**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**
**КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**
**КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ**

# КВАЛІФІКАЦІЙНА РОБОТА

На тему:
«Захист персональних даних інтелектуальною біометричною системою контролю доступом»

на здобуття освітнього ступеня магістра
Зі спеціальності 125 Кібербезпека та захист інформації .
(*код найменування спеціальності*)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

Виконав: здобувач вищої освіти групи СЗДМ-61
Роман Чечко

Керівник: Юрій Пепа Юрій Пепа
(Ім’я, Призвіше)

Рецензент:
(Ім’я, Призвіше)

Київ 2026

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**
**КІБЕОБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____Магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту

**ЗАТВЕРДЖУЮ**
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУРОБОТУ

_____ЧЕЧКУ Роману Олександровичу_____
*(прізвище, ім'я, по батькові здобувача)*

1. Тема кваліфікаційної роботи: «Захист персональних даних інтелектуальною біометричною системою контролю доступом»
«Захист персональних даних інтелектуальною біометричною системою контролю доступом»
керівник кваліфікаційної роботи _____Пепа Юрій к.т.н., доцент
*(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)*
затверджені наказом Державного університету інформаційно-комунікаційних технологій
від «30» жовтня 202 р. № 467

2. Строк подання кваліфікаційної роботи « 15» 12.2025р.

3. Вихідні дані до кваліфікаційної роботи:
_ Біометричні системи доступу.
_ Принцип роботи біометричних систем доступу.
__Штучний інтелект в моделі біометричного доступу .

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.__Перелік та пояснення роботи біометричних систем доступу _
2.__Мультимодальна біометрична система доступу ___
3.__Вдосконалення існуючої біометричної моделі доступу
5. Перелік графічного матеріалу: ____Презентація_матеріал на слайдах_____
6. Дата видачі завдання:_____15.10.25_____

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | Підбір науково-технічної літератури | 17.11.25 | |
| 2 | Написання першого розділу роботи | 22.11.25 | |
| 3 | Написання другого розділу роботи | 01.12.25 | |
| 4 | Написання третього розділу роботи | 14.12.25 | |
| 5 | Написання висновків по роботі | 14.12.25 | |
| 6 | Підготовка демонстраційних матеріалів | 15.12.25 | |
| 7 | Підготовка доповіді | 15.12.25 | |

Здобувач вищої освіти _____ Роман Чечко
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Юрій Пепа
*(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

# РЕФЕРАТ

Текстова частина магістерської кваліфікаційної робота містить: 79 Сторінок **14 рисунків 35 Джерел**

Об’єкт дослідження – Процес забезпечення інформаційної безпеки та захисту персональних даних у системах контролю доступу .

Предмет дослідження – Методи, алгоритми та технології захисту персональних даних у біометричних системах контролю доступу.

Мета роботи – дослідити інтелектуальну біометричну систему контролю доступу з метою підвищення рівня захисту персональних даних

*Методи дослідження* – аналітичні методи, опрацювання літератури за даною темою.

У роботі досліджені існуючі біометричні системи доступу, їх принцип роботи та стандарти що їх регулюють.

Область застосування – забезпечення безпеки в більшості областей

**Апробація:**

**Р.О. Чечко, К.І. Раус,** ОЦІНКА ЕФЕКТИВНОСТІ БІОМЕТРИЧНИХ СИСТЕМ. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.53-54. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова : ЗАХИСТ ІНФОРМАЦІЇ, БІОМЕТРІЯ, БІОМЕТРИЧНА ХАРАКТЕРИСТИКА, БІОМЕТРИЧНА ТЕХНОЛОГІЯ, ІДЕНТИФІКАЦІЯ, ІДЕНТИФІКАЦІЯ, ХАРАКТЕРИСТИКИ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ

## ABSTRACT

The text part of the master's qualification work contains: 79 Pages 14 Figures 35 Sources

*Object of research* – The process of ensuring information security and personal data protection in access control systems.

*Subject of research* – Methods, algorithms and technologies for protecting personal data in biometric access control systems.

The purpose of the work is to investigate an intelligent biometric access control system in order to increase the level of personal data protection

*Research methods* – analytical methods, literature review on this topic.

The work examines existing biometric access systems, their operating principle and the standards that regulate them.

Scope – ensuring security in most areas


Keywords: INFORMATION PROTECTION, BIOMETRY, BIOMETRIC CHARACTERISTICS, BIOMETRIC TECHNOLOGY, IDENTIFICATION, IDENTIFICATION, CHARACTERISTICS OF BIOMETRIC TECHNOLOGIES

# ЗМІСТ

## Перелік умовних позначень

СКУД – Система контролю і управління доступом

КД – контроль доступу

ЗІ – захист інформації

СЗІ – система захисту інформації СКД (Access Control Systems) – система контролю доступу

БД – база даних

НМ – нейронна мережа

БСД – біометрична система доступу

БХС – біометрична характеристика людини

# Вступ

У сучасних умовах стрімкого розвитку цифрових технологій питання забезпечення безпеки інформації та захисту персональних даних набуває особливої актуальності. Зростання обсягів оброблюваних даних, поширення електронних сервісів та діяльність організацій, що працюють з конфіденційною інформацією, потребують впровадження надійних та ефективних механізмів контролю доступу. Традиційні засоби автентифікації, такі як паролі чи ключові картки, вже не можуть повною мірою гарантувати необхідний рівень захисту, оскільки схильні до втрати, підробки або компрометації.

Біометричні системи, що ґрунтуються на фізичних або поведінкових характеристиках людини, виступають одним із найбільш перспективних напрямів підвищення інформаційної безпеки. Вони забезпечують високий рівень достовірності ідентифікації користувача, знижують ризик несанкціонованого доступу та мінімізують людський фактор. Разом із тим, сучасні виклики вимагають застосування не просто біометричних технологій, а інтелектуальних систем, здатних адаптуватися до змін, аналізувати складні дані та забезпечувати комплексний захист.

