней між ними. Це, зокрема, включає використання геометричних характеристик: відстані Прокрустеса між двома наборами рис або порівняння відстаней між ними, що виражається через формулу:

$$d(\mathcal{P}_1, \mathcal{P}_2) = \|\mathcal{P}_1 - \mathcal{P}_2\|_F \tag{1.1}$$

де *P1, P2* - це координати двох наборів рис обличчя;

|| ||*F* - норма Фробеніуса, що вимірює відстань між двома точками в просторі [17].

Такі методи застосовуються для швидкого розпізнавання обличчя, до прикладу, в 3D-зображеннях, де глибина та тривимірні орієнтири є вагомими.

Холістичні методи працюють з усією областю обличчя. Одним із популярних підходів є залучення аналізу головних компонент (PCA), що дозволяє проектувати зображення обличчя на низькорозмірний простір, який зберігає найважливіші

характеристики для задачі розпізнавання. У цьому випадку, основним кроком є знаходження власних векторів, що описують найбільші варіації в наборі зображень. Математично цей процес можна виразити через наступну задачу:

$$\max_{\mathbf{W}} \|\mathbf{XW}\|_F \tag{1.2}$$

де *X* - це матриця всіх зображень;

W- матриця власних векторів, яка максимізує дисперсію зображень у проекційному просторі [17].

Цей принцип дає можливість скоротити розмірність простору зображень, зберігаючи основні варіації для розпізнавання. Однак проблема з цим методом полягає в тому, що він може максимізувати варіацію, яка не має відношення до розпізнавання (наприклад, варіації, пов'язані з освітленням, позою чи виразом обличчя).

Для подолання цих обмежень можливо залучити метод лінійного дискримінантного аналізу (LDA), який мінімізує внутрикласову дисперсію і максимізує міжкласову дисперсію. Математично це можна виразити формулою:

$$W^* = \arg\max_W \left(\frac{W^T S_b W}{W^T S_w W} \right) \tag{1.3}$$

де *Sb* - це міжкласова матриця дисперсії;

Sw - класова матриця всередині дисперсії, обчислена за допомогою класів Ck та відповідних середніх значень μk [17].

Як наслідок, виявлення найбільш дискримінантних ознак обличчя та застосування їх для покращення точності розпізнавання стає простішим.

Технології, засновані на ознаках, зосереджуються на екстракції локальних характеристик з різних частин зображення обличчя. Вони стійкіші до змін виразів обличчя чи освітлення. Так, популярним є залучення бінарних ознак, наприклад, локальних бінарних патернів (LBP), що дозволяє створювати дескриптори з

локальних областей обличчя. Ці дескриптори можна впроваджувати для порівняння з іншими зображеннями за допомогою відстані Хі-квадрат:

$$\chi^2(a,b) = \sum_i w_i \frac{(a_i - b_i)^2}{a_i + b_i} \tag{1.4}$$

де *ai, bi* - це значення дескрипторів у різних точках;

wi - ваги, які визначають вплив кожного елементу.

Інший метод, що експлуатує локальні дескриптори, грунтується на інваріантних до масштабу та обертів ознаках SIFT (Scale-Invariant Feature Transform). Він дозволяє знаходити ключові точки на зображеннях, що дають можливість порівнювати зображення обличчя за допомогою відповідних дескрипторів. Математично процес полягає у створенні дескриптора для кожної точки зображення за багатоетапного аналізу та порівняння їх через евклідову відстань.

Гібридні методи поєднують в собі як холістичні, так і методи на основі ознак. Наприклад, у методі, що комбінує LBP з проекцією на простір PCA та LDA, можна спочатку екстрагувати дескриптори LBP з локальних регіонів, а потім проектувати їх на дискримінантний простір за допомогою методів зниження розмірності. Це дозволяє комбінувати переваги обох підходів, зберігаючи компактність та інформативність ознак.

Проте для досягнення ще більшої точності та адаптивності до складних варіацій, таких як зміни освітлення, виразів обличчя або кута зору, все більше популярності набувають методи глибинного навчання. Конволюційні нейронні мережі (CNN) є найбільш поширеним типом методів глибинного навчання для розпізнавання облич. Основна перевага методів глибинного навчання полягає в тому, що вони можуть бути навчені на великих обсягах даних для навчання представлення облич, яке є стійким до варіацій, що присутні в тренувальних даних. Тобто, замість того, щоб розробляти спеціалізовані ознаки, які є стійкими до різних типів внутрішньо класових варіацій (наприклад, освітлення, поза, вирази обличчя, вік тощо), CNN можуть навчати їх на основі тренувальних даних. Основний

недолік методів глибинного навчання полягає в тому, що для їх навчання потрібні дуже великі набори даних, що містять достатньо варіацій для узагальнення на невідомі зразки. На щастя, кілька великих наборів даних облич, що містять зображення в умовах реального світу, нещодавно були випущені в публічний доступ для навчання моделей CNN. Окрім навчання дискримінативних ознак, нейронні мережі можуть знижувати розмірність і використовуватись як класифікатори або за допомогою підходів до навчання метрик. CNN вважаються системами, що навчаються від початку до кінця, і не потребують комбінації з іншими специфічними методами.

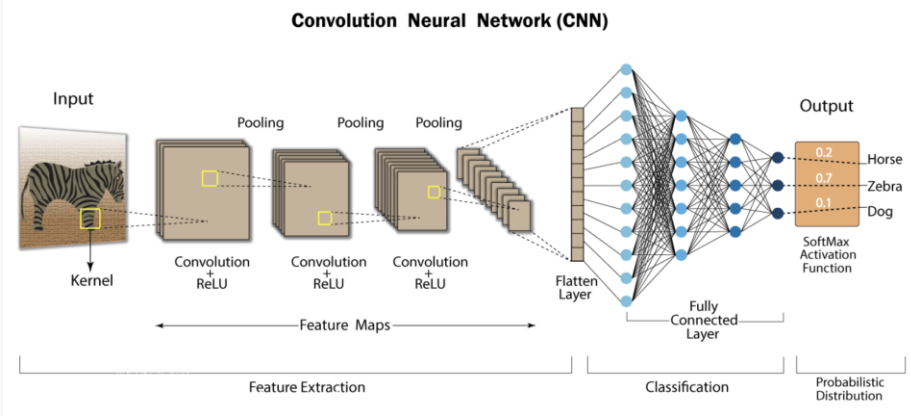


Рис. 1.21 Архітектура згорткової нейронної мережі (CNN) [13]

Моделі CNN для розпізнавання облич можна навчати різними підходами. Один із них полягає в розумінні задачі як класифікація, де кожен суб'єкт у тренувальному наборі відповідає класу. Після навчання модель можна експлуатувати для розпізнавання суб'єктів, які не присутні в тренувальному наборі, відкинувши етап класифікації і оперуючи ознаками попереднього етапу як представлення обличчя. У літературі з глибинного навчання ці ознаки зазвичай називаються ознаками вузької смуги. Після цього етапу навчання, модель можна додатково тренувати з іншими техніками для оптимізації ознак вузької смуги для цільового застосування (наприклад, спільний Бейєсівський підхід або донавчання моделі CNN з використанням іншої функції втрат). Інший поширений підхід до навчання представлення обличчя полягає в тому, щоб безпосередньо навчати

ознаки вузької смуги, оптимізуючи метрику відстані між парами облич [18] або трійками облич [19].

Ідея впровадження нейронних мереж для розпізнавання облич не є новою. Ранній метод, заснований на ймовірнісній нейронній мережі для прийняття рішень (PBDNN) [20], був запропонований у 1997 році для виявлення облич, локалізації очей і розпізнавання облич. PBDNN для розпізнавання облич був поділений на одну повністю з'єднану підмережу для кожного тренувального суб'єкта з метою зменшення кількості прихованих одиниць і запобігання перенавчанню. Два PBDNN були навчено з використанням інтенсивних і контурних ознак відповідно, а їхні виходи були комбіновані для прийняття фінального рішення про класифікацію. Інший ранній метод запропонував використання поєднання самонавчальної карти (SOM) і конволюційної нейронної мережі. Самонавчальна карта - це тип нейронної мережі, яка навчається без нагляду і проектує вхідні дані в нижчий вимір, зберігаючи топологічні властивості вхідного простору (тобто, входи, які знаходяться поруч у початковому просторі, будуть також поруч у вихідному просторі). Важливо зазначити, що жоден з цих двох ранніх методів не був вивченим від початку до кінця, а запропоновані архітектури нейронних мереж були поверхневими.

Методи глибинного навчання для розпізнавання облич набули популярності, коли ці моделі були масштабовані та навчалися на великих обсягах даних, що призвело до досягнення передових результатів. Зокрема, система DeepFace компанії Facebook, одна з перших підходів на основі CNN для розпізнавання облич, що використовує модель з великою потужністю, досягла точності 97.35% на еталонному наборі LFW, зменшивши помилку попереднього передового методу на 27% [17]. Автори тренували CNN з функцією втрат softmax, використовуючи набір даних, що містить 4,4 мільйона облич від 4,030 суб'єктів. У цій роботі були зроблені два нових внески: (i) ефективна система вирівнювання облич на основі явного 3D-моделювання облич і (ii) архітектура CNN, що містить локально з'єднані етапи, які, на відміну від регулярних конволюційних етапи, можуть навчати різні ознаки для кожної області на зображенні. Паралельно система DeepID досягла подібних

результатів, тренуючи 60 різних CNN на патчах, що складаються з десяти областей, трьох масштабів і RGB або сірого каналів.

Розрізняють три основні фактори, що впливають на точність методів CNN для розпізнавання облич: тренувальні дані, архітектура CNN і функція втрат. Як і в більшості застосувань глибинного навчання, для запобігання перенавчанню необхідні великі тренувальні набори. CNN стають точнішими з більшим числом зразків на клас, оскільки модель навчається стійким ознакам при варіаціях всередині класу. Однак для розпізнавання облич важливо, щоб тренувальні набори містили велику кількість суб'єктів, щоб модель могла узагальнювати ознаки для нових осіб.

Розглядаючи глибше концепт DeepFace - це легкий фреймворк для розпізнавання облич, розроблений для мови програмування Python. Він базується на гібридному методі, що інтегрує передові моделі, такі як VGGFace, FaceNet, DeepFace, Dlib тощо. Фреймворк переважно використовує три модулі: DeepFace для роботи з обличчями, OpenCV для зчитування вхідних зображень та Matplotlib для візуалізації результатів.

Для роботи необхідно встановити та імпортувати всі потрібні бібліотеки у середовищі Python, як показано на рис. 1.22 та рис. 1.23.

```
pip install deepface
pip install opencv-python
pip install matplotlib
```

Рис. 1.22 Встановлення бібліотек у середовищі Python [16]

```
from deepface import DeepFace
import cv2
import matplotlib.pyplot as plt
```

Рис. 1.23 Імпортування встановлених бібліотек у середовищі Python [16]

Після цього, визиваючи метод “verify”, рис. 1.24, із двома зображеннями, можна буде побачити, чи обличчя належить одній і тій самій особі, приклад наведено на рис. 1.25.

```
def verify(img1_path,img2_path):
    img1= cv2.imread(img1_path)
    img2= cv2.imread(img2_path)

    plt.imshow(img1[:,:,::-1])
    plt.show()
    plt.imshow(img2[:,:,::-1])
    plt.show()    output = DeepFace.verify(img1_path,img2_path)
    print(output)
    verification = output['verified']
    if verification:
        print('They are same')
    else:
        print('The are not same')
```

Рис. 1.24 Код методу verify [16]

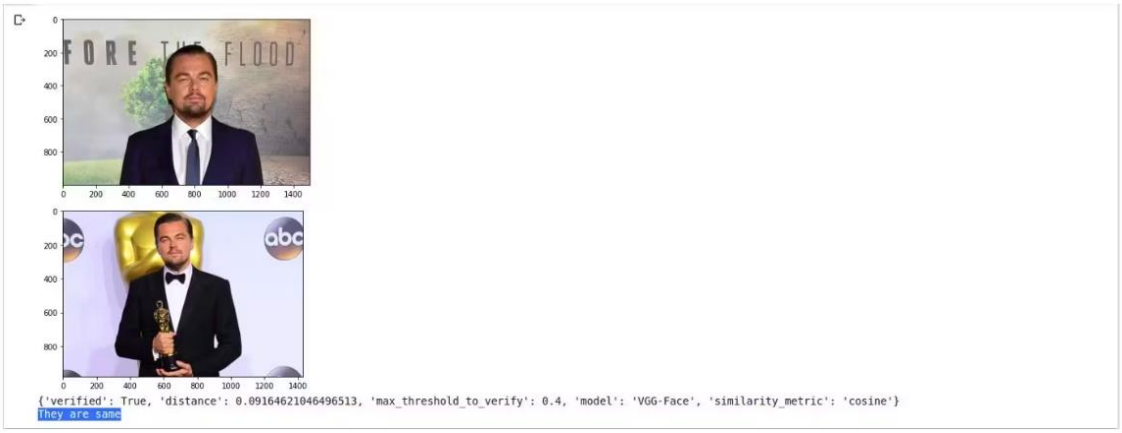


Рис. 1.25 Приклад роботи функції verify [16]

Попри високу ефективність, технологія комп’ютерного зору має низку технічних викликів. Наприклад, розпізнавання обличчя може бути ускладнене через зміну освітлення, пози чи наявність масок, як показано на рис. 1.26.

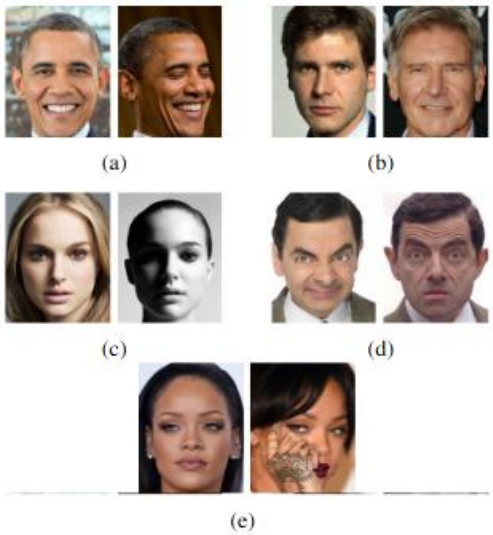


Fig. 1: Typical variations found in faces in-the-wild. (a) Head pose. (b) Age. (c) Illumination. (d) Facial expression. (e) Occlusion.

Рис. 1.26 Приклади ускладнення розпізнавання обличчя [17]

Також виникають питання конфіденційності даних, що потребує відповідних регуляторних рішень. Із розвитком алгоритмів глибокого навчання та зростанням обчислювальних можливостей очікується значне покращення точності та швидкості роботи біометричних систем. Використання новітніх технологій, таких як генеративно-змагальні мережі (GANs), дозволить створювати більш стійкі до атак системи, а інтеграція з блокчейном забезпечить додатковий рівень захисту даних. Комп’ютерний зір у біометричних системах є важливим інструментом для розширення можливостей автоматизації ідентифікації та підвищення рівня безпеки в різних галузях.

1.4. Етичні та правові аспекти використання біометричних даних

Біометричні дані є особливо чутливими, оскільки вони пов'язані з фізіологічними та поведінковими характеристиками особи. Їх збір і обробка можуть порушувати право на приватність, якщо ці дані використовуються без згоди власника або з порушенням чинних законів. У багатьох країнах

законодавство регулює збір, зберігання та обробку біометричних даних. Наприклад, в Європейському Союзі діє Загальний регламент про захист даних (GDPR), який вимагає отримання чіткої згоди від особи на обробку її біометричних даних.

Оскільки біометричні дані є постійними і важливими ідентифікаторами, їх втрата або несанкціонований доступ до них можуть призвести до серйозних наслідків, таких як шахрайство або крадіжка особистої інформації. Тому важливим аспектом є безпека систем, що зберігають біометричні дані. Враховуючи високий ризик, такі дані повинні бути надійно захищені від несанкціонованого доступу та повинна існувати чітка політика зберігання та обробки даних.

За даними на 2024 рік, у Сполучених Штатах Америки понад 405 компаній використовуватимуть біометричні інструменти безпеки, рис. 1.27. Лідером на ринку біометричних технологій є компанія Source, яка займає 51,36% ринку та має 208 клієнтів у США. Далі йдуть компанії CrossMatch з часткою ринку 17,04% (69 клієнтів), DataGrail (7,41% і 30 клієнтів), Vision-Box (6,67% і 27 клієнтів) та Ikena Forensic (4,69% і 19 клієнтів). Інші біометричні технології мають наступні частки ринку: EveVerify - 3,70%, Omega Technology - 2,96%, Tascent - 0,99%, eSSL - 0,74% та Dyadic - 0,74%.

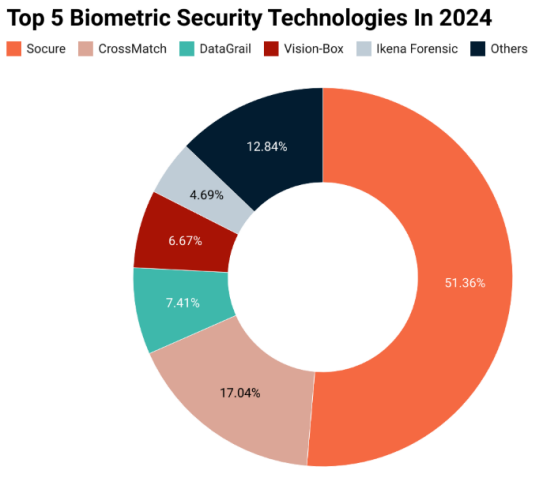


Рис. 1.27 Топ 5 біометричних технологій безпеки з 2024 р. [22]

Отже, біометричні технології вже стали важливим інструментом для забезпечення безпеки в різних сферах діяльності, що підтверджує їх швидкий розвиток та зростання попиту. Проте, з цим пов’язані й серйозні виклики у контексті захисту даних, що вимагає постійного вдосконалення механізмів безпеки та обробки біометричних даних.

Одна з головних етичних проблем використання біометричних даних полягає в обов'язку отримати явну і добровільну згоду від осіб, яких стосуються ці дані. У деяких випадках збір таких даних може відбуватись без повного усвідомлення користувачами наслідків та ризиків, які це може спричинити. Тому важливо, щоб системи, що обробляють біометричні дані, були прозорими про мету використання таких даних, а також методів їх зберігання та обробки. Прикладом закону про умови згоди є п.7 “Умови згоди” з Загального Регламент про Захист Даних (GDPR) [21].

Коли обробка даних ґрунтується на згоді, контролер повинен бути здатний продемонструвати, що суб'єкт даних надав свою згоду на обробку своїх персональних даних. Якщо згода надається в контексті письмової заяви, що також стосується інших питань, запит на згоду має бути чітко відокремлений від інших аспектів, поданий у зрозумілій і легкодоступній формі, з використанням чіткої та простої мови. Будь-яка частина такої заяви, що порушує вимоги регламенту, не матиме юридичної сили [21].

Суб'єкт даних має право в будь-який час відкликати свою згоду. Відкликання згоди не впливає на законність обробки даних, здійсненої до його відкликання. Перед наданням згоди суб'єкт має бути проінформований про це, і процес відкликання згоди має бути таким же простим, як і її надання [21]. Окрім цього, біометричні системи можуть бути піддані викривленням і помилкам, які призводять до дискримінації, наприклад, на основі статі, раси чи віку.