Інтелектуальні біометричні системи контролю доступу поєднують алгоритми штучного інтелекту, машинного навчання та способи багатофакторної автентифікації. Це дозволяє підвищити точність розпізнавання, виявляти підозрілу активність та забезпечувати надійний захист персональних даних відповідно до вимог національного та міжнародного законодавства у сфері інформаційної безпеки.

Актуальність обраної теми зумовлена необхідністю впровадження сучасних безпекових рішень для захисту конфіденційної інформації, а також постійним зростанням кількості кібератак, пов’язаних із несанкціонованим доступом. Розробка та дослідження інтелектуальної біометричної системи контролю доступу сприятиме підвищенню ефективності систем захисту даних, що є важливим як для державних установ, так і для приватного сектору.

Об’єкт дослідження – Процес забезпечення інформаційної безпеки та захисту персональних даних у системах контролю доступу .

Предмет дослідження – Методи, алгоритми та технології захисту персональних даних у біометричних системах контролю доступу.

Мета роботи – дослідити інтелектуальну біометричну систему контролю доступу з метою підвищення рівня захисту персональних даних

Наукове завдання : описати біометричні системи, вдосконалити існуючу .

## 1.Біометричні система доступу

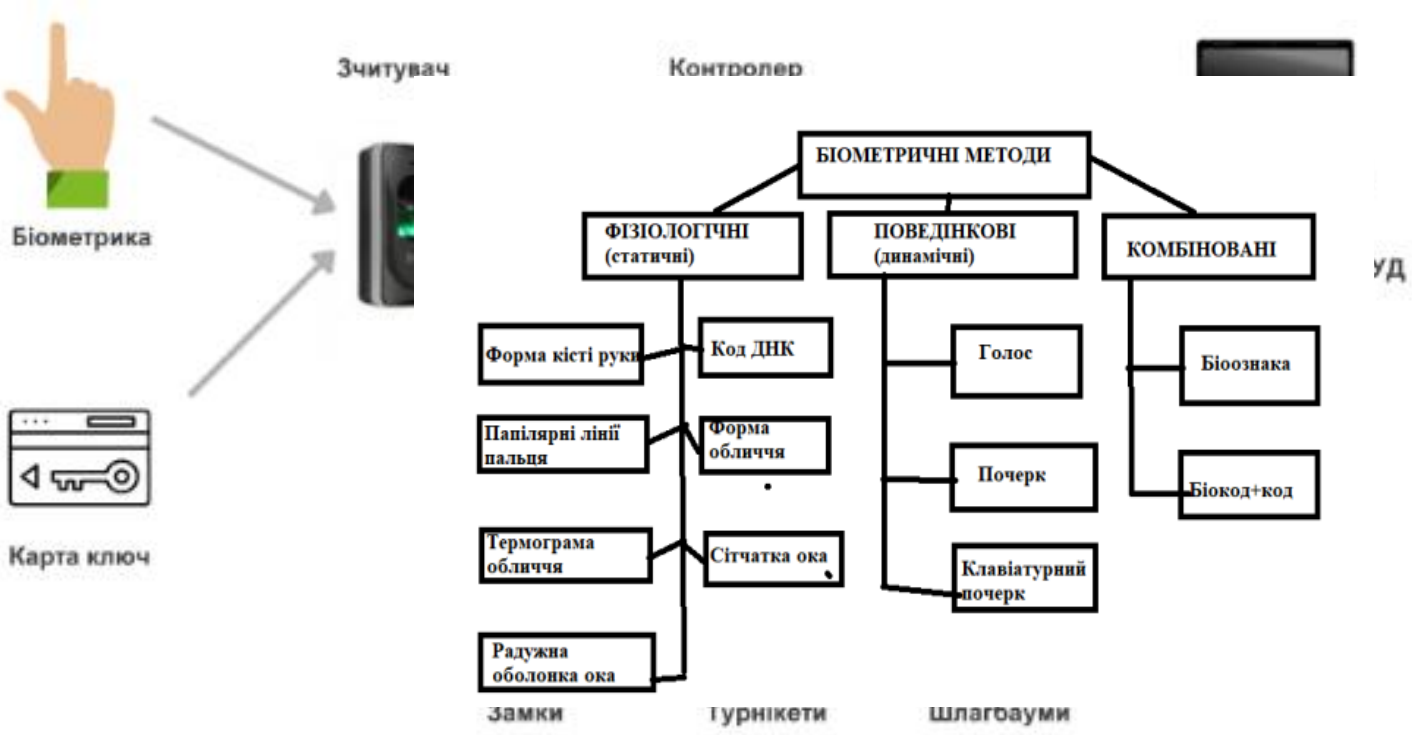


Рис.1 Біометричні системи доступу

Рис.2 класифікація біометричних методів

Біометрична система доступу – це програмний комплекс безпеки , який використовує унікальні біологічні характеристики людини та поділяються на Біометричні та Поведінкові біометричні характеристики . Особливості створення біометричних систем в інформаційній безпеці та захисту інформації В завданнях інформаційної безпеки та захисту інформації БСКД застосовуються для заміни процедури входу в автоматизовані системи через пароль, смарт-карти тощо на вхід через біометричні характеристики особистості. Широка спроможність використання засобів БСКД є ідентифікація або верифікація за біометричними параметрами в корпоративній мережі або під час входу на робочу станцію автоматизованої системи. Для захисту робочої станції 12 автоматизованої

системи створюються шаблони біометричних даних найчастіше ними є відбитки пальців, які зареєстровані користувачами, які перебувають на ОІД. Після успішної реалізації процедури ідентифікації користувач отримує доступ. Протягом реалізації технології в корпоративній мережі шаблони БШ активних користувачів, які працюють в мережі, зберігаються централізовано на спеціально створеному сервері аутентифікації. В період входу в мережу, користувач, піддається процедурі біометричної ідентифікації, яка взаємодіє безпосередньо зі спеціалізованим сервером, на якому і перевіряються сформовані ідентифікатори. Створення в структурі корпоративної мережі окремого сервера біометричної автентифікації дає можливість зберігати на такому сервері конфіденційну інформацію, доступ до якої надається виключно на основі біометричної ідентифікаційної ознаки власника інформації. В даній сфері отримало широкого застосування такі технології розпізнавання, як відбиток пальця, райдужна оболонка ока, голос, почерк, набір інформації клавіатурою.

Біометрична ідентифікація – це процес автоматичного розпізнавання або підтвердження особи за допомогою вимірювання та аналізу унікальних рис, притаманних тільки їй. Важливо підкреслити, що мова йде не лише про «впізнавання» у вузькому сенсі, а про цілісний процес обробки сигналів: від збору даних через сенсори, їх попередньої нормалізації, до вилучення ключових ознак і зіставлення з базою реєстрових шаблонів.

Українські закони що регулюють процедури збору та обробки біометричних даних :

В нашій країні ще донедавна продовжувалася боротьба з «міткою звіра», доки в цьому питанні не була поставлена крапка рішенням Верховного суду у складі колегії суддів Касаційного адміністративного суду 26.03.2018 р. у справі №806/3265/17.

Загалом, питання збору, використання та обробки біометричних даних регулюється низкою нормативних актів:

- Цивільний кодекс України;

- Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» (далі – Закон ЄДДР);

- Закон України «Про захист персональних даних» (*далі – Закон ЗПД*);

- Закон України «Про інформацію»;

- Закон України «Про правовий статус іноземців і осіб без громадянства»;

- Закон України «Про біженців та осіб, які потребують додаткового або особливого захисту»;

- Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства, затверджене постановою КМУ від 27.12.2017 р. №1073 (*далі – Положення*);

- Інструкція про порядок фіксації біометричних даних (параметрів) іноземців та осіб без громадянства посадовими особами Державної міграційної служби України, її територіальних органів і територіальних підрозділів, затверджена наказом МВС України від 23.11.2018 р. №944 (зареєстрована в МЮ України 17.12.2018 р. за №1428/32880).

Українське законодавство значно вужче захищає права українських громадян, якщо порівнювати з GDPR, BIPA і CCPA, в результаті чого можливі зловживання. Хоча біометричні технології спрощують автентифікацію та мали б посилювати захист, фактичний збір і зберігання даних створюють нові загрози для нашої безпеки та водночас є причиною виникнення нових проблем (конфіденційності щодо збору та зберігання біометричних даних).

# 1 Біометричні характеристики та методи їх перевірки

-Відбитки пальців – кожна людина має свій унікальний візерунок свого відбитка пальців , на даний момент є найпоширенішим методом БСД;

При цій системі доступу використовується контактний та безконтактний оптичний сканер.

## 1.8 Контактний оптичний сканер

Контактний оптичний сканер – складається з оптоволоконної матриці з дуже великою щільністю , чутливість кожного елемента дозволяє зчитувати залишкове світло що потрапляє на палець в точці натиску на поверхні сканеру, після чого за допомогою алгоритмів відбувається зліпок зображення відбитку.

### .8.3 Переваги контактного оптичного сканеру:

- Висока якість зображення ;
- Невисока вартість обладнання;
- Простота конструкції ;
- Висока точність у стандартних робочих умовах;
- Підтримка великої кількості алгоритмів роботи з різним програмним забезпеченням;

### 1.1.2 Недоліки контактного оптичного сканеру:

- Низька гігієнічність , через часту взаємодію з поверхнею ;
- Накопичення бруду на поверхні , що викликають помилки ідентифікації;
- Зношення сенсорної панелі;
- Чутливість до стану відбитка – при мікротравмах чи потрісканій шкірі може ;некоректно спрацювати.
- Нижча стійкість до атак порівняно з 3D-технологіями;
- Низька ефективність при неправильному прикладанні пальця;
-Вразливість перед залишковим відбитком.


Рис.3 Контактний Сканер відбитків пальців

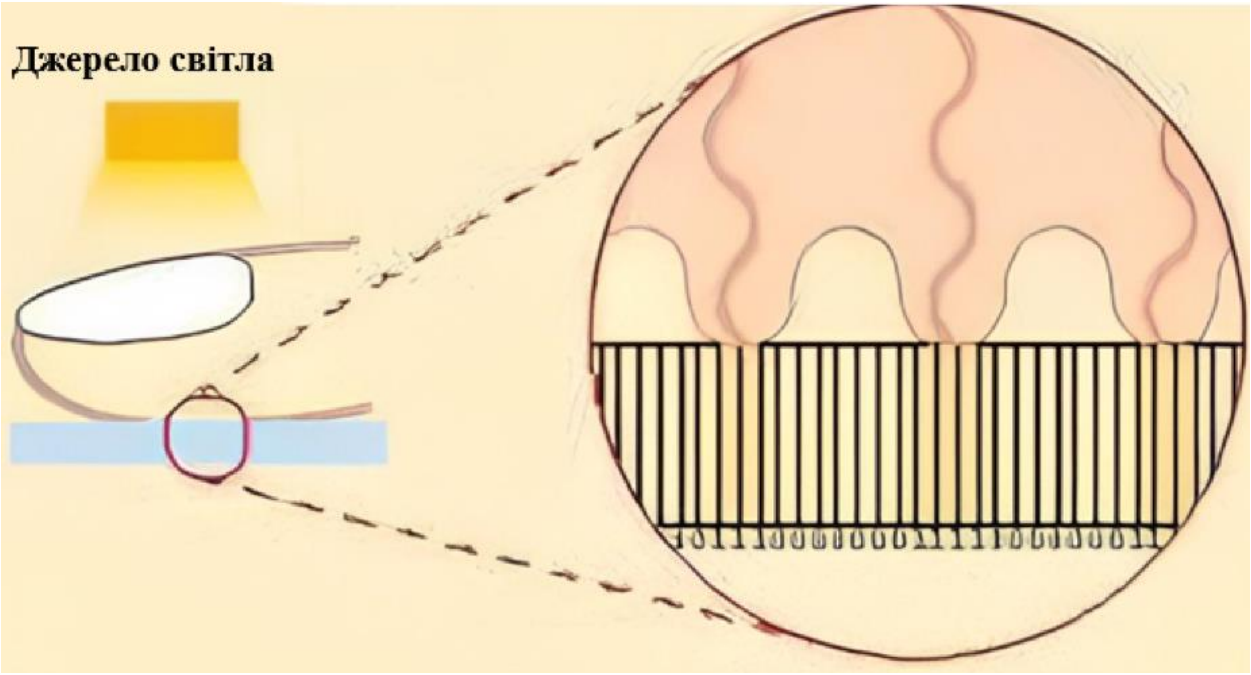


Рис.4 Схема роботи контактного оптичного сканеру

### 1.1.3 Стандарти контактного оптичного сканеру відбитків пальців:

- ***ISO/IEC 19794-4 –*** Регламентує формат зображення відбитків пальців, отриманих як оптичними, так і ємнісними сканерами;