Неправомірне використання цих даних може призвести до ситуацій, коли окремі категорії осіб втрачають доступ до певних послуг або піддаються несправедливим переслідуванням. Зокрема, це стосується ситуацій, коли біометрична ідентифікація використовується для масового спостереження або

автоматичних систем контролю. Згідно зі звітом TransUnion на рис. 1.28, випадки шахрайства з використанням викрадених особистих даних збільшилися на 113% у період з 2019 по 2023 рік, тоді як Федеральна торговельна комісія (FTC) повідомляє про зростання кількості скарг на 54% за той самий період. У 2020 та 2021 роках кількість скарг досягла рекордного рівня - 1,4 мільйона щороку, що на 115% більше, ніж у 2019 році. Статистичні дані FTC за цей період свідчать, що 76% випадків крадіжки особистих даних у 2021 році були пов’язані з використанням існуючих рахунків жертв. У 2021 році 25% постраждалих дізналися про інцидент завдяки повідомленням від фінансових установ, 19% - виявивши підозрілу активність на своїх рахунках, і лише 9% - помітивши втрату грошей. Найчастіше жертвами ставали американці віком від 30 до 39 років, які у 2023 році становили 30% усіх зареєстрованих випадків. Близько 30% жертв повідомили, що вони стикалися з кількома типами крадіжок особистих даних протягом свого життя, але понад половину постраждалих (56%) змогли вирішити свої проблеми протягом одного дня або менше. У 2023 році серед осіб віком до 19 років найпоширенішими видами шахрайства були ті, що пов’язані з працевлаштуванням або податками (62%). Крадіжка особистих даних лідирувала серед усіх шахрайських випадків, становлячи 94% звітів, за нею йшли фішингові атаки (88%) та шахрайства в онлайн-знайомствах (82%). У 2021 році найбільші фінансові втрати, пов’язані з крадіжкою даних - $3,4 тис. на одну особу - спостерігалися у випадках, коли дані використовувалися для відкриття нових рахунків, таких як кредитні чи банківські. Водночас жертви шахрайств із використанням кредитних карток у середньому втрачали $620 [23].

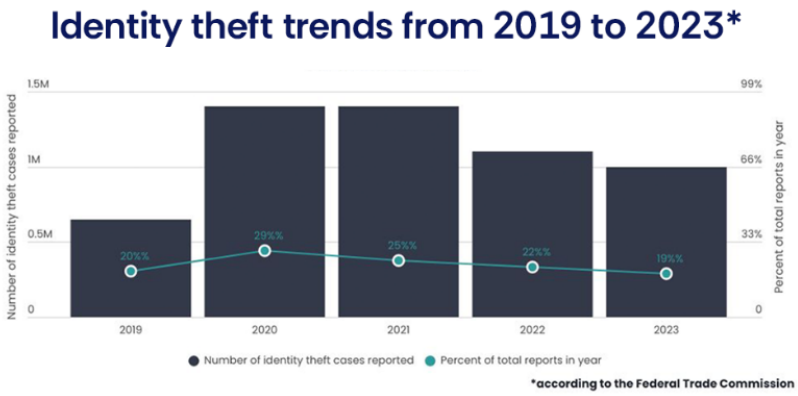


Рис. 1.28 Тенденції крадіжки особистих даних 2019-2023 рр. [23]

Так, наприклад, функція “Крип” виникає, коли інформація використовується для інших цілей, ніж ті, для яких вона була зібрана. Це стає серйозною проблемою, коли другорядне використання інформації не повідомляється особам під час надання ними своїх даних.

Ще однією загрозою для приватності є таємне або пасивне збирання біометричної інформації без згоди, участі чи обізнаності осіб. Наприклад, біометричні дані про обличчя можуть бути зібрані з фотографій, що робляться, коли люди не знають про це, а латентні відбитки пальців можуть бути зібрані з поверхонь, до яких люди торкались, навіть після того, як вони залишили їх. Ця загроза зростає з розвитком технологій, здатних непомітно збирати біометричну інформацію, або робити це на відстані.

На рис. 1.29 та рис. 1.30 проаналізовано профілі жертв крадіжки особистих даних, включаючи їхній вік, способи виявлення шахрайства, подальші дії та інші аспекти. Згідно з даними за 2023 рік, більшість жертв становили представники покоління міленіалів (37%) та покоління X (29%). Крадіжка особистих даних частіше трапляється у жінок (54%), ніж у чоловіків (46%). Білі американці складають 70% жертв, за ними йдуть латиноамериканці (12%) та афроамериканці (11%). Найбільшою групою жертв у 2021 році були люди, які заробляють від $50 до $100 тис. на рік, і вони становили 32% від загальної кількості постраждалих. Найменшою групою були особи з доходом понад $200 тис. на рік - 11%. У 86% випадків жертви успішно вирішували фінансові або кредитні проблеми після

інциденту. Серед постраждалих 71% змінили паролі на фінансових рахунках, у той час як серед тих, хто не ставав жертвою, це зробили лише 48%. Однак 43% американців не знають, які дії потрібно вжити у разі онлайн-атаки, і лише 39% жертв знали, до кого звертатися та як повідомляти про крадіжку особистих даних.

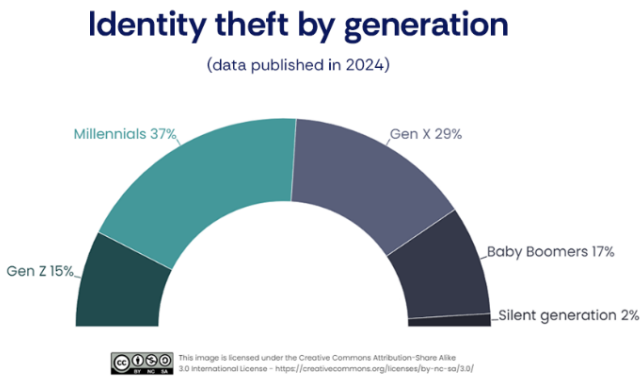


Рис. 1.29 Крадіжка особистих даних за генерацією [23]

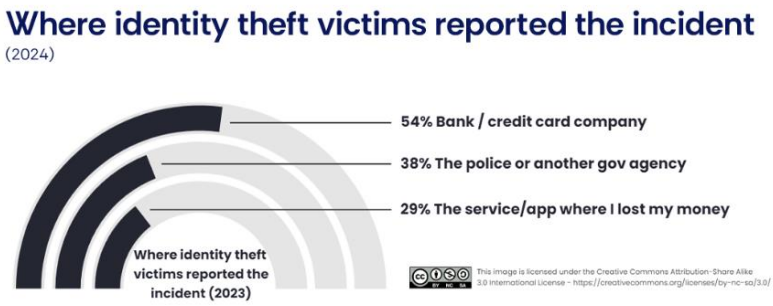


Рис. 1.30 Розподіл звернень жертв крадіжки особистих даних 2024 р. [23]

Отже, біометричні технології потребують ретельного регулювання на рівні держави. Законодавство повинно визначати чіткі межі для збору, обробки та зберігання біометричних даних, зокрема, гарантувати захист прав громадян та контролювати впровадження таких технологій. У багатьох країнах вже ухвалено закони, які стосуються біометрії (наприклад, GDPR в ЄС або Закон про біометричні дані в США), але постійно виникають нові виклики, пов'язані з розвитком технологій.

РОЗДІЛ 2 АПАРАТНА ЧАСТИНА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

2.1. Технічні вимоги до апаратної частини системи

Апаратна частина біометричних систем є основою для забезпечення їх функціональності та ефективності. Вона включає набір спеціалізованих пристроїв, що забезпечують збір, обробку, зберігання та передачу біометричних даних. Ключові апаратні компоненти біометричних систем можна умовно поділити на кілька категорій: біометричні сенсори, процесори або мікроконтролери, модулі зв’язку, засоби зберігання даних та джерела живлення. Вибір цих компонентів є критичним для функціонування системи та виконується з урахуванням вимог до точності, надійності, швидкості обробки даних, енергоспоживання й масштабованості системи. Зокрема, поширеними стандартами є ISO/IEC: ISO/IEC 19794 (біометричні дані) або ISO/IEC 30107 (біометричне розпізнавання), IP65 для захисту сенсорів від пилу та вологи, NIST SP 800-76 - Рекомендації Національного інституту стандартів США для біометричних систем, тощо.

Із метою побудови прототипу системи біометричного контролю доступу на основі зчитування відбитків пальців, створено задачу для допомоги вибору апаратного забезпечення та технічного обґрунтування.

Для забезпечення швидкої ідентифікації користувачів необхідно оцінити продуктивність обчислювальної платформи та відповідність її вимогам до швидкості ідентифікації ≤ 0.5 с. Якщо кількість користувачів 3000 осіб, а максимальне допустиме навантаження 500 запитів/день, то середній час обробки одного запиту обчислюється як:

$$T_{\text{іден}} = \frac{24 \times 60 \times 60}{500} \approx 172.8 \text{ с} \tag{2.1}$$

Оскільки система має обробляти кожен запит не більше ніж за 0.5 с, використання багатоядерного процесора ARM Cortex-A53 забезпечує відповідність цьому параметру.

Наступним кроком треба розрахувати пам’ять для зберігання шаблонів відбитків пальців. Оберемо формат збереження: ISO/IEC 19794-2, середній розмір одного шаблону - 512 байт.

$$V_{\text{пам}} = 3000 \times 2 \times 512 = 3.07\ \text{MB} \tag{2.2}$$

Отже, мінімальний обсяг пам’яті для бази відбитків - 4 МБ. Далі оцінено енергоспоживання та час автономної роботи при споживаній потужності 1 Вт, резервному часі роботи 8 год та напрузі акумулятора 12 В. Необхідна ємність акумулятора:

$$C_{\text{акум}} = \frac{1 \times 8}{12} = 0.67\ \text{Ah} \tag{2.3}$$

Тобто, рекомендовано акумулятор ≥1 Ah. Далі розраховано швидкість передачі даних. Середній розмір одного відбитка складає 512 байт, максимальне навантаження системи – 500 запитів/день, а часовий проміжок передачі – 10 мс. Отримано мінімальну швидкість передачі:

$$V_{\text{перед}} = \frac{512 \times 8}{10 \times 10^{-3}} = 409.6\ \text{kbps} \tag{2.4}$$

Тоді вибір UART (115200 bps) або Wi-Fi (≥1 Mbps) забезпечує достатню швидкість.

Важливо також конкретизувати вимоги до безпеки - для захисту даних передбачається шифрування AES-128, відповідність ISO/IEC 19794-2 та захист від несанкціонованого доступу.

Поєднавши всі вимоги, створено технічне завдання із наступними пунктами, табл. 2.1.

Таблиця 2.1

Технічне завдання (ТЗ) для апаратної частини системи біометричного контролю доступу на основі зчитування відбитків пальців

Розділ ТЗ	**Вимоги**
1. Мета та область застосування	Опис системи: "Розробка апаратної частини для біометричного контролю доступу з використанням сканера відбитків пальців". Система призначена для експлуатації в корпоративних офісах, державних установах та промислових об'єктах. Основні сценарії використання включають автоматизований контроль доступу без необхідності у фізичних ключах або картках.
2. Вимоги до функціоналу	Швидкість ідентифікації ≤ 0.5 с. Підтримка 3000 користувачів. Резервне живлення (8 год автономії) з можливістю гарячої заміни батареї. Підтримка чорних/білих списків для управління доступом. Журнал доступу з можливістю експорту даних. Інтерактивна система оповіщення (LED-індикатори, звукові сигнали при успішному або невдалому вході).
3. Апаратні вимоги	Сенсор: FAR ≤ 0.001%, роздільна здатність 500 dpi. Процесор: ARM Cortex-A53, 4 ядра. Енергоспоживання ≤ 1 Вт. Тип підключення: UART, Wi-Fi. Внутрішня пам'ять для збереження даних та швидкого оновлення списку користувачів.
4. Стандарти та безпека	Відповідність ISO/IEC 19794-2 (відбитки пальців). Шифрування AES-128 для захисту переданих даних. Сертифікація FBI PIV. Захист від несанкціонованого доступу (механізми аутентифікації адміністратора).

5. Критерії прийняття	Успішне тестування на 500 запитів/день. Відмовостійкість у умовах високої вологості (IP65). Тестування в екстремальних умовах (діапазон температур −20°C до +60°C, стійкість до пилу, механічних впливів). Допустимий рівень помилкових відмов ≤ 1% у складних умовах експлуатації.

Після обгрунтування ТЗ та вимог до апаратного забезпечення системи, досліджено відповідні апаратні компоненти в розділі 2.2.

2.2 Дослідження апаратних компонентів для біометричних систем

Найпоширенішими типами сенсорів є сканери відбитків пальців, камери для розпізнавання обличчя, сканери райдужки ока та мікрофони для розпізнавання голосу. Проаналізувавши кожну з цих категорій, було створено табл. 2.2.

Таблиця 2.2

Порівняльна характеристика типів сенсорів

Назва	**Принцип роботи**	**Технічні характеристики**	**Переваги**	**Недоліки**	**Приклади пристроїв**
Сканери відбитків пальців	Сканери захоплюють зображення відбитків пальців за допомогою оптичних, ємнісних або ультразвукових технологій.	Роздільна здатність: 500 dpi або вище. Швидкість сканування: ≤ 0.5 сек. Типи: оптичні, ємнісні,	Висока точність (до 98%). Низька вартість. Простота споживання.	Чутливість до забруднень. Можливість підробки (для дешевих моделей).	Authentec AES3500. Fingerprint Cards FPC1020.

		ультразвукові.			
Камери для розпізнавання обличчя	Камери захоплюють зображення обличчя, яке потім аналізується за допомогою алгоритмів штучного інтелекту.	Роздільна здатність: Full HD (1920*1080) або вище. Підтримка інфрачервоного освітлення (IR). Частота кадрів: ≥ 30 fps.	Можливість роботи на відстані. Невразливість до фізичного контакту.	Чутливість до освітлення. Можливість обману за допомогою фотографій.	Sony IMX477. Omnivision OV5640.
Сканери райдужки ока	Сканери захоплюють унікальні патерни райдужної оболонки ока за допомогою інфрачервоного освітлення.	Роздільна здатність: ≥ 1.3 Мп. Дальність сканування: 20–50 см. Швидкість сканування: ≤ 2 сек.	Найвища точність (до 99%). Невразливість до фізичного контакту.	Висока вартість. Повільна обробка.	IrisGuard AD100. LG IrisAccess 4000.
Мікрофони для розпізнавання голосу	Мікрофони захоплюють голосові дані, які потім аналізуються для ідентифікації особи.	Частота дискретизації: ≥ 16 кГц. Чутливість: −42 dB	Низька вартість. Простота інтеграції.	Чутливість до шуму. Нижча точність (до 90%).	Knowles SPH0645LM4H.

Отже, розглядаючи ці типи сенсорів, для задачі, де потрібна висока точність та низька вартість, обрано сканери відбитків пальців. Існує три категорії: оптичні, ємнісні та ультразвукові, рис. 2.2. Оптичні сканери дозволяють роздільну здатність від 500 dpi, що дозволяє отримувати чіткі зображення. Ємнісні сканери використовують електричне поле для захоплення відбитків, що робить їх більш стійкими до забруднень. Ультразвукові сканери гарантують акуратність за рахунок реалізації звукових хвиль.

Обраний сенсор - Suprema BioMini Plus 2, рис. 2.1. Основними критеріями вибору стали його роздільна здатність у 500 dpi, що забезпечує високу якість зображення, швидкість зчитування ≤ 0,2 с, алгоритм обробки - сертифікація FBI PIV, що гарантує відповідність міжнародним стандартам та інтерфейс USB 2.0, що спрощує інтеграцію в систему.

SPECIFICATIONS

	BioMini Plus	BioMini Plus2
Manufacturer	Xperix Inc.	
Connection	USB 2.0	
Supported OS (*)	Microsoft Windows Android Linux (x86-64)	
Resolution	500 ppi	
Image capture area (Platen size)	16 x 19 mm (0.6" x 0.7")	
Fingerprint image size	260 x 340 pixels	315 x 354 pixels
Sensor type	Optical	
Device size	66 x 90 x 58 mm (2.6" x 3.5" x 2.3")	
Operating temperature	-10°C ~ +50°C	

Рис. 2.1 Зовнішній вигляд та специфікація Suprema BioMini Plus 2 [28]

Обсяг даних, які необхідно обробити при роздільній здатності 300*400 пікселів з глибиною 8 біт на піксель один відбиток займає 120 КБ без стиснення та ≈ 30 КБ після компресії. Це дозволяє швидко передавати дані мережею без надмірного навантаження.

Процесор обробки даних - це обчислювальний модуль, що виконує аналіз зібраних даних і порівняння з еталонними зразками. Його функціонування базується на виконанні складних алгоритмів обробки зображень, машинного навчання та нейронних мереж. Наприклад, при обробці відбитка пальця процесор виконує етапи нормалізації зображення, виділення характерних мініцій (розгалужень, завершень папілярних ліній) та формування цифрового шаблону, який порівнюється із записами в базі даних, рис. 2.2. Для забезпечення високої продуктивності сучасні процесори інтегрують гетерогенні архітектури, такі як ARM Cortex-A53/A72 (для загальних обчислень), DSP (цифрові сигнальні процесори для оптимізації обробки зображень) та NPU (нейронні процесори для прискорення роботи алгоритмів ШІ).

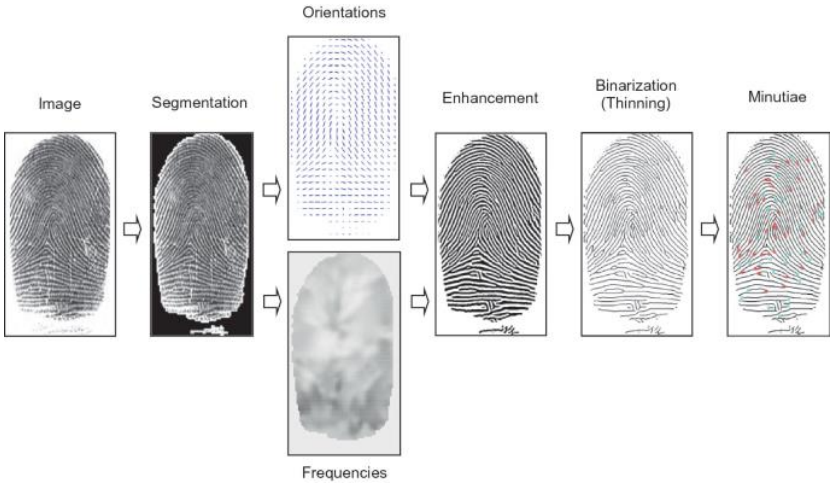


Рис. 2.2 Аналіз відбитків пальців [27]

ARM Cortex-A53 на рис. 2.3 підходить до задачі через свою високу обчислювальну здатність (до 1,2 ГГц), чотири ядра для ефективної багатозадачності та підтримку складніших біометричних алгоритмів. Хоча його енергоспоживання більше, ніж у, наприклад, ARM Cortex-M4, він все ще забезпечує хорошу енергоефективність для складних обчислень. Цей процесор буде корисний для обробки великих обсягів біометричних даних та реалізації точних алгоритмів розпізнавання, що дозволяє масштабувати систему в майбутньому.

1.2.1 ARM architecture

The Cortex-A53 processor implements the ARMv8-A architecture. This includes:

- Support for both AArch32 and AArch64 Execution states.
- Support for all exception levels, EL0, EL1, EL2, and EL3, in each execution state.
- The A32 instruction set, previously called the ARM instruction set.
- The T32 instruction set, previously called the Thumb instruction set.
- The A64 instruction set.

The Cortex-A53 processor supports the following architecture extensions:

- Optional Advanced SIMD and Floating-point Extension for integer and floating-point vector operations.

  Note

  — The Advanced SIMD architecture, its associated implementations, and supporting software, are commonly referred to as NEON technology.

  — To perform floating-point operations, you must implement the Advanced SIMD and Floating-point Extension. There is no software API library for floating-point in the ARMv8-A architecture.

  — You cannot implement floating-point without Advanced SIMD.

- Optional ARMv8 Cryptography Extensions.

  Note

  You cannot implement the Cryptography Extensions without Advanced SIMD and Floating-point.

See the *ARM® Architecture Reference Manual ARMv8, for ARMv8-A architecture profile* for more information.

Рис. 2.3 Зовнішній вигляд та специфікація ARM Cortex-A53 [29]

Контролери доступу - електронні пристрої, що керують механізмами відкриття дверей або активації доступу. Для управління процесом аутентифікації та відкриття дверей обрано контролер ZKTeco InBio460, рис. 2.4. Його перевагами є кількість підтримуваних користувачів 3000, тобто більше, ніж у альтернативних рішень, як HID VertX V1000, кількість точок доступу - до 4 дверей на один контролер, що підходить для офісних будівель, підтримка RS-485 - зменшує затримки при обробці запитів та шифрування: AES-128 забезпечує безпечну передачу даних. Середній час обробки одного запиту становить 0,3-0,5 с, що відповідає заданим вимогам швидкодії.

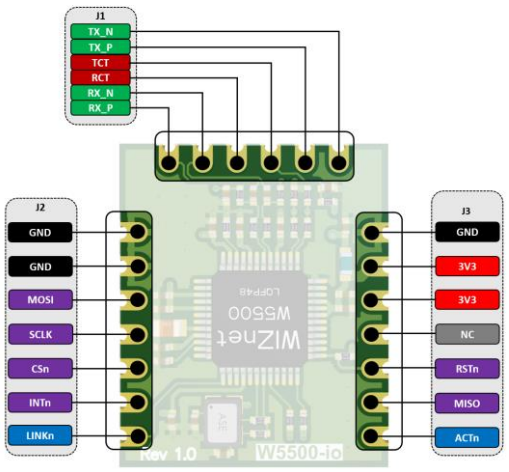
	inBio-160	inBio-260	inBio-460
Number of doors controller	1 Door	2 Door	4 Door
Numbers of readers supported	4 (2 RS-485 Reader, 2 26-bit wiegand reader)	8 (4 RS-485 Reader, 4 26-bit wiegand reader)	12 (8 RS-485 Reader, 4 26-bit wiegand reader)
Types of readers supported	26-bit Wiegand and RS485 FR Series Reader	26-bit Wiegand and RS485 FR Series Reader	26-bit Wiegand and RS485 FR Series Reader
Number of Inputs	3(exit Device and Door Status, 1 AUX)	6(2 Exit Device, 2 Door Status, 2 AUX)	12(4 Exit Device, 4 Door Status, 4 AUX)
Number of Outputs	2 (1-Form C Relay for Lock and One Form C Relay for Aux Output)	4 (2-Form C Relay for Lock and 2-Form C Relay for Aux Output)	8 (4-Form C Relay or Lock and 4-Form C Relay for Aux Output)
Card holders Capacity	30,000	30,000	30,000
Fingerprint Capacity	3,000	3,000	3,000
Log Events Capacity	100,000	100,000	100,000
Communication	TCP/IP and RS-485	TCP/IP and RS-485	TCP/IP and RS-485
Package Dimension	350(L)×90(H)×300(W)mm	350(L)×90(H)×300(W)mm	350(L)×90(H)×300(W)mm
Package Weight	3.6kg	3.6kg	3.7kg
CPU	32 bit 400MHz CPU	32 bit 400MHz CPU	32 bit 400MHz CPU
RAM	32M	32M	32M
Flash Memory	128M	128M	128M
Power	9.6V-14.4V DC	9.6V-14.4V DC	9.6V-14.4V DC
Operating Temp	0-45 °C	0-45 °C	0-45 °C
Operating Humidity	20% to 80%	20% to 80%	20% to 80%

Рис. 2.4 Зовнішній вигляд та специфікація ZKTeco InBio 460 [30]

Комунікаційні модулі - засоби для передачі даних між сенсорами, серверами та іншими елементами системи (Wi-Fi, Bluetooth, Ethernet тощо). Для забезпечення зв'язку між компонентами системи використовується комбінація Wiznet W5500 (Ethernet) та ESP32 (Wi-Fi). Обґрунтування вибору:

Характеристику Wiznet W5500 зображено на рис. 2.5. Його апаратна реалізація - TCP/IP, що робить навантаження на контролер мінімальним. Пропускна здатність становить 100 Mbps, споживана потужність - 0,18 Вт.

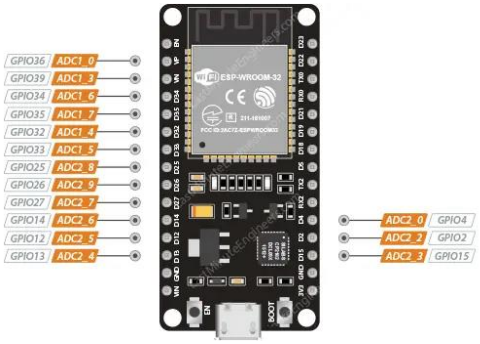
ESP32 (Wi-Fi) на рис. 2.6 має двохядерний Xtensa LX6 (240 МГц) та підтримку WPA2-Enterprise для безпечного зв'язку. Енергоспоживання в режимі очікування становить 0,01 Вт, у режимі передачі 0,8 Вт. Система обробляє 500 запитів на день, кожен з яких передає ≈ 30 КБ даних. Загальний добовий трафік становить 15 МБ, що легко обробляється мережею 100 Mbps.



DATA SHEET

Embedded Core	TCP/IP, MAC & PHY
Host Interface	Fast SPI
TX/RX Buffer	32KB
Number of Hardware Socket	8
Network Performance	Max 15Mbps
Operation Temp (°C)	-40 ~ 85
Process	0.13μm
Package Type	48LQFP (7x7)

Рис. 2.5 Зовнішній вигляд та технічний паспорт Wiznet W5500 [31]



Categories	Items	Specifications
Certification	RF certification	FCC/CE-RED/IC/TELEC/KCC/SRRC/NCC
	Bluetooth certification	BQB
	Green certification	RoHS, REACH
Test	Reliablity	HTOL/HTSL/uHAST/TCT/ESD
Wi-Fi	Protocols	802.11 b/g/n (802.11n up to 150 Mbps)
		A-MPDU and A-MSDU aggregation and 0.4 μs guard interval support
	Frequency range	2.4 GHz ~ 2.5 GHz
Bluetooth	Protocols	Bluetooth v4.2 BR/EDR and BLE specification
	Radio	NZIF receiver with –97 dBm sensitivity
		Class-1, class-2 and class-3 transmitter
		AFH
	Audio	CVSD and SBC
Hardware	Module interfaces	SD card, UART, SPI, SDIO, I²C, LED PWM, Motor PWM, I²S, IR, pulse counter, GPIO, capacitive touch sensor, ADC, DAC
	On-chip sensor	Hall sensor
	Integrated crystal	40 MHz crystal
	Operating voltage/Power supply	2.7 ~ 3.6V
	Minimum current delivered by power supply	500 mA
	Recommended operating temperature range	–40°C ~ 65°C
	Package size	(18.00±0.10) mm x (31.40±0.10) mm x (3.30±0.10) mm

Рис. 2.6 Зовнішній вигляд та специфікація ESP32 [32]

Блоки живлення - це модулі, що забезпечують стабільну роботу всіх компонентів системи. Для стабільної роботи системи обрано Mean Well HDR-15-12 у поєднанні з резервним акумулятором Yuasa NP7-12. Причинами вибору стали вихідна напруга 12 В, 1.25 А, ККД > 85% та захист від перевантаження для Mean Well HDR-15-12, рис. 2.7. Для Yuasa NP7-12, зображеного на рис. 2.8 – ємність в 7 А/год, автономна робота при споживанні 0,8 А – ≈8 годин без живлення.

Specifications

Technical data		Information	
Brand	MEAN WELL	Commodity	8504408390
Item number	HDR-15-12	Warranty pack	36 Months Bring-In
Series	HDR-15	RoHS	Compliant
Description	AC-DC Ultra slim DIN rail power supply; Input range 85-264VAC; Output 12VDC at 1.25A; Pass LPS	Packing quantity	160
Application	Installation UL 508 IT AV EN/UL/IEC 62368-1	Net weight (gram)	70
Technology	AC/DC		
Power Format	DIN rail		
Output Power (W)	15		
Output Voltage (V)	12		
Output Current (A)	1.25 1.25		
Input Voltage (V)	110/230 universal input 85 - 264		
IP Rating	No IP assigned		
Width (mm)	67		
Height (mm)	24		
Depth (mm)	97		
Dimming Technology	No Dimming		

Рис. 2.7 Зовнішній вигляд та технічний паспорт Mean Well HDR-15-12 [32]

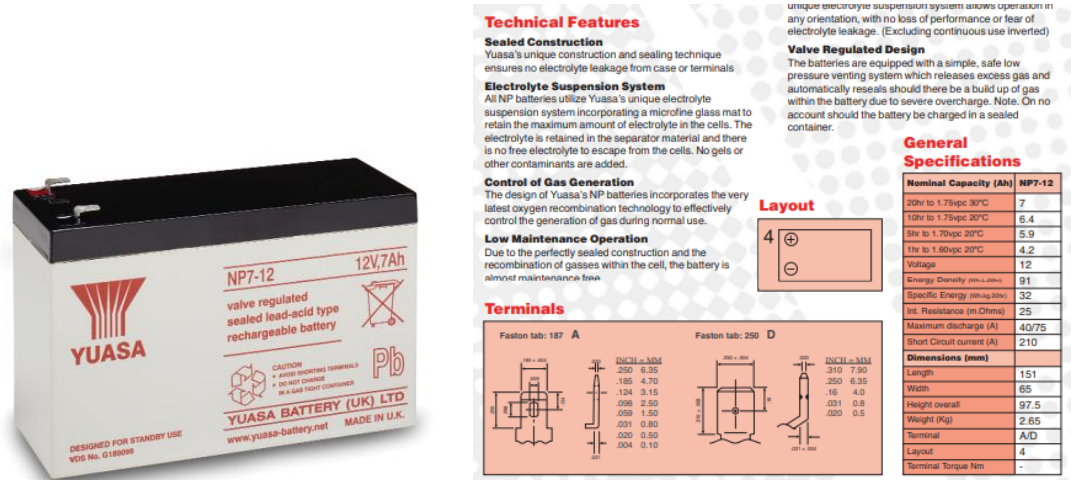


Рис. 2.8 Зовнішній вигляд та технічний паспорт Yuasa NP7-12 [34]

Обрані апаратні компоненти забезпечують швидку та надійну ідентифікацію користувачів, стійкість до зовнішніх умов та відповідність міжнародним стандартам безпеки. Завдяки резервному живленню та підтримці сучасних методів шифрування система гарантує безперервну роботу та захист від несанкціонованого доступу. Обгрунтувавши всі ці аспекти можна стверджувати, що запропоноване технічне рішення відповідає поставленим завданням і може бути інтегроване у широкий спектр застосувань, зокрема в корпоративних, державних та промислових об’єктах.

2.3. Інтеграція біометричних сенсорів у систему контролю доступу

Інтеграція біометричних сенсорів у систему контролю доступу є важливим елементом, що забезпечує точність та безпеку процесу ідентифікації користувачів. Задля безперешкодної та безпечної роботи системи, усі її компоненти (процесори, контролери доступу та комунікаційні модулі) повинні працювати синхронно з біометричними сенсорами. На рис. 2.9 зображено етапи, через які проходить процес контролю доступу.

Спочатку відбувається захоплення даних через біометричний сенсор (наприклад, сканер відбитків пальців або камера). Ці дані передаються до процесора обробки, де вони обробляються за допомогою алгоритмів штучного

інтелекту та порівнюються зі зразками, що зберігаються в базі даних. Далі приймається рішення про ідентифікацію.

На третьому етапі відбувається активація доступу - якщо ідентифікація успішна, процесор надсилає сигнал до контролера доступу. Контролер активує механізми відкриття дверей або інші засоби контролю доступу.

На етапі передачі даних, комунікаційний модуль передає результати ідентифікації до зовнішнього сервера, що зберігає дані для подальшого аналізу. Під час усього процесу відбувається енергозабезпечення через блок живлення.

Рис. 2.9 Схема взаємодії компонентів інтеграції біометричних сенсорів у систему контролю доступу

На рис. 2.10 представлено схему підключення компонентів біометричної системи контролю доступу, розроблену за допомогою Fritzing Software. Основні компоненти системи включають сканер відбитків пальців, підключений до Arduino через TX, RX, VCC та GND; LCD-дисплей, підключений через I2C (SDA, SCL); кнопки управління, підключені до цифрових пінів Arduino; релейний модуль: керує соленоїдним замком, підключеним до 12V.

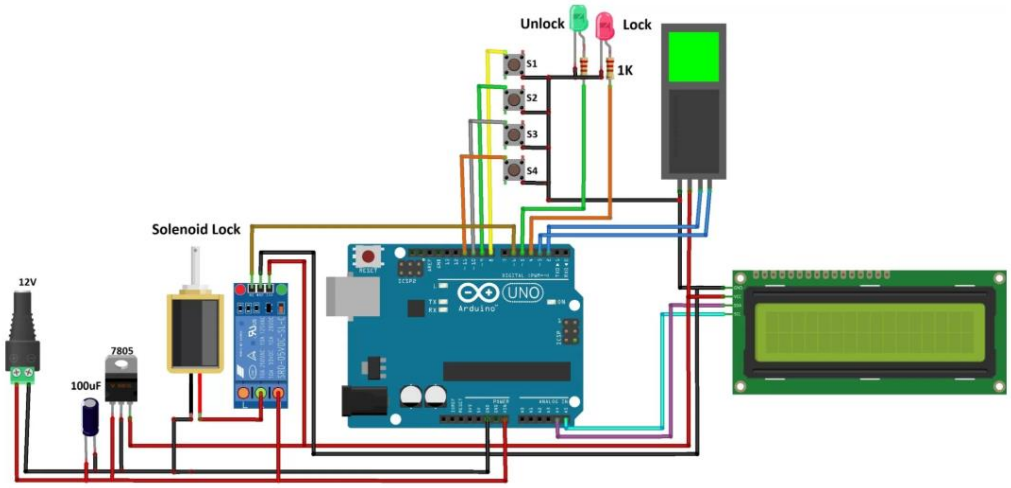


Рис. 2.10 Схема підключення компонентів біометричної системи

Підключення сканера відбитків пальців: TX - Arduino D2, RX - Arduino D3, VCC - Arduino 5V, GND - Arduino GND. Підключення LCD-дисплея через I2C: SDA - Arduino A4, SCL - Arduino A5, VCC - Arduino 5V, GND - Arduino GND. Підключення кнопок управління: Кнопки (enroll, delete, up, down) підключені до цифрових пінів 8, 9, 10, 11 та GND. Підключення релейного модуля: IN - Arduino D6, VCC - Arduino 5V, GND - Arduino GND, COM - Соленоїдний замок, NC -12V.

Принцип роботи: Користувач сканує відбиток пальця за допомогою сканера. Дані передаються до Arduino, де відбувається їх обробка та порівняння з шаблонами в базі даних. Якщо ідентифікація успішна, Arduino активує релейний модуль, який відкриває соленоїдний замок. Стан дверей (відкрито або закрито) відображається на LCD-дисплеї та через LED-індикатори.

2.4. Принципи роботи системи контролю доступу на основі біометрії

Біометричні системи контролю доступу зазвичай включають кілька основних компонентів: сенсори для зчитування біометричних характеристик, мікроконтролери або процесори для обробки отриманих даних, модулі зв’язку для передачі інформації, засоби зберігання шаблонів та виконавчі механізми (наприклад, реле або соленоїдні замки). Одним із критично важливих аспектів є

шифрування переданих даних на всіх етапах, що забезпечує захист біометричних зображень або відбитків пальців від несанкціонованого доступу. Використання сучасних криптографічних алгоритмів, таких як AES (Advanced Encryption Standard), є стандартним підходом для забезпечення безпеки під час передачі даних через комунікаційні канали (наприклад, Wi-Fi або UART). Схему принципу роботи біометричної системи доступу наведено на рис. 2.11.

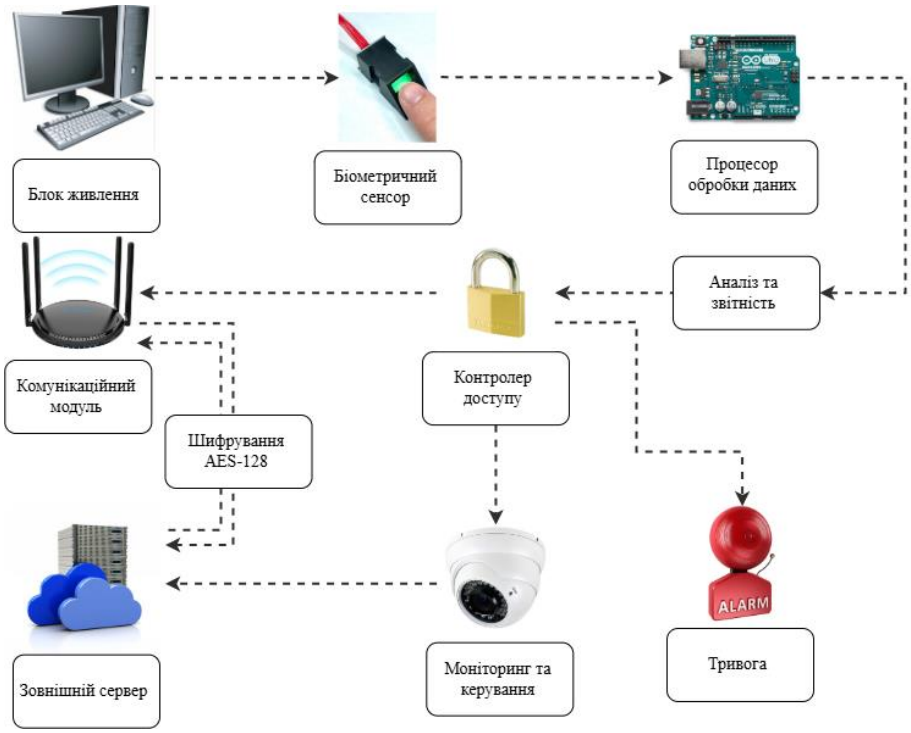


Рис. 2.11 Принцип роботи біометричної системи доступу

Для прикладу роботи системи контролю доступу на основі біометрії, покращено реалізацію системи біометричного доступу з рис. 2.10, імплементуючи Arduino Mini як базу, рис. 2.12. Принципова схема включає модуль відбитків пальців - пристрій для захоплення біометричних даних та їх попередньої обробки; Arduino Mini - центральний мікроконтролер, що отримує та аналізує дані, а також приймає рішення про надання або відмову у доступі; РК-дисплей 16*2 - компонент для виведення повідомлень користувачеві (наприклад, "Доступ дозволено" або "Прикладіть палець"); реле - електронний перемикач, який активується у разі позитивної ідентифікації; соленоїдний замок - механізм блокування дверей, що

відкривається за допомогою електричного сигналу; кнопки керування - для реєстрації нових користувачів, видалення даних або зміни налаштувань системи.

У колірній схемі проводів червоний відповідає за живлення (VCC, 5V, 12V), чорний - за заземлення (GND), синій та жовтий - за дані (SDA, SCL, TX, RX) і зелений, фіолетовий, рожевий - за керуючі сигнали (реле, кнопки).