- ***ISO/IEC 19794-2*** – Описує формат зберігання мінутій (галужень, кінців ліній), які виділяються із зображення;

- ***ISO/IEC 19794-1*** – Визначає правила: обміну даними, структуру заголовків, вимоги до метаданих;

- ***ISO/IEC 29794-4 –*** Регулює методики оцінки якості відбитків пальців ;

- ***ISO/IEC 30107 –*** захисту від підробок;

- ***ISO/IEC 19792 –*** Регулює безпеку біометричних систем;

- ***ISO 14443 / ISO 19092 –*** Регулює передачу даних у карткових або банківських системах, де використовується відбиток пальця**.**

## 1.8 Безконтактний оптичний сканер

Безконтактні сканери працюють за принципом знімання фото або 3D-карти відбитка без фізичного дотику. У зв’язку з потребами безпеки та зменшенням санітарних ризиків.

### 1.8.3 Переваги безконтактного оптичного сканеру:

-Висока гігієнічність ;

-Відсутність зносу сенсору ;

-Відсутність залишкового відбитку;

-Краща точність для складних пальців;

-Адаптивність до систем штучного інтелекту :

-Можливість до віддаленого користування .

### 1.2.2 Недоліки контактного оптичного сканеру:

- Висока вартість;
- Чутливість до зовнішнього освітлення;
- Високі вимоги до точності позиціонування;
- Складні алгоритми реконструкції 3D-відбитків;
- Уразливість до оптичних перешкод;
- Відсутність фізичної фіксації пальця;
- Складність захисту від підробок у вигляді фото або відео;
- Вища залежність від чистоти шкіри та світло відбивання.

### 1.2.3 Стандарти безконтактного оптичного сканеру відбитків пальців:

- ***ISO/IEC 19794-4:2011*** **/ 2019 – стандарт, який регулює :** формати зображень відбитків пальців, вимоги до роздільної здатності, характеристики оптики та якості, методи стиснення;

- ***ISO/IEC 19794-13:2018*** – стандарт регулює схеми «скелетонізації» відбитка (використовується у нейронних touchless-системах для побудови цифрового шаблону);

- ***ISO/IEC 29794*** – вимоги до якості біометричних даних;

- ***ISO/IEC 30107*** - стандарт визначає методи захисту від атак;

- ***ISO/IEC 38520*** – Це новітній стандарт, спеціально створений для безконтактного сканування відбитків пальців . визначає : методи тестування touchless-систем, допустимі спотворення (перспективні, геометричні), вимоги до 3D-реконструкції та трансформації до 2D, параметри оцінки продуктивності;

- ***ISO/IEC 39794-4:2023*** – вимоги спеціально для безконтактного сканування;

- *ISO/IEC 19989* – зберігання відбитків від витіку ;

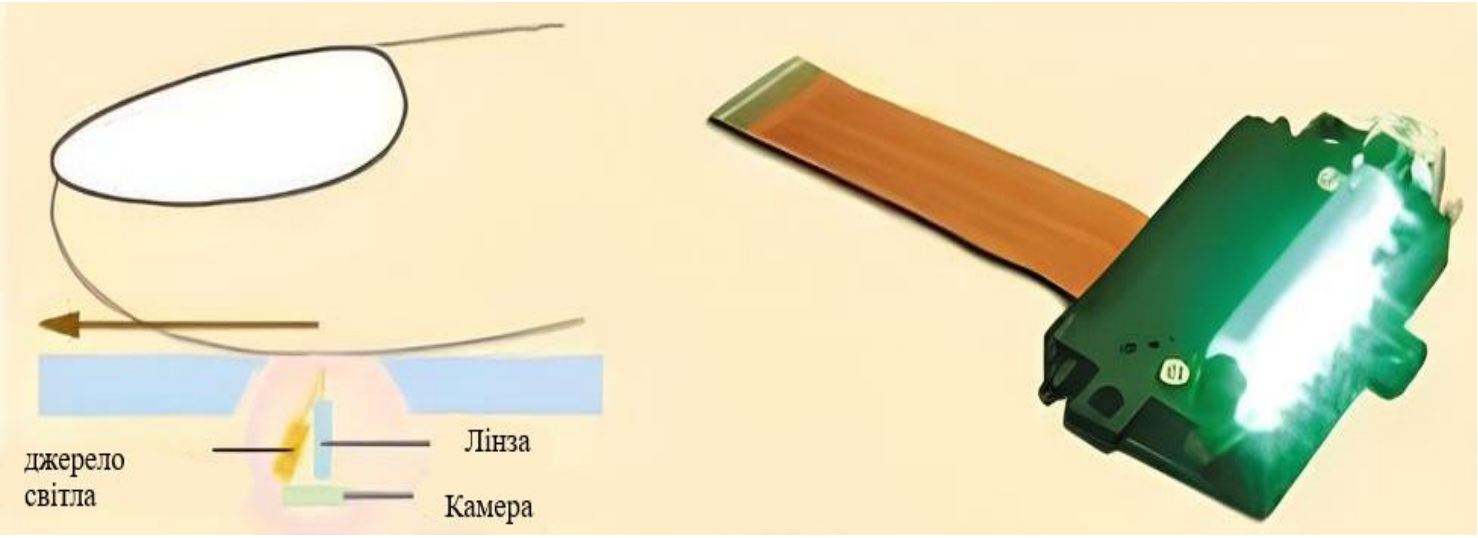


Рис.5 Принцип роботи безконтактного оптичного сканеру


Рис.6 Безконтактний сканер відбитків пальців

## 1.3 Технологія розпізнавання обличчя

Розпізнавання обличчя – проводиться аналіз геометрії обличчя тобто перевірка відстані маж очима , контури носа , щелепи , будова черепа… Сучасні моделі використовують 3D моделі та нейромережі для перевірки обличчя ;

### 1.3.1Принцип роботи :

- Виявлення обличчя – визначення позиції голови прийнято здійснювали детектором Віоли-Джонса, що в чистому вигляді будується за допомогою Machine Learning . Він використовує каскад Хаара, який є набором примітивів, для яких розраховують їх згортку з зображенням. Використовуються найпростіші примітиви, що складаються з прямокутників і мають всього два рівні, +1 і -1. При стандартному розмірі примітива в 24x24 пікселя, можливі 162 тисячі різних ознак і занадто довга процедура розрахунку.. Стандарт ***ISO/IEC 2382-37:2017*** встановлює терміни та базові принципи біометричних операцій, включно з детекцією обличчя.;

- Вирівнювання та нормалізація обличчя : виправляє нахил голови центрує очі нормалізує освітлення встановлює однаковий розмір і масштаб;

- Виділення ключових точок таких як очі , брови , краї губ і … Зазвичай 68-128 точок (у сучасних нейромережах більше за 468);

- Генерація біометричного шаблону на основі ключових точок та текстури формується унікальний біометричний шаблон. Нейромережі (FaceNet, ArcFace, DeepFace) переводять зображення у математичний вектор (256–1024 чисел), що характеризує пропорції обличчя форму носа, щелепи, очей текстурні особливості.

- Порівняння з базою даних;

- Прийняття рішення.

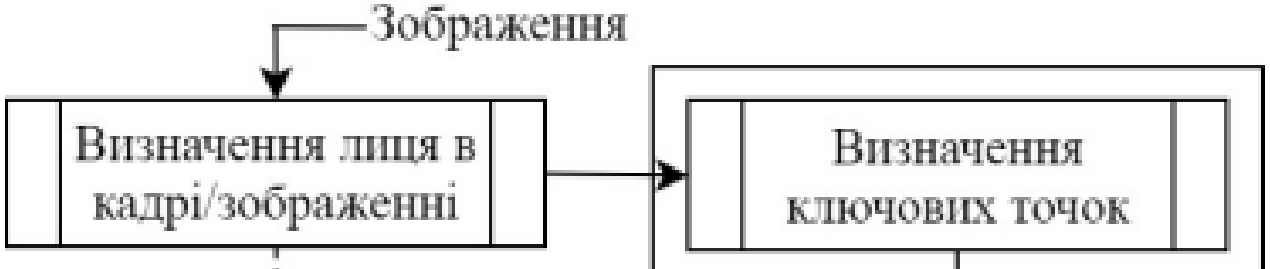

Рис.7 Схема роботи т**ехнології розпізнавання обличчя**

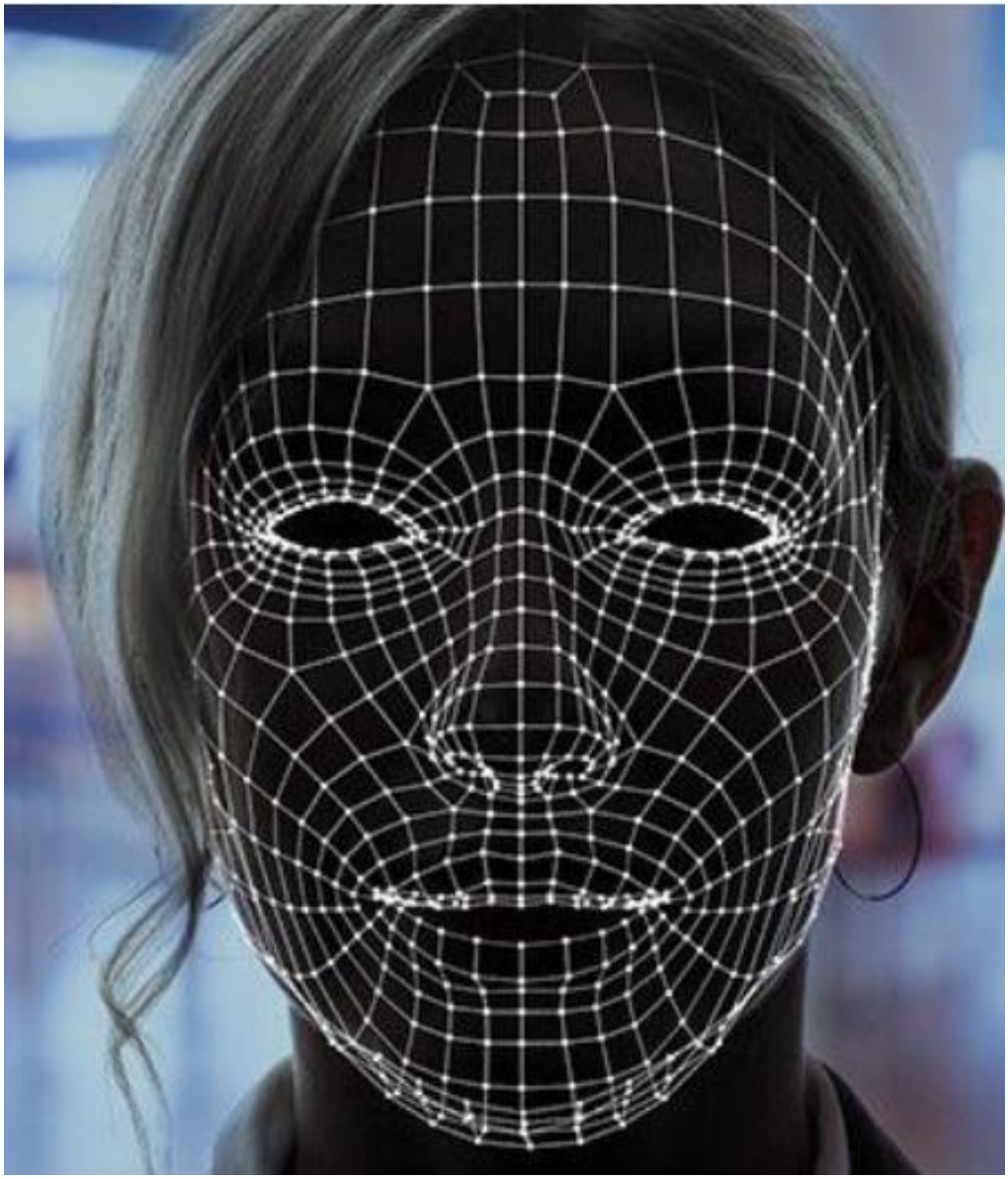

Рис.8 Система розпізнавання обличчя (вигляд сканування 3D моделі)