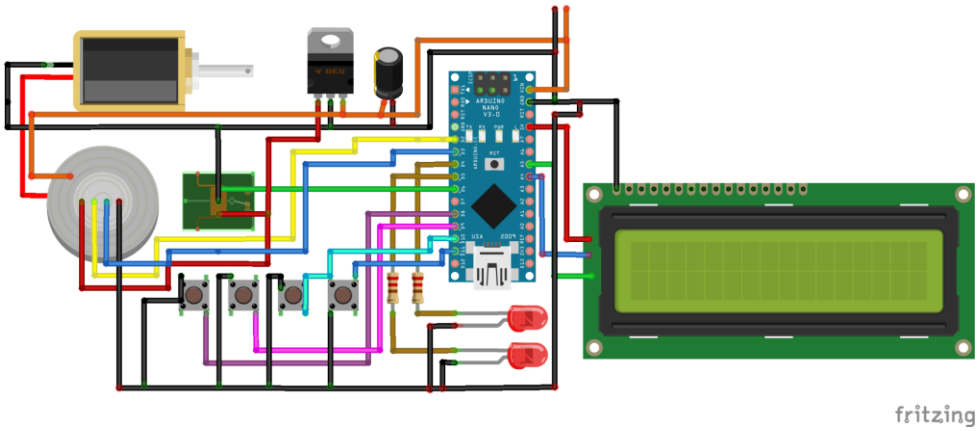


Рис. 2.12 Принципова схема біометричної системи безпеки з використанням Arduino Mini

Як згадувалося в пункті 2.3, алгоритм роботи системи складається з чотирьох наступних етапів, рис. 2.13:

1. Реєстрація користувача. Відбитки пальців зчитуються, аналізуються та зберігаються у внутрішній базі даних контролера у форматі ISO/IEC 19794-2

2. Ідентифікація. Прикладений до сенсора палець сканується, отримані дані порівнюються з шаблонами у базі.

3. Прийняття рішення. Якщо збіг виявлено, мікроконтролер активує реле, що замикає або розмикає соленоїдний замок.

4. Верифікація та журналювання. Дані про кожен запит зберігаються у пам’яті пристрою або передаються на сервер для подальшого аналізу

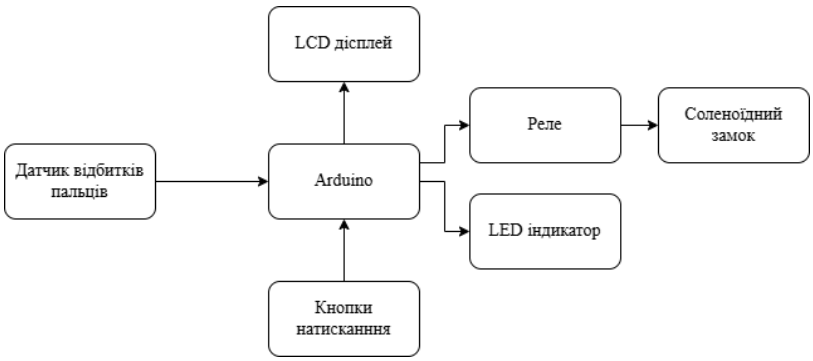


Рис. 2.13 Схема біометричної системи безпеки з використанням Arduino та датчика відбитків пальців

Існує багато реалізацій таких систем, які відрізняються за методами обробки та збереження даних. Одним із сучасних прикладів є платформа TruFace Manager та термінал TruFace Terminal, що застосовують для ідентифікації обличчя, як показано на рис. 2.14.

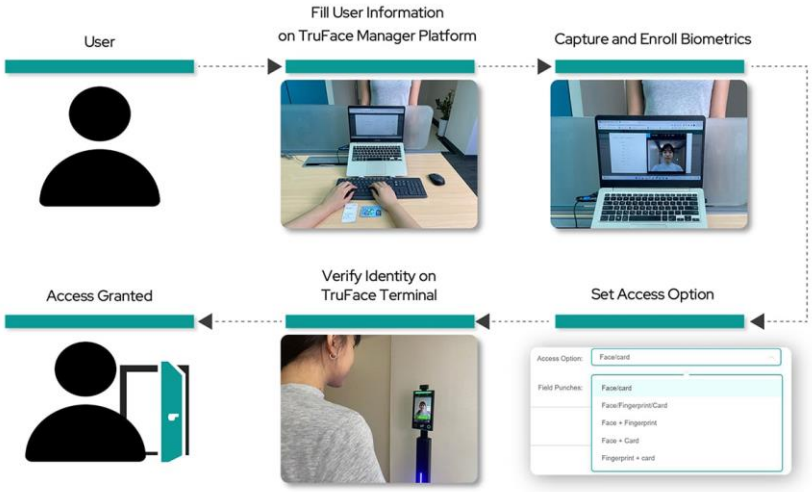


Рис. 2.14 Простий біометричний контроль доступу [24]

На першому етапі користувач проходить процес заповнення інформації на платформі TruFace Manager, де вводить свої персональні дані. Після цього система захоплює та реєструє біометричні дані (наприклад, зображення обличчя) за допомогою біометричного сенсора. Ці дані передаються до процесора обробки даних, де вони обробляються та зберігаються як еталонний зразок у базі даних. На етапі верифікації особи користувач підходить до TruFace Terminal, де

біометричний сенсор знову захоплює зображення обличчя. Процесор порівнює отримані дані із зразком у базі даних. Якщо ідентифікація успішна, контролер доступу активує механізм відкриття дверей або інші засоби контролю доступу, що призводить до надання доступу. Паралельно комунікаційний модуль передає дані про ідентифікацію до зовнішнього сервера для зберігання та подальшого аналізу.

2.5. Використання технологій Інтернету речей (IoT) для підвищення ефективності систем контролю доступу

Інтернет речей (IoT) має значний вплив на розвиток сучасних технологій безпеки і популярність IoT зростає досить швидко, рис. 2.15, зокрема в системах контролю доступу. Завдяки реалізації підключення великої кількості різноманітних пристроїв до Інтернету, IoT забезпечує нові можливості для моніторингу та управління доступом в реальному часі. Від простих систем контролю доступу, що обмежуються фізичними ключами або картками, до більш складних і адаптивних рішень на основі біометрії, IoT дозволяє значно підвищити рівень безпеки та ефективності.

Інтеграція технологій IoT у системи контролю доступу дозволяє здійснювати віддалене управління, автоматизацію процесів, а також покращує аналіз даних для більш ефективного управління ресурсами та прийняття рішень. Використання таких технологій, як хмарні платформи для моніторингу, інтеграція з системами "розумного будинку", а також аналіз великих даних для виявлення аномалій та прогнозування можливих проблем, дозволяє значно підвищити ефективність та безпеку таких систем.

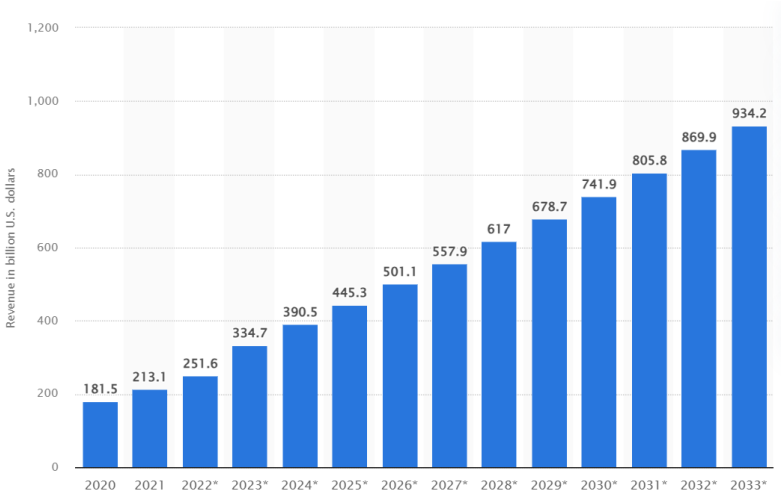


Рис. 2.15 Загальний річний дохід Інтернету речей (IoT) у всьому світі з 2020 по 2033 рік [14]

Одним з ефективних способів здійснення віддаленого моніторингу стану апаратних компонентів є використання протоколу MQTT для передачі даних про стан різних компонентів системи, таких як температура процесора або стан інших критичних елементів. MQTT - протокол на основі TCP, що базується на моделі публікації-підписки. Цей протокол зв'язку підходить для передачі даних між пристроями з обмеженими ресурсами, які мають низьку пропускну здатність і низькі вимоги до потужності. Принцип роботи MQTT наведено на рис. 2.16.

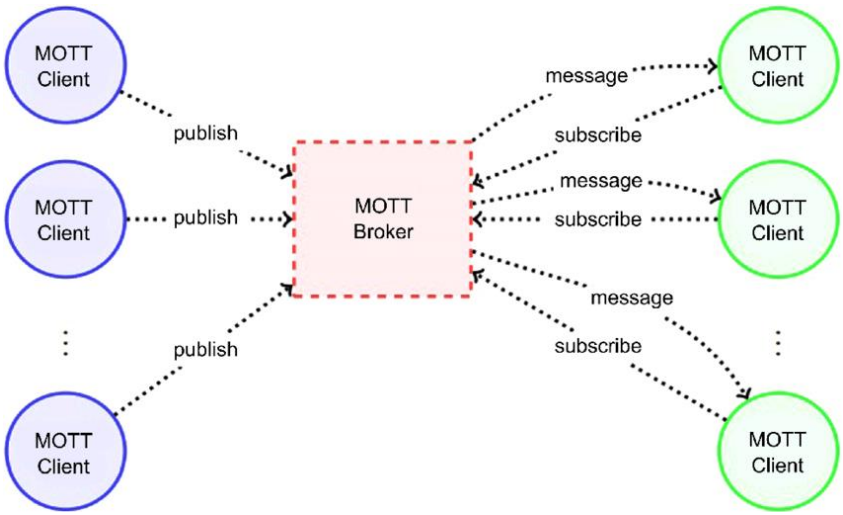


Рис. 2.16 Модель протоколу MQTT [36]

Інтеграція технологій IoT у системи контролю доступу спрямована на підвищення їхньої ефективності та автоматизації, але більшість цих систем зберігають дані на локальних носіях, таких як microSD-карти, що вимагає фізичного доступу до пристрою для їх зчитування і не є надійним від несанкціонованого доступу. Тому вирішено вдосконалити розроблену в минулому розділі систему з біометричним сканером відбитків пальців шляхом інтеграції з платформою ThingsBoard. Це дозволить зберігати та візуалізувати дані у хмарному середовищі, забезпечуючи зручний доступ та управління інформацією.

Система складається з Arduino UNO як основного контролера; LCD-дисплея 16*2 для відображення інформації; Wi-Fi модуля ESP8266-01 для бездротової передачі даних; сканера відбитків пальців GT511C3 (FPS) для біометричної ідентифікації; адаптера 12V для живлення пристроїв.

Принцип роботи складає наступні етапи: Спочатку користувач проходить ідентифікацію за відбитком пальця.Arduino UNO передає зчитані дані через ESP8266 до платформи ThingsBoard. На інформаційній панелі ThingsBoard дані обробляються та візуалізуються. Тим часом, адміністратор може віддалено переглядати історію відвідуваності.

Для реалізації проекту використано два окремі скетчі для програмування: Arduino UNO, що контролює роботу сканера відбитків пальців та передає дані до ESP8266 та сам ESP8266, що встановлює з’єднання з сервером ThingsBoard та передає отримані дані у форматі JSON.

Щоб підключити ESP8266 до Wi-Fi маршрутизатора та синхронізувати з сервером ThingsBoard, необхідно налаштувати серійну комунікацію та ініціалізувати підключення до мережі. У функції setup(), рис. 2.17, відкривається серійна комунікація на швидкості 9600 бодів (baud), ініціалізується Wi-Fi модуль для підключення до маршрутизатора та підключається клієнт до серверу ThingsBoard, задаючи відповідний порт. Окрім цього, ініціалізується змінна lastSend, щоб відстежувати час останнього відправлення даних.

```
void setup()
{
  Serial.begin(9600);
  delay(10);
  InitWiFi();
  client.setServer( thingsboardServer, 1883 );
  lastSend = 0;
}
```

Рис. 2.17 Функція setup()

У функції loop() перевіряється наявність активного з'єднання з сервером, рис. 2.18. Якщо з'єднання не встановлено, спрацьовує функція повторного підключення reconnect(). Потім програма перевіряє наявність вхідних даних з серійного порту. Якщо дані доступні, вони зчитуються по одному символу, конкатенуються в рядок Name. Якщо символом є новий рядок, то рядок обрізається від зайвих символів і відправляється на сервер ThingsBoard у форматі JSON за допомогою функції Send_to_Thingsboard(). Після цього змінна Name очищується для отримання нових даних. Відсутність нових даних не призводить до зупинки програми - продовжується підтримка підключення за допомогою виклику client.loop().

```
void loop() {
  // Перевіряємо, чи підключений клієнт. Якщо ні, виконуємо перепідключення.
  if (!client.connected()) {
    reconnect();
  }

  // Перевіряємо, чи є доступні дані в серійному порту.
  if (Serial.available()) {
    char a = Serial.read(); // Зчитуємо один символ із серійного порту.
    Name = Name + String(a); // Додаємо зчитаний символ до змінної Name.

    // Перевіряємо, чи символ є "Carriage Return" (код 13 - новий рядок).
    if (a == 13) {
      Name.trim(); // Видаляємо зайві символи нового рядка (/n або /r).
      Serial.println(Name); // Виводимо отриманий рядок у серійний порт.
      Send_to_Thingsboard(); // Відправляємо отримані дані на платформу Thingsboard.
      Name = ""; // Очищаємо змінну Name для прийому нового рядка.
    }
  }

  // Викликаємо метод обробки клієнта, щоб підтримувати з'єднання та обробляти повідомлення.
  client.loop();
}
```

Рис. 2.18 Функція loop()

Сервер ThingsBoard приймає інформацію у форматі JSON, тому дані мають бути сформовані у форматі JSON з ESP8266, що можна зробити за допомогою простого функціоналу конкатенації рядків в Arduino. Для фінальної схеми модуль FTDI замінено на Arduino UNO, до якого підключені датчик GT511C3 FPS і дисплей LCD, рис. 2.19.

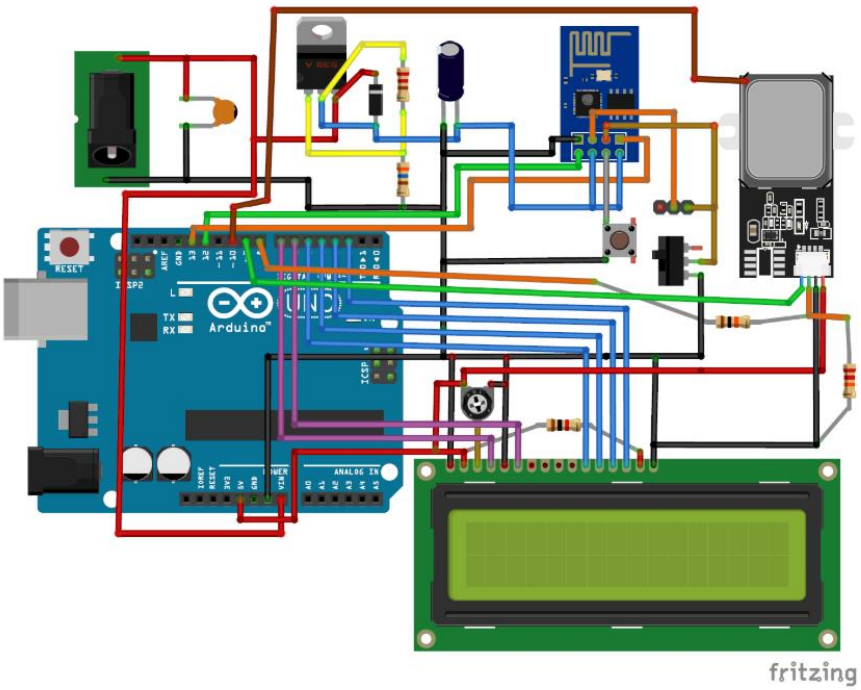


Рис. 2.19 Схема для системи біометричного обліку присутності на основі Інтернету речей, залучаючи Arduino та Thingsboard [37]

Живлення всієї системи може здійснюватися через адаптер напругою 12 В, який підключається безпосередньо до виводу Vin на платі Arduino UNO. Дисплей 16*2 LCD відповідає за відображення імені ідентифікованої особи.

Програмне забезпечення для Arduino реалізує функцію реєстрації та розпізнавання відбитків пальців. У процесі реєстрації створюється унікальний шаблон відбитка, після чого користувачеві надається унікальний ідентифікатор (ID). Під час аутентифікації система шукає відповідний ID, зв’язує його з іменем та передає ці дані через серійну комунікацію на модуль ESP8266. Надалі отримана інформація надсилається на платформу ThingsBoard для подальшої обробки та зберігання.

Першим етапом програмування є створення відповідності між ідентифікаційним номером та іменем користувача. Далі треба підключити та ініціалізувати кілька бібліотек в Arduino IDE: GT511C3 FPS - бібліотека для роботи з біометричним сканером відбитків пальців, що забезпечує реєстрацію та ідентифікацію користувачів; бібліотека для ємнісного сенсора дотику - для перевірки дотику до металевого корпусу сканера.