### 1.3.2 Переваги технології розпізнавання обличчя :

- Безконтактність – користувач не торкається сенсора, що підвищує гігієнічність і зручність;

- Висока швидкість – Розпізнавання відбувається за 0.1–1 секунду, що важливо для систем контролю доступу;

- Можливість використання у великих потоках людей. Технологія може працювати в натовпах , на відстані , без потреб в активному керуванні ;

- Підтримка штучного інтелекту . ***ISO/IEC 30137-1:2020*** описує використання відео аналітики для розпізнавання обличь у реальному часі;

- Можливість роботи з низькою якістю зображення;

- Простота інтеграції;

### 1.3.3 Недоліки технології розпізнавання обличчя :

- Сильна залежність від освітлення та умов зйомки;

- Ризик помилкового спрацювання **;**

- Можливість обману Технологію можуть атакувати: фотографією, 3D-маскою, відеороликом. Тому використовують визначення «живості».;

- Питання конфіденційності та законодавчі обмеження;

- Менша унікальність порівняно з іншими біометріями;

### 1.3.4 Стандарти технології розпізнавання обличчя :

- ***ISO/IEC 19794-5*** – цей стандарт визначає: вимоги до формату та якості зображень обличчя; правила освітлення, пози, експресії; допустимі кути повороту голови; вимоги до фото для біометричних паспортів та документів; рекомендації для систем живої зйомки (live capture).

- ***ISO/IEC 39794-5*** – вона регламентує: нові формати зображень; параметри для нейромережевих систем; вимоги для 3D-сканування обличчя; вимоги до відеопотоку для face recognition;

- ***ISO/IEC 30137*** – визначає: вимоги до відеокамер у системах розпізнавання облич; стандарти щодо якості відеопотоку; мінімальні характеристики зображень для високої точності; умови освітлення та стабільності кадру;

- ***ISO/IEC 2382-37*** **–** класифікація та визначення для всіх біометричних методів, включно з розпізнаванням облич;

- ***ISO/IEC 30107*** **-** це стандарт боротьби з підробками;

- ***ISO/IEC 24745*** **– захист біометричних даних та шаблонів.**

## 1.4 Біометричний сканер райдужної оболонки ока

Радужну оболонку ока  та сітківка ока – один з найточніших біометричних параметрів , яка використовує інфрачервоне світло для сканування складних деталей (понад 200 точок), пропонуючи **безконтактний**, гігієнічний та надзвичайно надійний метод, що практично неможливо обдурити, і він стійкий до окулярів, лінз та змін освітлення, а також може перевіряти реакцію зіниці на світло для захисту від підробок.  Через те що має складний та унікальний візерунок що зберігається протягом всього життя , дуже складно підробити ;

### 1.4.1 Принцип роботи сканера райдужної оболонки ока:

Технологія розпізнавання райдужки включає кілька послідовних етапів, які стандартизовані у міжнародних документах ***ISO/IEC 19794-6, ISO/IEC 29794-6 та ISO/IEC 30107*** (захист від атак).

- Захоплення зображення : Сканер формує висококонтрастне зображення райдужки в діапазоні **ближнього інфрачервоного світла;**

- Локалізація райдужної оболонки ;

- Нормалізація та уніфікація ;

- Створення біометричного шаблону . За допомогою фільтрів (Gabor wavelets, Log-Gabor, Haar-like features) створюється цифровий код райдужки – **IrisCode**, запропонований Джоном Даугманом (світовий стандарт);

- Порівняння;

- Прийняття рішення.


Рис. 9 Біометричний термінал контролю доступу з розпізнаванням райдужної оболонки ока

### 1.4.2 Переваги біометричного сканера райдужної оболонки ока:

- Висока точність (одна з найкращих у біометрії)**;**
- Стійкість візерунка до змін протягом життя;
- Неможливість підробки NIR-сканер оцінює: глибину структури тканини, живість ока, автоматичні рухи зіниці, мікро-судинну сітку**;**
- Гігієнічність та безконтактність;
- Працездатність у складних умовах;

### 1.4.3 Недоліки біометричного сканера райдужної оболонки:

- Висока вартість обладнання ;
- Залежність від умов освітлення;
- Вимоги до правильного позиціонування ока;
- Потенційна чутливість до офтальмологічних патологій;
- Приватність та психологічний бар’єр.

### 1.4.4 Стандарти біометричного сканера райдужної оболонки

- ***ISO/IEC 19794-6:2011*** – вимоги до формату зображення райдужної оболонки; допустимі розміри, якість, роздільна здатність зображення; параметри для 2D та 3D-захоплення; мінімальні умови освітлення; специфікації для систем контролю доступу, кордонів, відеоспостереження;

- ***ISO/IEC 29794-6:2015*** – визначає :метрики оцінки якості захопленого зображення; пороги прийнятності для використання в системах розпізнавання; оцінку фокусу, контрастності, засвічення, шумності; вимоги до камер і оптичних сенсорів;

- ***ISO/IEC 29109-6:2016 –*** це стандарт тестування на відповідність;

- ***ISO/IEC 30136:2018*** – дозволяє порівнювати різні системи за реальними умовами використання;

- ***ISO/IEC 19989-2:2021*** – оцінка стійкості до атак.

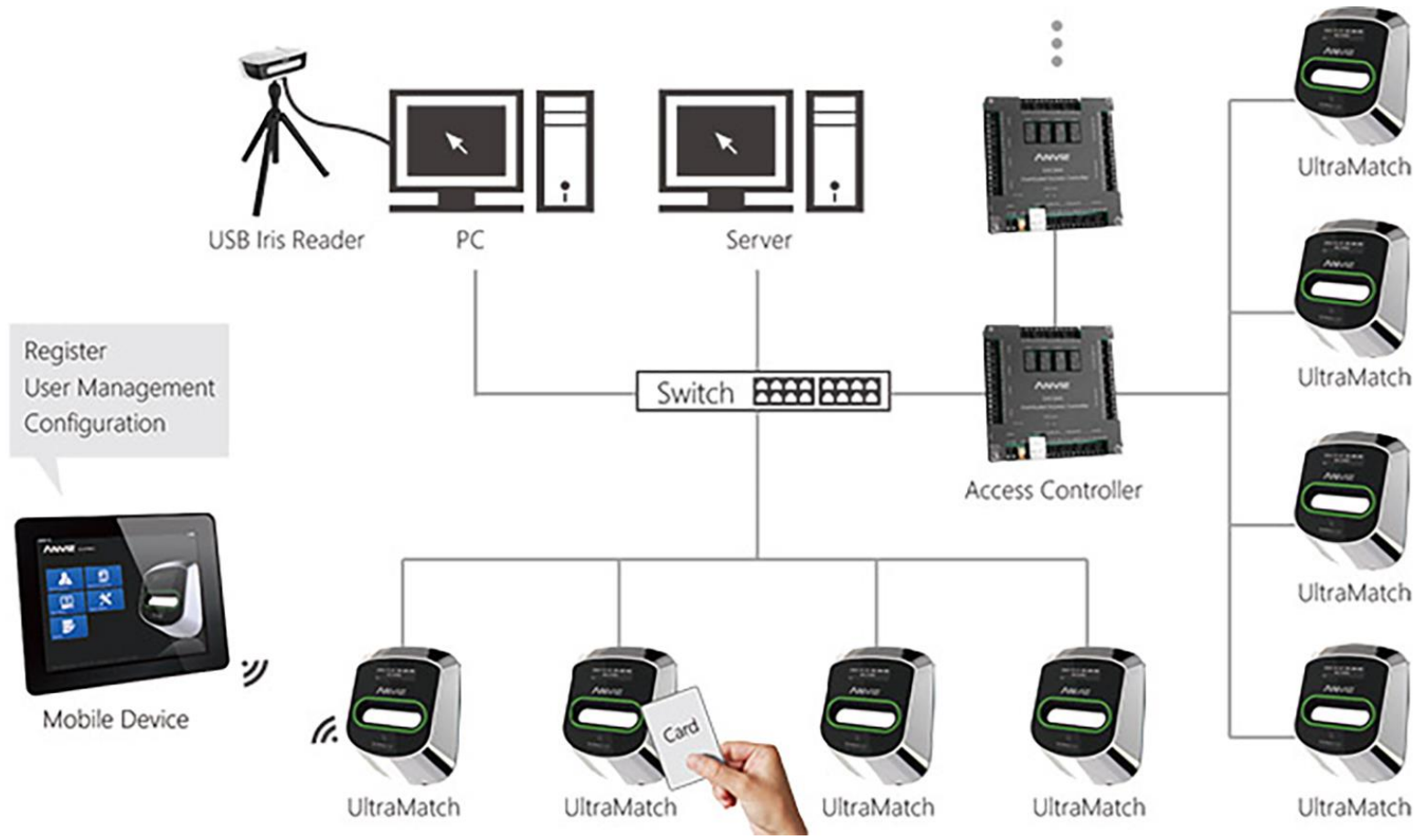


Рис. 10 схема роботи Біометричного терміналу з розпізнавання радужної оболонки ока

## 1.5 Біометрична система безпеки геометрія долоні , кисті руки

Геометрія руки є відносно стабільною ознакою, яка мало змінюється протягом життя дорослої людини (за винятком травм або значної зміни ваги). Саме тому такі системи широко застосовуються у сферах, де потрібна швидка та недорога ідентифікація великої кількості людей.

Геометрія долоні – використовуються вимірювання форми , довжини , товщини долоні та пальців , співвідношення пропорцій кисті , контури силуету руки , тривимірні характеристики поверхні .

### 1.5.1 Принцип роботи біометричної системи геометрії долоні:

- Захоплення зображення руки;
- Формування Геометричної моделі ;
- Зіставлення ;
- Прийняття рішення .

### 1.5.2 Переваги біометричної системи геометрії долоні:

- Висока швидкість роботи;
- Стійкість до забруднень, потовиділення та мікро пошкоджень;
- Висока прийнятність користувачами;
- Простота використання ;
- Низькі ризики підробки;
- Надійна робота у різних умовах;

### 1.5.3 Недоліки біометричної системи геометрії долоні:

- Низька унікальність порівняно з іншими біометричними ознаками;
- Великий розмір обладнання;
- Деградація точності при значних фізичних змінах;
- Контакт із поверхнею (у деяких моделей);
- Менш придатна для об’єктів високої секретності.

### 1.5.4 Стандарти біометричної системи геометрії долоні:

- ***ISO/IEC 19794-10:2015*** – стандарт необхідний для сумісності систем різних виробників;

- ***ISO/IEC 19785*** – загальна структура для зберігання й передачі біометричних даних;

- ***ISO/IEC 29794-1*** – описує: вимоги до якості біометричного зразка; прийнятні й неприйнятні показників; параметри оцінки надійності зображення руки;

- ***ISO/IEC 30107*** – регламентує виявлення атак шляхом підробки;

- ***ISO/IEC 19795*** – Оцінка продуктивності біометричних систем.