Після встановлення необхідних бібліотек здійснюється підключення модулів до мікроконтролера. Передача даних між ESP8266 та Arduino UNO відбувається через піні Rx та Tx, підключені до пінів 12 та 13 відповідно. Біометричний сканер GT511C3 підключено до пінів 9 і 8, а сенсор дотику - до піна 10. Дисплей LCD під’єднано до пінів D2-D7, як зображено на рис. 2.20.

```
SoftwareSerial ESP(12, 13); // Налаштування програмного серійного з'єднання з ESP8266 (RX - 12, TX - 13)
FPS_GT511C3 fps(9, 8); // Підключення сканера відбитків пальців FPS до пінів D9 (TX) і D8 (RX)

const int rs = 7, en = 6, d4 = 5, d5 = 4, d6 = 3, d7 = 2; // Визначення пінів для підключення LCD-дисплея
LiquidCrystal lcd(rs, en, d4, d5, d6, d7); // Ініціалізація LCD-дисплея з вказаними пінами

int capSensePin10  = 10; // Пін, до якого підключено металевий корпус сенсора для ємнісного визначення дотику
```

Рис. 2.20 Конфігурація апаратних з'єднань

Оновлено функції setup() та loop(). У функції setup() ініціалізується серіальна комунікація для Arduino та ESP8266 на швидкості 9600 бод, виводиться вітальне повідомлення на LCD-дисплеї, встановлюється зв’язок зі сканером GT511C3 FPS, а також вимикається його світлодіод. Додається підключення до Wi-Fi через InitWiFi(), налаштовується сервер MQTT для передачі даних на ThingsBoard і ініціалізується змінна для відстеження часу відправки даних, рис. 2.21.

```
void setup() {
  Serial.begin(9600); // Ініціалізація серійного зв’язку
  ESP.begin(9600); // Ініціалізація ESP8266 з baud rate 9600

  // Ініціалізація LCD-дисплея 16x2
  lcd.begin(16, 2);
  lcd.print("GT511C3 FPS"); // Відображення вступного повідомлення (1 рядок)
  lcd.setCursor(0, 1);
  lcd.print("with Arduino"); // Відображення вступного повідомлення (2 рядок)
  delay(2000);
  lcd.clear(); // Очистка екрану

  fps.Open(); // Ініціалізація сканера відбитків пальців
  fps.SetLED(false); // Вимкнення світлодіода FPS при запуску

  delay(10);
  InitWiFi(); // Підключення до WiFi
  client.setServer(thingsboardServer, 1883); // Налаштування сервера MQTT
  lastSend = 0; // Обнулення таймера відправлення даних
}
```

Рис. 2.21 Оновлена функція setup()

У функції loop() перевіряється стан ємнісного сенсора дотику. Якщо значення менше 50, вмикається світлодіод сканера. Обробляються дані, отримані через серіальний порт: після введення нового рядка дані передаються на сервер ThingsBoard. Також виконується підключення до MQTT-сервера для безперервної передачі даних, рис. 2.22.

```
void loop() {
  // Перевірка підключення клієнта, якщо відключено - спроба перепідключення
  if (!client.connected()) {
    reconnect();
  }
  // Перевірка дотику до сенсора
  int capSense10 = opcs.readCapacitivePin(capSensePin10);
  if (capSense10 < 50) { // Якщо є дотик
    fps.SetLED(true); // Увімкнути світлодіод FPS
    delay(500);
  }
  // Обробка вхідних даних із серійного порту
  if (Serial.available()) {
    char a = Serial.read(); // Зчитування символу
    Name = Name + String(a); // Додавання символу до рядка
    if (a == 13) { // Перевірка на новий рядок (код 13 - Enter)
      Name.trim(); // Видалення пробілів, /n або /r з отриманих даних
      Serial.println(Name); // Виведення імені у серійний монітор
      Send_to_Thingsboard(); // Відправлення даних на сервер
      Name = ""; // Очищення змінної Name після надсилання
    }
  }
  client.loop(); // Підтримка зв'язку з сервером MQTT
}
```

Рис. 2.22 Оновлена функція loop()

Перевірка відбитка пальця включає ідентифікацію відбитка за допомогою fps.Identify1_N(). Якщо ID дорівнює 200, відбиток не розпізнано. Якщо ID дорівнює 0, це адміністратор і запускається функція реєстрації нового відбитка пальця. Якщо

ID відмінне від 0 і 200, виводиться ім'я користувача і воно відправляється на ESP, рис. 2.23.

```
63  // Ідентифікація відбитка пальця
64  int id = fps.Identify1_N(); // Отримання ID відбитка пальця
65  lcd.clear(); // Очистити LCD екран
66  if (id == 200) { // Якщо відбиток не розпізнано
67    lcd.print("Unkown");
68    lcd.setCursor(0, 1);
69    lcd.print("Try Again!!"); // Повідомлення про невідомого користувача
70  }
71  else if (id == 0) { // Якщо це адміністратор
72    lcd.print("Welcome");
73    lcd.setCursor(0, 1);
74    lcd.print("***ADMIN***"); // Привітання для адміністратора
75    delay(2000); // Затримка 2 секунди
76    Enroll(); // Виклик функції для реєстрації нового відбитка
77  }
78  else { // Якщо користувач розпізнаний
79    lcd.print("Thank You");
80    lcd.setCursor(0, 1);
81    lcd.print(Name_List[id]); // Виведення імені користувача
82    ESP.println(Name_List[id]); // Відправка імені на ESP
83    Serial.println("Sent Value to ESP"); // Виведення повідомлення в серійний монітор
84  }
85  delay(1000); // Затримка 1 секунда
```

Рис. 2.23 Оновлена функція loop() - Ідентифікація відбитку пальця

Для тестування системи необхідно завантажити код на плату Arduino UNO та підключити її до модуля ESP. Після подачі живлення на екран LCD має вивести повідомлення “Press Finger”. Після виявлення зареєстрованого відбитка пальця LCD відобразиться повідомлення “Thank you” разом з ім’ям ідентифікованої особи. Це ім’я буде передане до модуля ESP, який у свою чергу відправить дані на платформу ThingsBoard.

Після того, як LCD відобразить ім’я, це свідчитиме про успішну передачу даних на платформу ThingsBoard. Для перевірки необхідно увійти у вкладку “Device” на ThingsBoard, вибрати пристрій та натиснути “Latest Telemetry”. Останній запис має показати ім’я ідентифікованої особи. Якщо дані не відображаються, варто перевірити підключення модуля ESP та переконатися, що він отримує та передає дані.

Отже, представлено розширену схему на рис. 2.24, що інтегрує IoT для зручного зберігання та візуалізації даних, а також для забезпечення безпеки на більш високому рівні.

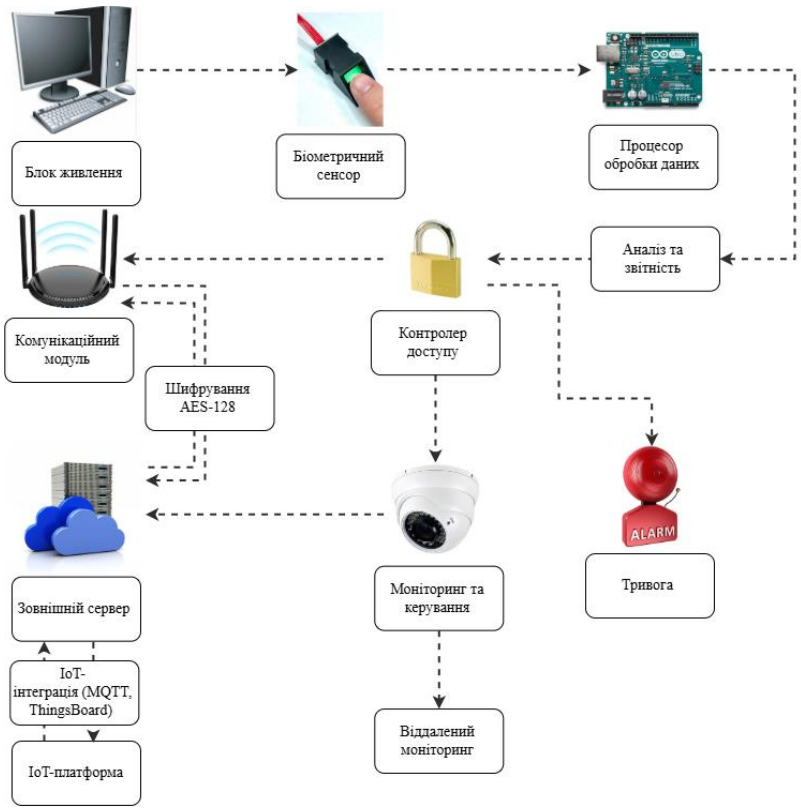


Рис. 2.24 Схема роботи біометричної системи доступу, з додаванням IoT

Подальші етапи розробки зосереджуються на програмній частині системи контролю доступу, де важливими аспектами будуть архітектура програмного забезпечення, розробка алгоритмів для обробки біометричних даних, використання штучного інтелекту для вдосконалення процесів перевірки особи, а також створення системи управління доступом через веб-інтерфейс.

РОЗДІЛ 3 ПРОГРАМНА ЧАСТИНА СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1. Архітектура програмного забезпечення системи

Програмне забезпечення розробленої системи контролю доступу ґрунтується на клієнт-серверній архітектурі, де основну обчислювальну логіку виконує сервер, а біометричні дані надходять із периферійного пристрою - контролера ESP32 з підключеним сенсором відбитків пальців (у перспективі - камерою для розпізнавання обличчя).

Програмна архітектура включає кілька функціональних модулів, що можна побачити на рис. 3.1, що починаються зі збору біометричних даних - відбитку пальця (в подальших розділах також з можливістю сканування обличчя) за допомогою ESP32. Після сканування, дані передаються на сервер по бездротовому з’єднанню (Wi-Fi). Для обміну між контролером і сервером задіяно протокол MQTT поверх Wi-Fi. ESP32 надсилає запит на сервер зі зчитаними біометричними даними для подальшої обробки. Наступним модулем є серверна частина (Python), що приймає вхідні запити від ESP32, обробляє біометричні дані, проводить їх верифікацію шляхом порівняння з базою шаблонів користувачів. У разі успішної ідентифікації надсилається відповідь про дозвіл або заборону доступу. Для зберігання шаблонів відбитків пальців або облич (у майбутній версії), а також ведення логування входів та відмов існує база даних користувачів SQLite. Останнім модулем є керування доступом, що отримує результат перевірки особи та активує або блокує електронний замок.

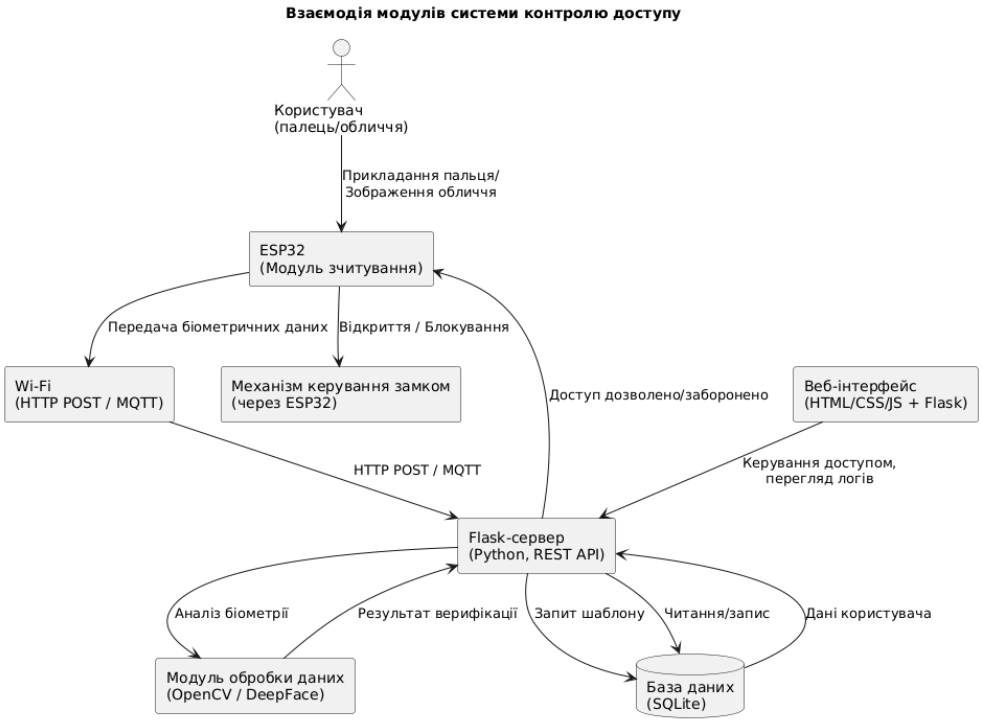


Рис. 3.1 Архітектура програмного забезпечення системи

3.2 Розробка алгоритмів для обробки біометричних даних

Як уже згадувалося в розділі 2.2, процес обробки біометричних даних з відбитку пальця складається з попередньої обробки (підпроцеси можна побачити на рис. 2.2), виділення ознак, створення шаблону, порівняння з базою даних та оптимізацією. Зокрема, передбачається, що зображення відбитка пальця було отримане за допомогою сенсора Suprema BioMini Plus 2.

Перший етап є невід’ємним і включає в себе нормалізацію яскравості, фільтрацію шуму та бінаризацію, схему було наведено раніше на рис. 2.2. Код з даним алгоритмом було реалізовано в Google Colab і можна побачити на рис. 3.2.

```
[13] from google.colab import files
     from google.colab.patches import cv2_imshow
     from urllib.request import urlretrieve
     import hashlib
     import time

     # Завантаження тестового зображення
     uploaded = files.upload()
     filename = next(iter(uploaded))

     # OpenCV
     image = cv2.imread(filename)

     # Попередня обробка зображення
     def preprocess_fingerprint(image):
         gray = cv2.cvtColor(image, cv2.COLOR_BGR2GRAY)
         equalized = cv2.equalizeHist(gray)
         filtered = cv2.medianBlur(equalized, 5)
         _, binary = cv2.threshold(filtered, 0, 255, cv2.THRESH_BINARY + cv2.THRESH_OTSU)
         return binary

     binary_image = preprocess_fingerprint(image)
     cv2_imshow(binary_image)
```

Рис. 3.2 Попередня обробка відбитка пальця

Було проведено експеримент на зображенні з інтернету, рис. 3.3 ліворуч. Результатом, на рис. 3.3 праворуч, є бінаризоване зображення відбитка пальця з підвищеною якістю для подальшої обробки.

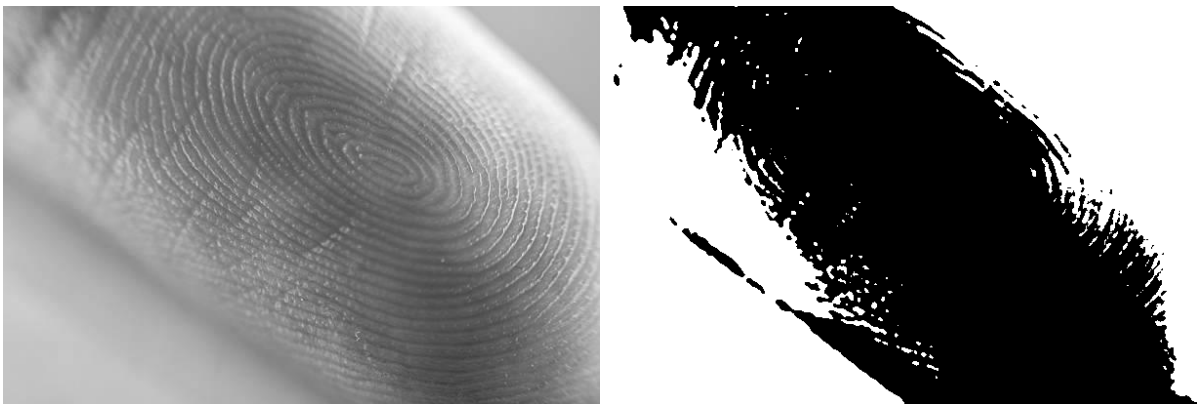


Рис. 3.3 Оригінал та результат обробки

Для етапу виділення ознак було використано алгоритм SIFT (Scale-Invariant Feature Transform) , що знаходить ключові точки на відбитку, рис. 3.4. Найбільш позитивна якість у SIFT - забезпечення інваріантність до масштабування, поворотів і освітлення. Метод виявляє локальні особливості (keypoints), які відповідають унікальним характеристикам відбитка. У результаті отримано кількість знайдених точок та їх розташування, рис. 3.5.

```python
# Виділення ознак (SIFT)
def extract_features(image):
    sift = cv2.SIFT_create()
    keypoints, descriptors = sift.detectAndCompute(image, None)

    # Візуалізація ключових точок
    img_with_keypoints = cv2.drawKeypoints(image, keypoints, None, flags=cv2.DRAW_MATCHES_FLAGS_DRAW_RICH_KEYPOINTS)

    return descriptors, img_with_keypoints

# Використовуємо binary_image з попередньої комірки
descriptors, img_with_keypoints = extract_features(binary_image)

cv2_imshow(img_with_keypoints)
print(f"Знайдено ключових точок: {len(descriptors)}")
```

Рис. 3.4

Застосування алгоритму SIFT для знаходження критичних точок

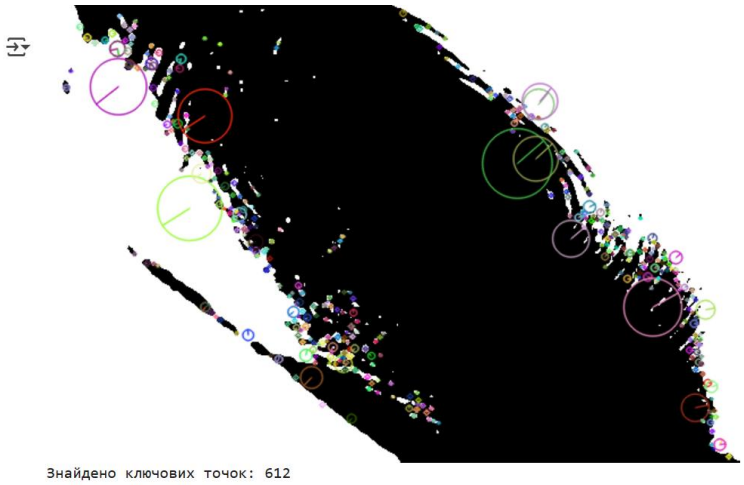


Рис. 3.5 Результат виділення ознак на відбитку пальця

На етапі створення шаблону, рис. 3.6, виділені дескриптори бінаризуються. Масив бітів ущільнюється в байти за допомогою np.packbits. Результат хешується з використанням криптографічного алгоритму SHA-256, що гарантує унікальність шаблону.

```
[16] # Створення шаблону (хешування)
     def create_template(descriptors):
         # Перевірка: чи дескриптори не порожні
         if descriptors is None or len(descriptors) == 0:
             print("Не вдалося створити шаблон: дескриптори відсутні.")
             return None

         # Конвертація дескрипторів у бінарний формат
         binary_descriptors = np.packbits(np.where(descriptors > 0, 1, 0))

         # Хешування за допомогою SHA-256
         template_hash = hashlib.sha256(binary_descriptors.tobytes()).hexdigest()

         return template_hash

     # Виклик функції для створення хешу
     template_hash = create_template(descriptors)

     # Виведення результату
     if template_hash:
         print(f"Шаблон успішно створено.\nХеш шаблону:\n{template_hash}")
     else:
         print("Шаблон не створено.")
```

Рис. 3.6 Процес створення шаблону (хешування дескрипторів)

Під час порівняння отриманого шаблону з наявними у базі даних використано імітацію реальної БД, рис. 3.7. Код обчислює відсоток збігів між символами нового та збережених хешів користувачів й обирає користувача із найбільшим збігом. В залежності від проценту результату, доступ або дозволяється, або відхиляється.

```
def compare_with_database(new_template, threshold=0.9):
    # Імітаційна база даних (реальні хеші замінені прикладами)
    database = {
        "user1": "a1b2c3d4e5f6g7h8i9j0a1b2c3d4e5f6g7h8i9j0a1b2c3d4e5f6g7h8",
        "user2": "1234567890abcdef1234567890abcdef1234567890abcdef12345678"
    }

    best_match = None
    best_score = 0

    for user_id, db_template in database.items():
        # Порівняння хешів за схожістю символів
        score = sum(a == b for a, b in zip(new_template, db_template)) / len(new_template)

        if score > best_score:
            best_score = score
            best_match = user_id

    return best_match, best_score

# Виклик функції
best_match, match_score = compare_with_database(template_hash)
```

Рис. 3.7 Порівняння отриманого шаблону з наявними у базі даних

В кінці реалізовано візуалізацію результатів, де можна побачити оригінальне зображення, бінаризовану версію, візуалізацію ключових точок, текстові результати порівняння, графік дескрипторів та хеш шаблону, рис. 3.8.

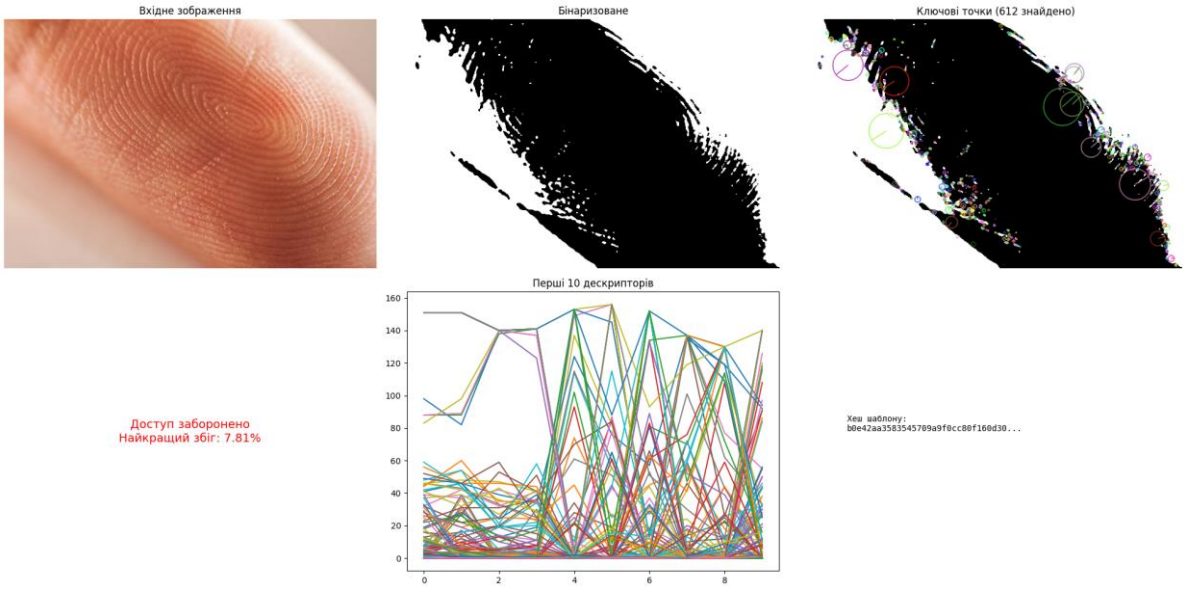


Рис. 3.8 Виведені для порівняння результати біометричної ідентифікації за відбитком пальця

3.3. Використання штучного інтелекту для покращення процесів перевірки особи та контролю доступу

Методи обробки зображень в системах біометричної ідентифікації, наприклад, SIFT, поступово доповнюються або замінюються моделями глибокого навчання. Це дозволяє підвищити точність розпізнавання та зменшити кількість помилкових спрацьовувань. Окрім цього, моделі глибокого навчання допомагають завадити спуфінгу, що є однією з центрових проблем біометрії. Прикладом такої моделі є згорткові нейронні мережі CNN, що попередньо навчаються на певному датасеті. Однією з архітектур CNN є ResNet (Residual Network). ResNet розроблена для вирішення проблеми затухання градієнтів та деградації якості моделі при збільшенні її глибини, вона дозволяє будувати надзвичайно глибокі моделі, які стабільно тренуються. Отже, для покращення точності коду, сконструйованого в розділі 3.2, додано імплементацію ResNet, рис. 3.9.

```python
# Створення моделі ResNet
def create_fingerprint_model(input_shape=(224, 224, 3)):
    base_model = ResNet50(weights='imagenet', include_top=False, input_shape=input_shape)
    x = base_model.output
    x = GlobalAveragePooling2D()(x)
    model = Model(inputs=base_model.input, outputs=x)
    for layer in base_model.layers:
        layer.trainable = False
    return model

model = create_fingerprint_model()
```

Рис. 3.9 Код для моделі ResNet

Після проходження зображення через ResNet, отримується вектор ознак, що представляє унікальні характеристики відбитка. Потім порівнюються два такі вектори за допомогою косинусної подібності. Для демонстрації порівняння було додано опцію імпортування другого фото, трошки зміненого за розміром та орієнтацією, рис. 3.10.

Рис. 3.10 Оригінальне зображення (ліворуч) та видозмінене зображення (праворуч)

У результаті отримано коефіцієнт схожості 89,23%, як можна побачити на рис. 3.11. Даний результат має такий великий коефіцієнт розрізності через обрізання деяких частинок відбитку на відредагованому зображенні.

```
# Порівняння ознак
def compare_features(f1, f2):
    similarity = np.dot(f1, f2) / (np.linalg.norm(f1) * np.linalg.norm(f2))
    return similarity

similarity_score = compare_features(features1, features2)

# 📢 Результат
print(f"\n Коефіцієнт схожості: {similarity_score:.2%}")
if similarity_score >= 0.9:
    print(" Відбитки схожі (ймовірно однакові відбитки)")
else:
    print(" Відбитки різні")
```

```
Коефіцієнт схожості: 89.23%
Відбитки різні
```

Рис. 3.11 Результат застосування ResNet на двох майже ідентичних зображеннях

Порівнюючи два алгоритми “з” та “без” технології ResNet отримано результат на рис. 3.12. Можна побачити, що SIFT показує збіг схожих відбитків, у той час як у ResNet збігу не знайдено.

```
# Класичний метод
_, sift_result = compare_sift(des1, des2)

# ResNet
_, resnet_result = compare_resnet(image1, image2)

# Порівняння
print("SIFT збіг:", "Збіг знайдено" if sift_result else "Збіг не знайдено")
print("ResNet збіг:", "Збіг знайдено" if resnet_result else "Збіг не знайдено")
```

```
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 227ms/step
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 213ms/step
SIFT збіг: Збіг знайдено
ResNet збіг: Збіг не знайдено
```

Рис. 3.12 Результат порівняння алгоритму “з” та “без” технології ResNet

Розроблений модуль ШІ може бути реалізований у вигляді окремого серверу, що працює паралельно з існуючими модулями Python-сервера, інтерфейс якого розроблено в наступному розділі, та взаємодіє з ними через API. Для цього можна користуватися фреймворками TensorFlow або PyTorch.

3.4. Система управління доступом через веб-інтерфейс

Для ефективного керування системи контролю доступу було розроблено макет веб-інтерфейсу в Figma, що забезпечує зручну взаємодію адміністратора з програмним забезпеченням. Інтерфейс дозволяє контролювати поточний стан

пристрою, переглядати й редагувати зареєстрованих користувачів та додавати нових, а також показувати історію спроб доступів з інформацією особи.

Інтерфейс містить п’ять головних сторінок, що починаються з логіну адміністратора, рис. 3.13 ліворуч. Адміністратор може також вийти з облікового запису. У налаштуваннях, рис. 3.14 праворуч, можна керувати базовими опціями: переглянути підлаштовані пристрої, нотифікації, мова, тощо.

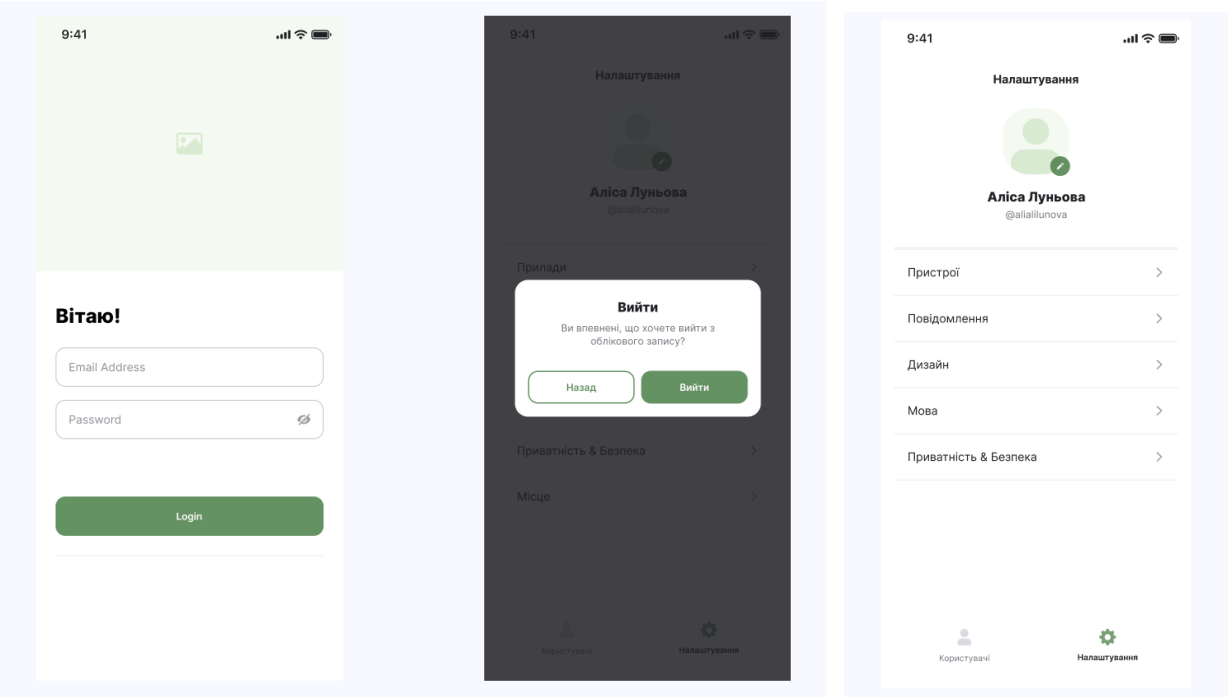


Рис. 3.13 Інтерфейс входу та виходу з системи; сторінка налаштувань

Головна сторінка, рис. 3.14 ліворуч, відображає назву системи, статус підключення пристрою (ESP32), а також інформацію про спроби доступу за поточну добу: ініціали та ID особи. Сторінка “Користувачі” на рис. 3.14 посередині містить список з усіма зареєстрованими користувачами та їх персональною інформацією. Адміністратор може не тільки додавати нових користувачів, а й редагувати їх дані, або видаляти з системи за допомогою іконки з верхнього правого краю. Якщо в даних якогось з користувачів є помилка, або зауваження, можна побачити знак оклику (!) біля ID даного користувача.

Якщо адміністратор хоче додати нову особу, необхідно ввести її параметри, рис. 3.14 ліворуч. Наведено опцію або сканування відбитку пальця або

завантаження фото обличчя особи. Сканування відбитку пальця ініціює запит до Python-сервера, концепт якого описано в розділі 3.3. У свою чергу, сервер ініціює або запит до ESP32 для зчитування, або передає дані до підключеного модуля ШІ для обробки скану відбитку або зображення обличчя.

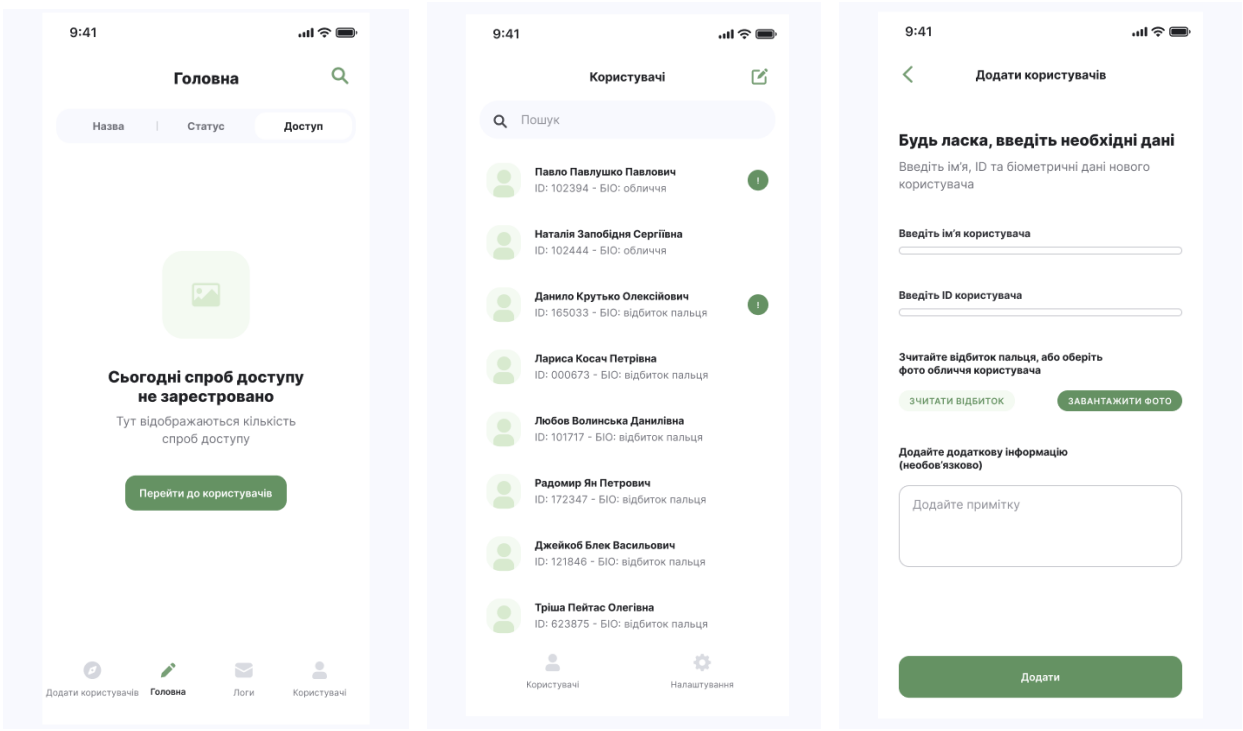


Рис. 3.14 Інтерфейс головної сторінки, сторінки з користувачами та додаванням користувачів

Побудований веб-інтерфейс є центральною частиною системи, що поєднує апаратні компоненти (ESP32, біометричні сенсори) з програмною логікою (сервер, база даних SQLite) і передбачає перспективу розширення технології або її змінення.

3.5. Безпека та захист даних у системі

Кожна сучасна система, особливо, система, що транслює персональні дані як біометрія, має бути міцно захищена за принципами конфіденційності, цілісності та доступності (CIA Triad).

Так, наприклад, розроблений інтерфейс в розділі 3.4 має вбудований механізм авторизації, який не передбачає реєстрацію нових акаунтів, рис. 3.15. Це обмежує доступ до системи виключно призначеним особам.

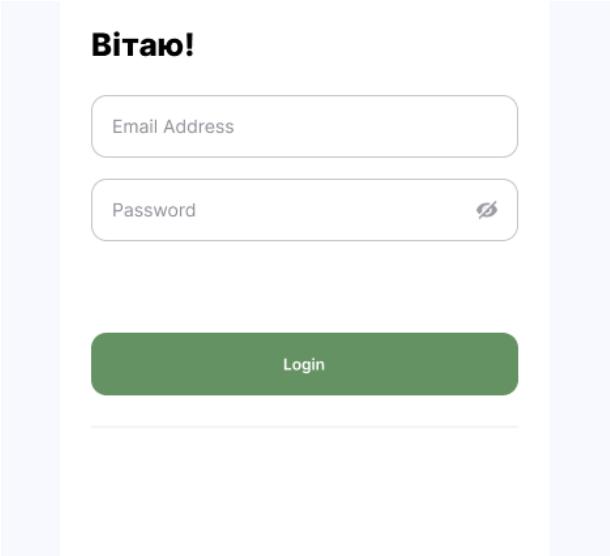


Рис. 3.15 Інтерфейс сторінки входу в системи без опції реєстрації

У розділі 3.2 було описано, що шаблони відбитків пальців хешуються за допомогою алгоритму SHA-256, що унеможливлює зворотнє отримання зображення. Важливо також коректно зберігати створені хеші у SQLite, рис. 3.15. Ця база даних користувачів фізично ізольована на сервері, а доступ до неї обмежено лише системним процесом Python-сервера.

```
print("Хеш шаблону:", template_hash)

# Підключення до локальної бази
conn = sqlite3.connect("biometric_system.db")
cursor = conn.cursor()

# Створення таблиці, якщо ще не існує
cursor.execute('''
    CREATE TABLE IF NOT EXISTS users (
        id INTEGER PRIMARY KEY AUTOINCREMENT,
        name TEXT NOT NULL,
        template_hash TEXT NOT NULL
    )
''')

# Додавання користувача з хешованим шаблоном
name = "Аліса Луньова"
cursor.execute('INSERT INTO users (name, template_hash) VALUES (?, ?)', (name, template_hash))

conn.commit()
conn.close()
```

Рис. 3.15 Збереження хешу у SQLite базу даних

Для перевірки механізму збереження біометричних даних проведено тестування, зображене на рис. 3.16. У ході експерименту симульовано біометричний шаблон у вигляді бітового масиву. Його було хешовано через алгоритм SHA-256, конкретні функції аналогічні до застосованих на рис. 3.6. Збережений хеш порівняно з новим зразком, за повного збігу хешів доступ дозволено.

```
# === 3. ПЕРЕВІРКА СПРОБИ ДОСТУПУ ===

# Симуляція нової спроби входу (використаємо той самий шаблон)
new_descriptors = descriptors.copy()  # або змінити для імітації помилкового входу
new_byte_data = np.packbits(new_descriptors)
new_hash = hashlib.sha256(new_byte_data).hexdigest()

# Перевірка в базі
cursor.execute('SELECT name FROM users WHERE template_hash = ?', (new_hash,))
result = cursor.fetchone()

if result:
    print(f"Доступ дозволено. Користувач знайдений: {result[0]}")
else:
    print("Доступ заборонено. Користувача не знайдено.")

conn.close()
```

```
Згенерований хеш шаблону: c1253429a85a31b2c6f88c68b6db3bf871373c9ab3b4fb4595ddbeb88ee4470d
Користувача збережено у базу.
Доступ дозволено. Користувач знайдений: Аліса Луньова
```

Рис. 3.16 Перевірка спроби доступу

Додатковими мірами безпеки для передачі даних між компонентами системи є інтегрування протоколу MQTT для комунікації між ESP32 та сервером, описаного в розділі 2.5 та додаткове шифрування біометричних даних за допомогою AES-128 перед передачею, описаного у розділі 2.1.

Особливу увагу приділено захисту персональних даних відповідно до вимог GDPR (розділ 1.4), тобто, мінімізація збережених даних - за допомогою лише хешів біометричних шаблонів та можливості повного видалення даних користувача за його запитом чи за запитом адміністратора.

ВИСНОВКИ

У результаті проведеного дослідження та розробки автоматизованої системи контролю доступу на основі біометричних даних і технологій штучного інтелекту можна зробити такі висновки:

Біометричні методи, зокрема розпізнавання обличчя, відбитків пальців, голосу, сітківки ока, тощо, є найбільш перспективними в аспекті зручності використання, швидкості обробки та унікальності ознак. Аналіз ринку продемонстрував динамічне зростання впровадження таких технологій у різних сферах - фінансовій, урядовій, освітній, медичній та інших. Найпоширенішими методами залишається сканування відбитка пальця та обличчя.

Апаратна частина системи, що базується на мікроконтролері (наприклад, ESP32), у поєднанні з біометричним сенсором, забезпечує доступність реалізації системи з застосуванням сучасних засобів Інтернету речей (IoT). Такий підхід дозволяє значно полегшити контроль системи і підвищити захист даних, що зберігаються або транслюються.

Програмне забезпечення, реалізоване з методами штучного інтелекту та бібліотек для комп’ютерного зору, зокрема Python-бібліотек, дозволяє обробляти та аналізувати біометричні дані в режимі реального часу. Застосування алгоритмів глибокого навчання помітно покращує точність ідентифікації і зменшує необхідність великого сховища для порівняння даних, наприклад, відбитків пальця, між собою.

Етичні та правові аспекти впровадження біометричних систем вимагають чіткого дотримання стандартів захисту персональних даних. У роботі було розглянуто основні положення GDPR, які мають бути враховані при застосуванні технологій, що працюють з біометрією.

Створена система є масштабованою та придатною для адаптації до різних сценаріїв використання - від локального контролю доступу до інтеграції в розумні будинки чи корпоративні мережі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Rachel German K. Suzanne Barber. Current Biometric Adoption and Trends. Current Biometric Adoption and Trends. URL: https://identity.utexas.edu/sites/default/files/2020-09/Current%20Biometric%20Adoption%20and%20Trends.pdf.

2. LLP A. A. Fingerprint Biometrics Market to Reach $74.1 Billion by 2032 at 7.8% CAGR: Allied Market Research. GlobeNewswire News Room. URL: https://www.globenewswire.com/news-release/2024/02/12/2827191/0/en/Fingerprint-Biometrics-Market-to-Reach-74-1-Billion-by-2032-at-7-8-CAGR-Allied-Market-Research.html.

3. Jaimit Patel Anubhav Ayush Kumar Singh Rachit Kumar Tiwari Abhi Singh and Bhupinder Kaur. Biometric Authentication System For Access Control. Biometric Authentication System For Access Control. URL: https://ceur-ws.org/Vol-3706/Paper13.pdf.

4. AI security revolution: Exploring biometric innovations in access control. evalink: Integrated Security Solutions. URL: https://www.evalink.io/blog/the-future-of-access-control-biometrics-and-the-evolution-of-AI-security.

5. Srikanth Mandru. How AI can Improve Identity Verification and Access Control Processes. Scientific Research and Community | Open Access Journals. URL: https://onlinescientificresearch.com/articles/how-ai-can-improve-identity-verification-and-access-control-processes.pdf.

6. С. С. Шрамко О. В. Гальцова. ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОТИДІЇ ЗЛОЧИННОСТІ. Науково-дослідний інститут вивчення проблем злочинності імені академіка В.В. Сташиса. URL: https://ivpz.kh.ua/wp-content/uploads/2020/12/Матеріали-семінару_Використання-техн-штучного-інтел_5.11.2020.pdf.

7. Андрій Георгійович Гуралюк. ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІННОВАЦІЙНА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ У ПЕДАГОГІЧНИХ ДОСЛІДЖЕННЯХ. Welcome to - Digital Library NAES of Ukraine. URL:

https://lib.iitta.gov.ua/id/eprint/739798/1/VNIASO-AHS%20of%20Edu&Sci-RB-18-2023-67-79.pdf.

8. Test scores of AI systems on various capabilities relative to human performance. Our World in Data. URL: https://ourworldindata.org/grapher/test-scores-ai-capabilities-relative-human-performance.

9. Facial Recognition Market to Grow by USD 11.82 Billion (2024-2028), Rising Identity Threats Drive Growth, AI's Impact on Market Trends - Technavio. PR Newswire: press release distribution, targeting, monitoring and marketing. URL: https://www.prnewswire.com/news-releases/facial-recognition-market-to-grow-by-usd-11-82-billion-2024-2028-rising-identity-threats-drive-growth-ais-impact-on-market-trends---technavio-302305422.html.

10. What Science Really Says About Facial Recognition Accuracy and Bias Concerns - Security Industry Association. Security Industry Association. URL: https://www.securityindustry.org/2022/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/.

11. 29+ Biometrics Statistics for 2024. URL: https://photoaid.com/blog/biometrics-statistics/.

12. Мокін В.Б Дратований М.В. НАУКА ПРО ДАНІ: МАШИННЕ НАВЧАННЯ ТА ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ. URL: https://pdf.lib.vntu.edu.ua/books/2024/Mokin_2024_263.pdf.

13. Research Gate. URL: https://www.researchgate.net/.

14. Statista. URL: https://www.statista.com/.

15. GeeksForGeeks. URL: https://www.geeksforgeeks.org/.

16. How to Use Deep Learning for Face Detection and Recognition Systems?. Turn AGI Research into Real-World Impact | Turing. URL: https://www.turing.com/kb/using-deep-learning-to-design-face-detection-and-recognition-systems.

17. Daniel S´aez Trigueros Li Meng. Face Recognition: From Traditional to DeepLearning Methods. URL:

https://www.researchgate.net/publication/328685305_Face_Recognition_From_Traditional_to_Deep_Learning_Methods.

18. H. Fan, Z. Cao, Y. Jiang, Q. Yin, and C. Doudou, “Learning deep facerepresentation,” arXiv preprint arXiv:1403.2802, 2014.

19. F. Schroff, D. Kalenichenko, and J. Philbin, “Facenet: A unifiedembedding for face recognition and clustering,” in Proceedings of theIEEE conference on computer vision and pattern recognition, pp. 815-823, 2015

20. S.-H. Lin, S.-Y. Kung, and L.-J. Lin, “Face recognition/detection byprobabilistic decision-based neural network,” IEEE transactions onneural networks, vol. 8, no. 1, pp. 114-132, 1997.

21. General Data Protection Regulation GDPR. URL: https://gdpr-info.eu/.

22. Biometrics Statistics By Usage, Industries, Demands and Facts. Coolest Gadgets. URL: https://www.coolest-gadgets.com/biometrics-statistics/.

23. Grucela A. 65+ identity theft statistics to know going into 2025. URL: https://blog.incogni.com/identity-theft-statistics/.

24. Biometric Access Control System A Complete Guide. ARATEK | The World Leader in Biometrics Technology. URL: https://www.aratek.co/news/biometric-access-control-system-a-complete-guide.

25. Biometrics (Mainguet Jean-FranÃ§ois). URL: https://biometrics.mainguet.org/types/fingerprint/apple/Authentec_AES3500_flyer_prelim.pdf.

26. ShenZhen2U –PCB|Source|Assembly|Components. URL: https://www.shenzhen2u.com/doc/Module/Fingerprint/710-FPC1020_PB3_Product-Specification.pdf.

27. Fingerprint Analysis and Representation / D. Maltoni et al. SpringerLink. URL: https://link.springer.com/chapter/10.1007/978-3-030-83624-5_3.

28. Suprema BioMini Plus and BioMini Plus2 fingerprint readers - Neurotechnology.com. Fingerprint, face, eye iris, voice and palm print identification, speaker and object recognition software. URL: https://www.neurotechnology.com/fingerprint-scanner-suprema-biomini-plus.html.

29. ARM Cortex - A53 MPCore Processor. URL: https://docs.arduino.cc/resources/datasheets/cortexa53.pdf.

30. ZKTeco. Leading Suppliers of Smart Security Solutions and Systems. URL: https://www.zkteco.me/product-details/inbio160260460-1.

31. W5500. WIZNET.HK. URL: https://www.wiznet.hk/en/ethernet-controller/12-w5500.html.

32. Mean Well HDR-15-12. MEAN WELL Web: the official MEAN WELL Power Supplies distributor. URL: https://www.meanwell-web.com/en-gb/ac-dc-ultra-slim-din-rail-power-supply-input-range-hdr--15--12.

33. Welcome to Farnell Global | Global Electronic Component Distributor. URL: https://www.farnell.com/datasheets/612553.pdf.

34. New Espressif Module ESP32-WROVER-B | Espressif Systems. Wireless SoCs, Software, Cloud and AIoT Solutions | Espressif Systems. URL: https://www.espressif.com/en/news/new-espressif-module-esp32-wrover-b.

35. 2025 SecuGen Corporation. Biometric Standards. URL: https://secugen.com/biometric-standards/.

36. GeeksforGeeks. Introduction of Message Queue Telemetry Transport Protocol (MQTT) - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/introduction-of-message-queue-telemetry-transport-protocol-mqtt/.

37. IoT Based Biometric Attendance system using Arduino and Thingsboard. Circuit Digest - Electronics Engineering News, Latest Products, Articles and Projects. URL: https://circuitdigest.com/microcontroller-projects/iot-based-biometric-attendance-system-using-arduino-and-thingsboard.

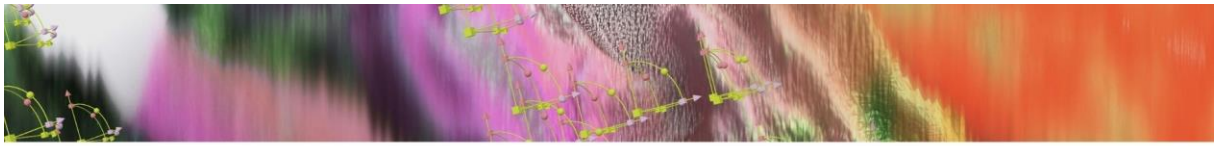
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ
НАУКОВИЙ КЕРІВНИК
Д. Т. Н. СТОРЧАК КАМІЛА ПАВЛІВНА

КИЇВ 2025 |

АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ І ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

ПРЕЗЕНТАЦІЯ ДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ
СТУДЕНТКИ ГРУПИ ІСД-41
СПЕЦІАЛЬНОСТІ 126 - ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ
ЛУНЬОВОЇ АЛІСИ ІГОРІВНИ



МЕТА: розробити **автоматизовану систему контролю доступу** на основі **біометричних даних** та технологій **штучного інтелекту**, що забезпечує **високу точність** ідентифікації, **безпеку даних** та **зручність використання**

ОБ'ЄКТ ДОСЛІДЖЕННЯ: біометричні системи контролю доступу та їх інтеграція з технологіями штучного інтелекту

ПРЕДМЕТ ДОСЛІДЖЕННЯ: методи та алгоритми обробки біометричних даних, апаратні та програмні рішення для реалізації системи контролю доступу

ЗАВДАННЯ

АНАЛІТИЧНА ЧАСТИНА

Провести **огляд сучасних біометричних технологій** та їх **застосування** в системах контролю доступу

Проаналізувати методи **використання штучного інтелекту** та **машинного навчання** для підвищення точності ідентифікації.

ПРАКТИЧНА ЧАСТИНА

Обґрунтувати вибір **апаратного забезпечення** для реалізації системи

Розробити **програмне забезпечення** для збору, обробки та зберігання біометричних даних із використанням **алгоритмів глибокого навчання**

Реалізувати **веб-інтерфейс** для адміністрування системи та забезпечення захисту даних відповідно до вимог GDPR

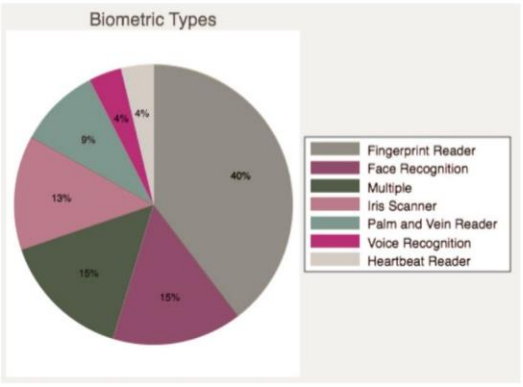
РОЗДІЛ 1: **БІОМЕТРІЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ - АНАЛІТИЧНИЙ БАЗИС**

1.1 ОСОБЛИВОСТІ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ

Біометрія **- унікальні фізіологічні та поведінкові характеристики**

Найпоширеніші методи: відбитки пальців, обличчя, сітківка ока

Надійність, унікальність, складність підробки



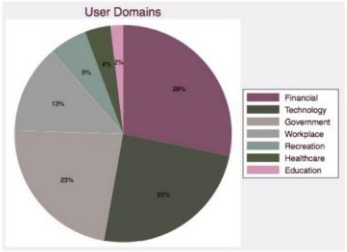
1.1 СФЕРИ ЗАСТОСУВАННЯ БІОМЕТРІЇ

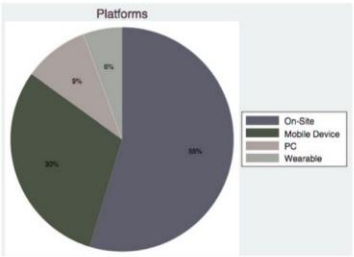
Загальні сфери послуг і діяльності, де використовують біометрію

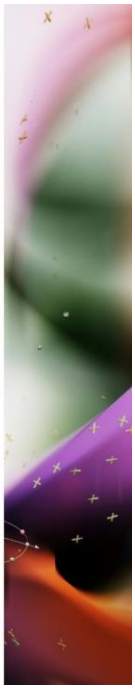
- Фінанси (банки, онлайн-платежі)
- Охорона здоров'я
- Транспорт, освіта, державні установи
- Розумні будинки, IoT

Платформи і пристрої для біометричної ідентифікації

- Стаціонарні системи
- Мобільні пристрої
- Персональні комп'ютери
- Носимі пристрої







Розділ 1: Біометрія та штучний інтелект - теоретичний базис

1.2 ШТУЧНИЙ ІНТЕЛЕКТ У БІОМЕТРІЇ

ШІ ДОЗВОЛЯЄ АДАПТИВНУ ОБРОБКУ ТА ВИЯВЛЕННЯ ШАБЛОНІВ

ВИКОРИСТОВУЄТЬСЯ ДЛЯ РОЗПІЗНАВАННЯ ТА ВАЛІДАЦІЇ ОСОБИ

ПІДВИЩЕННЯ ТОЧНОСТІ НАВІТЬ ЗА НИЗЬКОЇ ЯКОСТІ ДАНИХ

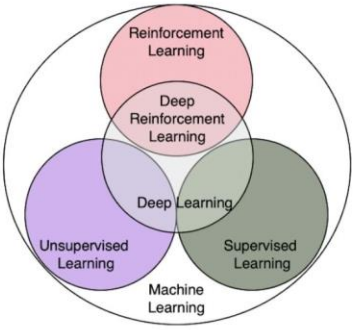
Розділ 1: Біометрія та штучний інтелект - теоретичний базис

1.2 МАШИННЕ НАВЧАННЯ

МЕТОДИ: SUPERVISED, UNSUPERVISED, REINFORCEMENT

АЛГОРИТМИ: SVM, K-NN, RANDOM FOREST, CNN

DEEP LEARNING - ТОЧНІСТЬ РОЗПІЗНАВАННЯ >99%



Розділ 1: Біометрія та штучний інтелект - теоретичний базис

1.3 КОМП'ЮТЕРНИЙ ЗІР У СИСТЕМАХ

ОТРИМАННЯ ТА ОБРОБКА ЗОБРАЖЕНЬ У РЕАЛЬНОМУ ЧАСІ

АЛГОРИТМИ: CNN, FACENET, DEEPFACE

ОСНОВНІ ЕТАПИ: ВИЯВЛЕННЯ, ВИРІВНЮВАННЯ, ВИЛУЧЕННЯ ОЗНАК, РОЗПІЗНАВАННЯ

Розділ 1: Біометрія та штучний інтелект - теоретичний базис

1.4 ЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ

БІОМЕТРИЧНІ ДАНІ = ЧУТЛИВА ІНФОРМАЦІЯ

ВАЖЛИВІСТЬ ПРОЗОРОСТІ, НЕДИСКРИМІНАЦІЇ, ОБМЕЖЕННЯ ДОСТУПУ

ПРОБЛЕМИ МАСОВОГО СТЕЖЕННЯ

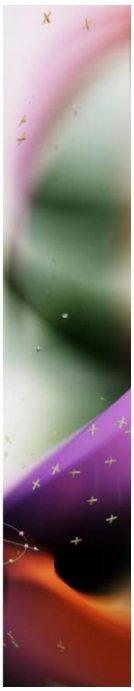
ПРАВОВІ АСПЕКТИ (GDPR)

Стандарти ЄС для **захисту персональних даних**

Ключові принципи: **згода, мінімізація даних, право на забуття**

Штрафи за порушення до 20 млн євро або 4% обороту

РОЗДІЛ 2: **АПАРАТНА РЕАЛІЗАЦІЯ**



Розділ 2: Апаратна реалізація

2.1 ТЕХНІЧНІ ВИМОГИ ДО ФУНКЦІОНАЛУ

Вимоги до функціоналу:

- Швидкість ідентифікації ≤ 0.5 с
- Підтримка 3000 користувачів
- Резервне живлення (8 год автономії) з можливістю гарячої заміни батареї
- Підтримка чорних/білих списків для управління доступом
- Журнал доступу з можливістю експорту даних. Інтерактивна система оповіщення

Апаратні вимоги:

- Сенсор: FAR (Коефіцієнт помилкового допуску) ≤ 0.001%, роздільна здатність 500 dpi (точок на дюйм)
- Процесор: ARM Cortex-A53, 4 ядра
- Енергоспоживання ≤ 1 Вт
- Тип підключення: UART, Wi-Fi

Розділ 2: Апаратна реалізація

2.1 ТЕХНІЧНІ ВИМОГИ ДО СТАНДАРТІВ БЕЗПЕКИ

Стандарти та безпека:

- Відповідність ISO/IEC 19794-2 (відбитки пальців)
- Шифрування AES-128 для захисту переданих даних
- Сертифікація FBI PIV
- Захист від несанкціонованого доступу

Критерії прийняття:

- Успішне тестування на 500 запитів/день
- Відмовостійкість у умовах високої вологості (IP65)
- Тестування в екстремальних умовах (діапазон температур -20°C до +60°C, стійкість до пилу, механічних впливів)
- Допустимий рівень помилкових відмов ≤ 1% у складних умовах експлуатації

Розділ 2: Апаратна реалізація

2.2 ДОСЛІДЖЕННЯ АПАРАТНИХ КОМПОНЕНТІВ

Сенсор Suprema BioMini Plus 2

Роздільна здатність 500 dpi, що забезпечує високу якість зображення

Швидкість зчитування ≤ 0,2 с

Алгоритм обробки - сертифікація FBI PIV

Процесор ARM Cortex-A53

Висока **обчислювальна здатність** до 1,2 ГГц

Чотири ядра для ефективної багатозадачності

Енергоефективність для складних обчислень, корисний для **обробки великих обсягів** біометричних даних

Контролер ZKTeco InBio460

Кількість **підтримуваних користувачів** 3000

Кількість **точок доступу** до 4 дверей на один контролер

Щифрування AES-128

Середній **час обробки** одного запиту становить 0,3-0,5 с

2.2 ДОСЛІДЖЕННЯ АПАРАТНИХ КОМПОНЕНТІВ

Комунікаційний модуль ESP32

Двохядерний Xtensa LX6 (240 МГц) та підтримка WPA2-Enterprise для **безпечного зв'язку**

Загальний **добовий трафік** 15 МБ

Блок живлення Mean Well HDR-15-12

Вихідна напруга 12 В, 1.25 А

ККД > 85%

Захист від **перевантаження**

2.3 ІНТЕГРАЦІЯ СЕНСОРА У СИСТЕМУ КОНТРОЛЮ ДОСТУПА

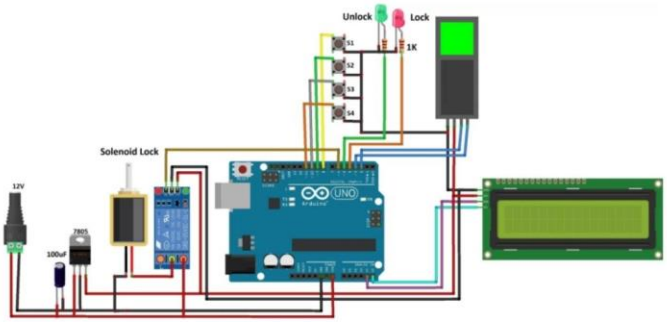
WIFI - З'ЄДНАННЯ З ESP32

БІБЛІОТЕКА ДЛЯ ARDUINO

ЗБЕРІГАННЯ ШАБЛОНІВ КОРИСТУВАЧІВ У БАЗІ

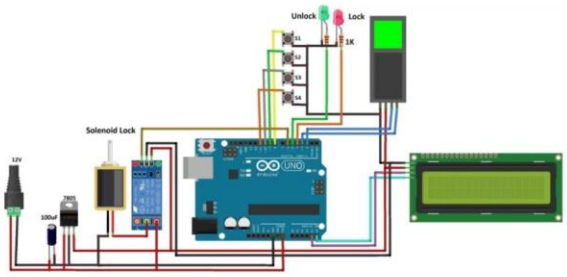
Розділ 2: Апаратна реалізація

2.3 СХЕМА ІНТЕГРАЦІЇ СЕНСОРА У СИСТЕМУ КОНТРОЛЮ ДОСТУПА З ВИКОРИСТАННЯМ ADRUINO



Розділ 2: Апаратна реалізація

2.3 СХЕМА ІНТЕГРАЦІЇ СЕНСОРА У СИСТЕМУ КОНТРОЛЮ ДОСТУПА З ВИКОРИСТАННЯМ ADRUINO



1. **Центральний мікроконтролер** - Arduino Nano (не ESP).
2. **Компоненти:**
   - Сканер відбитків пальців (FPS)
   - Arduino (TX/RX, VCC, GND)
   - LCD-дисплей (I2C)
   - Релейний модуль + соленоїдний замок
3. **Функціонал:**
   - Локальна ідентифікація відбитків
   - Відкриття замка при успішній аутентифікації

Підключення між компонентами - використовують **стандартні цифрові входи/виходи**.

Розділ 2: Апаратна реалізація

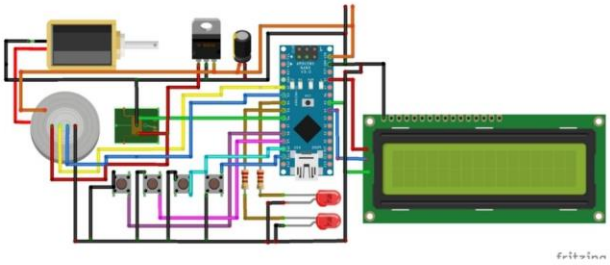
2.4 КОМПОНЕНТИ ДЛЯ РОБОТИ СИСТЕМИ

БІОМЕТРИЧНІ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ЗАЗВИЧАЙ ВКЛЮЧАЮТЬ КІЛЬКА ОСНОВНИХ КОМПОНЕНТІВ

1. **Сенсори** для зчитування біометричних характеристик
2. **Мікроконтролери** або процесори для обробки отриманих даних
3. **Модулі зв'язку** для передачі інформації
4. **Засоби зберігання** шаблонів та виконавчі механізми (наприклад, реле або соленоїдні замки)
5. **Шифрування переданих даних** на всіх етапах
6. Використання сучасних **криптографічних алгоритмів**, наприклад, AES (Advanced Encryption Standard) під час передачі даних через **комунікаційні канали** (Wi-Fi або UART)

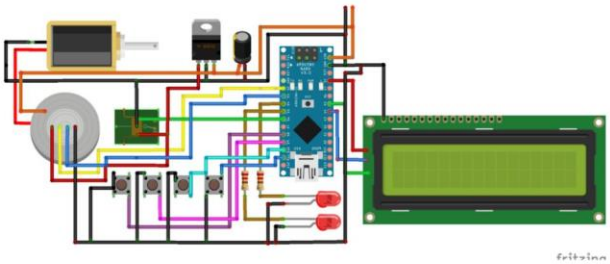
Розділ 2: Апаратна реалізація

2.4 ПРИНЦИП РОБОТИ СИСТЕМИ



1. **КОРИСТУВАЧ ПРИКЛАДАЄ ПАЛЕЦЬ**
2. **ДАНІ ПЕРЕДАЮТЬСЯ В ADRUINO**
3. **СИСТЕМА ПОРІВНЮЄ З БАЗОЮ**
4. **ДОСТУП НАДАНО АБО ВІДХИЛЕНО**

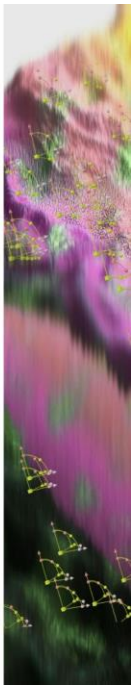
2.4 ПРИНЦИП РОБОТИ СИСТЕМИ



1. **Нові компоненти:**
   - Контролер ZKTeco InBio460 (підтримка 3000 користувачів)
   - RS-485 для зв'язку
2. **Поліпшення:**
   - Масштабування системи для 4 дверей
   - Шифрування AES-128

2.5 ПЕРЕВАГИ IOT В СИСТЕМІ КОНТРОЛЮ ДОСТУПА

ПЕРЕДАЧА ДАНИХ НА СЕРВЕР АБО В ХМАРУ	Дані логів, стан системи, доступи зберігаються онлайн
ВІДДАЛЕНИЙ МОНІТОРИНГ	Перевірка активності системи через веб-інтерфейс
ІНТЕГРАЦІЯ З ІНШИМИ ПРИСТРОЯМИ (РОЗУМНИЙ ДІМ)	Наприклад, автоматичне відкриття дверей або включення освітлення



Розділ 2: Апаратна реалізація

2.5 IOT ДЛЯ КРАЩОГО КЕРУВАННЯ СИСТЕМОЮ

НАВІЩО IOT В СИСТЕМІ?

Для віддаленого керування доступом - через інтернет, навіть не перебуваючи на місці

Для зберігання і аналізу даних у хмарі

Для гнучкої інтеграції з іншими системами безпеки

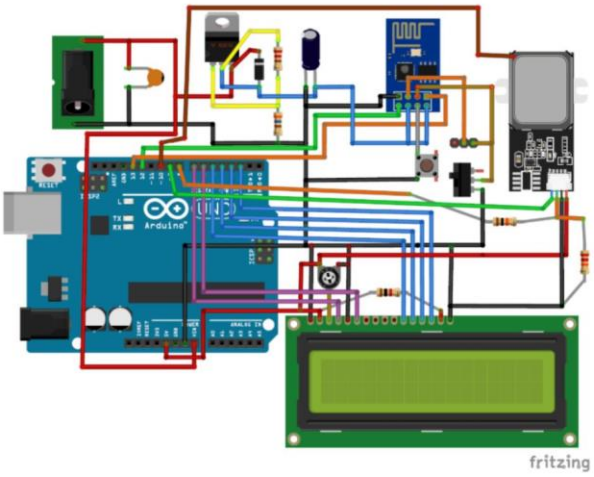
ШВИДКЕ РЕАГУВАННЯ НА ПОДІЇ

ЦЕНТРАЛІЗОВАНИЙ КОНТРОЛЬ ДОСТУПУ

МАСШТАБОВАНІСТЬ

Розділ 2: Апаратна реалізація

2.5 ІНТЕГРАЦІЯ IOT У СИСТЕМУ



1. **Нові компоненти:**
   - Модуль Wi-Fi ESP8266
   - Хмарна платформа ThingsBoard
2. **Функціонал:**
   - Віддалений моніторинг через MQTT
   - Журналювання подій у хмарі
   - Код: Фрагмент setup() для Wi-Fi (Рис. 2.17)

2.5 ІНТЕГРАЦІЯ ІОТ У СИСТЕМУ

1.ІДЕНТИФІКАЦІЯ КОРИСТУВАЧА:

Користувач прикладає палець до сканера відбитків GT511C3 FPS

Arduino UNO розпізнає відбиток і зіставляє його з зареєстрованим ID та іменем

2.ПЕРЕДАЧА ДАНИХ:

Ім'я користувача передається через серіальний порт до Wi-Fi модуля ESP8266

3.ОБРОБКА ТА НАДСИЛАННЯ В ХМАРУ:

ESP8266 формує дані у форматі JSON і передає їх на хмарну платформу ThingsBoard за допомогою протоколу MQTT

4.ВІЗУАЛІЗАЦІЯ ТА МОНІТОРИНГ:

У ThingsBoard дані зберігаються, візуалізуються у вигляді телеметрії та доступні адміністратору через веб-інтерфейс у реальному часі

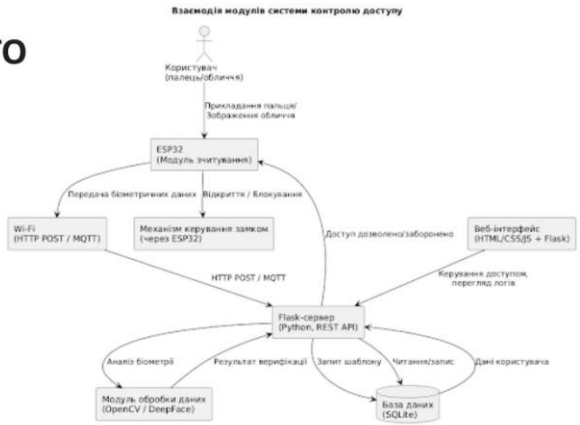
5.Виведення результату:

На LCD-дисплеї відображається ім'я ідентифікованого користувача та повідомлення про успішний доступ

РОЗДІЛ 3: **ПРОГРАМНА ЧАСТИНА**

3.1. АРХІТЕКТУРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

1. **Клієнт** (користувач, сенсор)
2. **Контролер** (ESP32)
3. **Сервер** (база даних, логіка)
4. **Інтерфейс** (веб-додаток)

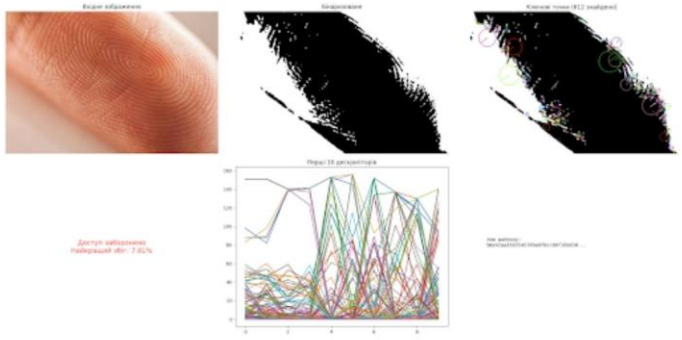


3.1. ПРИНЦИП РОБОТИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

1. **Збір біометричних даних:** Сканування відбитка пальця (або обличчя в майбутньому) за допомогою ESP32.
2. **Передача даних на сервер:** Відправлення зчитаних біометричних даних через Wi-Fi за допомогою протоколу MQTT.
3. **Обробка на сервері:** Прийом запиту сервером (Python). Верифікація біометричних даних шляхом порівняння з базою шаблонів (SQLite).
4. **Прийняття рішення:** Надсилання відповіді: дозвіл або відмова у доступі.
5. **Керування замком:** Активація або блокування електронного замка залежно від результату перевірки.

Розділ 3: Програмна частина

3.2 АЛГОРИТМИ ОБРОБКИ ДАНИХ



ОТРИМАННЯ ТА ФІЛЬТРАЦІЯ ДАНИХ

ВИЛУЧЕННЯ ОЗНАК

ПОРІВНЯННЯ З ШАБЛОНОМ

ПРИЙНЯТТЯ РІШЕННЯ

Розділ 3: Програмна частина

3.3 ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ ПРОЦЕСІВ ПЕРЕВІРКИ ОСОБИ ТА КОНТРОЛЮ ДОСТУПУ

DEEP LEARNING: CNN + FACENET/DEEPFACE

НАВЧАННЯ МОДЕЛЕЙ НА ВІДБИТКАХ/ОБЛИЧЧЯХ

ПІДВИЩЕННЯ ТОЧНОСТІ ТА СТІЙКОСТІ ДО ШУМУ

Розділ 3: Програмна частина

3.4 ВЕБ-ІНТЕРФЕЙС

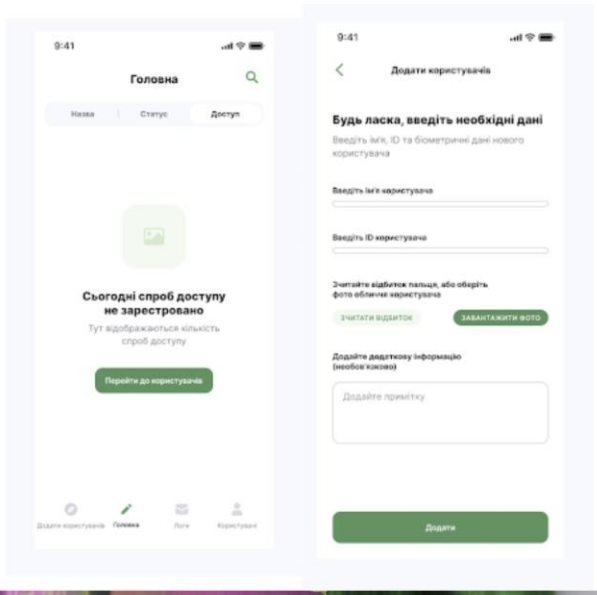
СТВОРЕНИЙ ВЕБ-ІНТЕРФЕЙС МАЄ СТОРІНКИ:

Вхід / Вихід з акаунту

Головна сторінка: Журнал доступу

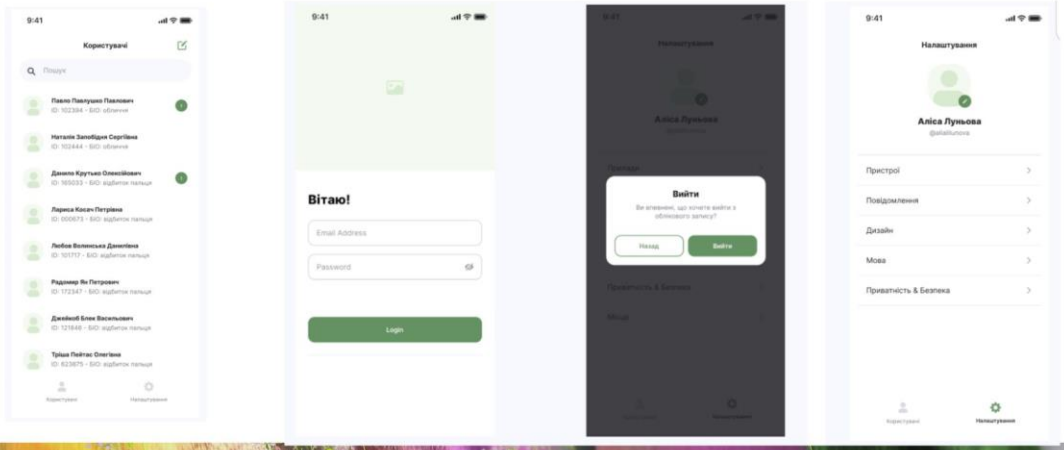
Реєстрація / редагування / видалення користувача

Налаштування



Розділ 3: Програмна частина

3.4 ВЕБ-ІНТЕРФЕЙС



3.5 БЕЗПЕКА ТА ЗАХИСТ

ХЕШУВАННЯ БІОМЕТРИЧНИХ ДАНИХ

Біометричні шаблони **не зберігаються** у відкритому вигляді
Перед збереженням у пам'яті пристрою або надсиланням - дані проходять **хешування** (наприклад, через SHA-256)

АВТОРИЗАЦІЯ КОРИСТУВАЧА

Адміністративна панель веб-інтерфейсу захищена **логіном** і **паролем**
Тільки **авторизовані користувачі** можуть **додавати** або **видаляти** шаблони
Впровадження **двофакторної автентифікації** можливе в майбутньому

Розділ 3: Програмна частина

3.5 БЕЗПЕКА ТА ЗАХИСТ

ЗАХИЩЕНА ПЕРЕДАЧА ДАНИХ (HTTPS + БАЗОВЕ ШИФРУВАННЯ)

Дані, які передаються між **мікроконтролером** (ESP32) і **сервером**, захищаються через **протокол HTTPS**
Для **внутрішніх обмінів** використовується **базове шифрування** (наприклад, **AES** або вбудоване шифрування в ESP32)

ВІДПОВІДНІСТЬ GDPR

Всі операції з біометрією відповідають принципам **GDPR**:
- Збір даних - **лише зі згоди користувача**
- Мінімізація: зберігаються **лише необхідні шаблони**
- Користувач має право **на видалення своїх даних** ("право на забуття")

Передбачена можливість **повного очищення бази даних** за запитом

АПРОБАЦІЯ

Апробація

АПРОБАЦІЯ ДОСЛІДЖЕННЯ ЗДІЙСНЮВАЛАСЬ У ФОРМІ УЧАСТІ В ФАХОВИХ КОНФЕРЕНЦІЯХ:

1. II всеукраїнська науково-технічна конференція «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» з поданням тези на тему «**Штучний інтелект та машинне навчання у побуті та промисловості**».

2. XV міжнародна наукова конференція студентів та молодих вчених «Сучасні інформаційні технології 2025» з поданням тези на тему «**Розробка системи багатофакторної аутентифікації з використанням біометричних даних і штучного інтелекту».**

ВИСНОВКИ

Висновки

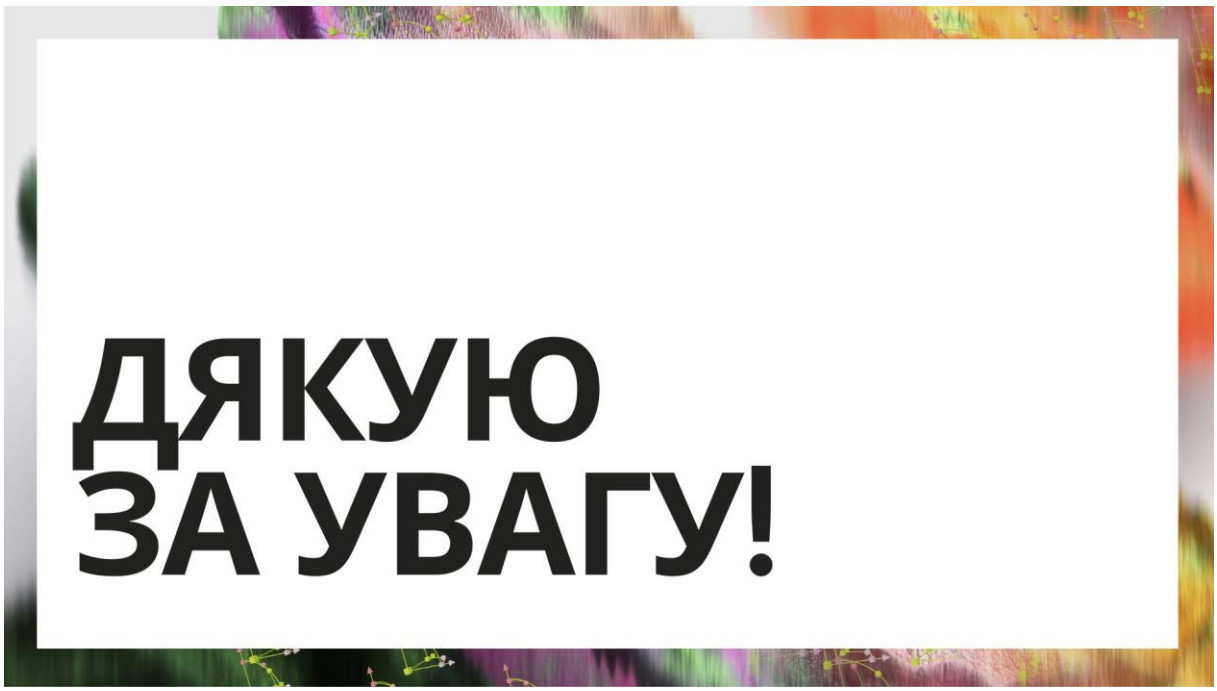
БІОМЕТРИЧНІ ТЕХНОЛОГІЇ (ЗОКРЕМА РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ТА ВІДБИТКІВ ПАЛЬЦІВ) **Є ЕФЕКТИВНИМИ, НАДІЙНИМИ ТА ЗРУЧНИМИ ДЛЯ КОНТРОЛЮ ДОСТУПУ**

ПОБУДОВА СИСТЕМИ НА БАЗІ МІКРОКОНТРОЛЕРА ESP32 ТА IOT-ПІДХОДІВ ЗАБЕЗПЕЧУЄ ДОСТУПНІСТЬ, ГНУЧКІСТЬ І БЕЗПЕКУ

ВИКОРИСТАННЯ AI ТА КОМП'ЮТЕРНОГО ЗОРУ (PYTHON, ГЛИБОКЕ НАВЧАННЯ) ДОЗВОЛЯЄ ОБРОБЛЯТИ БІОМЕТРИЧНІ ДАНІ В РЕАЛЬНОМУ ЧАСІ З ВИСОКОЮ ТОЧНІСТЮ

ДОТРИМАННЯ ВИМОГ GDPR Є КРИТИЧНО ВАЖЛИВИМ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

РОЗРОБЛЕНА СИСТЕМА МАСШТАБОВАНА Й ЛЕГКО АДАПТУЄТЬСЯ ДО РІЗНИХ СФЕР ЗАСТОСУВАННЯ - ВІД РОЗУМНИХ БУДИНКІВ ДО КОРПОРАТИВНИХ МЕРЕЖ


ДЯКУЮ
ЗА УВАГУ!