Рис.11 безконтактний сканер ідентифікації по венозній сітці та геометрії долоні

Рис. 12 контактний сканер ідентифікації по венозній сітці та геометрії долоні

## 1.6 Біометрична система безпеки на основі венозної сітки руки

Біометрична ідентифікація за венозним малюнком долоні або пальців одна з найнадійніших сучасних технологій контролю доступу. В її основі лежить аналіз унікального розташування підшкірних вен, які утворюють складний тривимірний візерунок. Візерунок вен є стабільним упродовж життя людини та практично не змінюється з віком, що робить його високоінформативним біометричним параметром.

### 1.6.1 Принцип роботи технології розпізнавання венозної сітки руки:

- Підсвічування руки інфрачервоним випромінюванням;
- Захоплення зображення камерою;
- Побудова біометричного шаблону;
- Порівняння зі збереженим шаблоном;
- Прийняття рішення .

### 1.6.2 Переваги біометричної системи венозної сітки:

- Висока стійкість до підробок;
- Надійність та стабільність характеристики;
- Гігієнічність;
- Висока точність;
- Придатність для людей з ушкодженнями шкіри;
- Висока швидкість роботи.

### 1.6.3 Недоліки біометричної системи венозної сітки:

- Висока вартість обладнання;
- Складність реалізації;
- Залежність від фізіологічного стану;
- Необхідність правильної позиції руки.

### 1.6.4 Стандарти технологій венозної біометрії

- ***ISO/IEC 19794-9*** Визначає формат представлення, зберігання та обміну даними венозних зображень.

- ***ISO/IEC 30107*** - Стандарти протидії підробкам . Використовується для сертифікації захисту від: штучних кінцівок, фальшивих венових моделей, підроблених матеріалів.

- ***ISO/IEC 29156*** – Надає рекомендації щодо впровадження технології у системах контролю доступу.

- ***ISO/IEC 19792*** – Оцінка безпеки біометричних систем, включаючи судинні технології.

- ***ISO/IEC 30136*** – Стандарти тестування якості біометричних алгоритмів, зокрема венозних.

## 1.7 Біометрична технологія ДНК

Біометрична ідентифікація за ДНК є одним із найнадійніших та науково обґрунтованих методів встановлення особи, оскільки генетичний код людини є унікальним (за винятком однояйцевих близнюків). Хоча ДНК-біометрія рідко використовується в системах оперативного контролю доступу через складність і тривалість аналізу, вона широко застосовується у криміналістиці, національних базах даних та деяких високо безпечних держсистемах.

### 1.7.1 Принцип роботи біометричної технології аналізу ДНК:

- Збір біологічного матеріалу;
- Виділення ДНК;
- Ампліфікація послідовностей ДНК;
- Створення генетичного профілю;

- Порівняння з базою даних;

### 1.7.2 Переваги біометричної технології аналізу ДНК:

- Абсолютна унікальність;
- Незмінність протягом життя;
- Висока точність і наукова обґрунтованість;
- Стійкість до підробок ;
- Можливість ідентифікації за мінімальною кількістю матеріалу.

### 1.7.3 Недоліки біометричної технології аналізу ДНК:

- Тривалість процедури;
- Висока вартість обладнання;
- Умовна неінвазивність ;
- Неможливість використовувати у звичайних системах доступу;

### 1.7.4 Стандарти біометричної технології аналізу ДНК

- ***ISO/IEC 19794-14:2013*** – регламентує структуру, формат та типи даних для ДНК-профілю;

- ***ISO/IEC 30107*** – система захисту від підробок, включає вимоги щодо перевірки автентичності біологічного зразка.

- ***ISO/IEC 24745:2011*** – описує принципи захисту біометричних шаблонів;

- ***ISO/IEC 22116:2007*** – описує процедури тестування ідентифікаційних систем для ДНК.

Рис.13 Прилад для виділення ДНК та його аналізу

## 1.8 Поведінкові біометричні характеристики

Поведінкові біометричні характеристики - це унікальні ознаки, що описують динаміку поведінки людини, тобто індивідуальний спосіб виконання певних дій: друкування, ходьба, підпис, мова тощо. На відміну від фізіологічних характеристик (відбитки пальців, райдужка, обличчя), поведінкові біометричні ознаки відображають психофізіологічні та моторні закономірності, які формуються протягом життя. Використовується в :

- Банківській сфері;
- Мобільних пристроях;
- Кібербезпека підприємств за допомогою ШІ або іншого ПО;
- Відеоспостереження і безпека об’єктів;
- Електронна комерція;
- Державні інституції та правоохоронні органи;
- Медичні та терапевтичні системи.

### 1.8.1 Види поведінкових біометричних характеристик:

- Динаміка підпису;
- Голос ;
- Манера ходи ;
- Біометрія клавіатурного почерку;
- Поведінковий профіль користувача;

### 1.8.2 Принцип роботи поведінкових біометричних систем

- Захоплення даних;
- Попередня обробка;
- Екстракція ознак;
- Формування біометричного шаблону ;
- Порівняння;

- Прийняття рішення.

### 1.8.3 Переваги поведінкових біометричних технологій:

- Високий рівень зручності;
- Можливість безперервної автентифікації;
- Важко підробити;
- Низькі вимоги до обладнання;
- Дешевші у впровадженні.

### 1.8.4 Недоліки поведінкових біометричних технологій:

- Нестабільність;
- Нижча точність;
- Нижча точність;
- Потреба в постійній адаптації моделей;
- Можливі атаки на моделі машинного навчання.

**Стандарти поведінкових біометричних технологій:**

- ***ISO/IEC 19795*** - вимоги до точності та безпеки;
- ***ISO/IEC 30107*** - Biometric Presentation Attack Detection;
- ***ISO/IEC 2382-37*** - біометрична термінологія;
- ***ISO/IEC 19794-13*** - формат біометричних шаблонів голосу;
- ***ISO/IEC 19794-7*** - міжнародний стандарт, що встановлює формати обміну даними динаміки підпису, які реєструються за допомогою пристроїв, таких як планшети або системи професійних пір'яних пристроїв;
- ***ISO/IEC 30108*** - включає поведінкові моделі ідентифікації.

## 1.9 Висновки

Біометричні системи доступу посідають ключове місце серед сучасних технологій автентифікації завдяки здатності ідентифікувати особу на основі унікальних фізіологічних та поведінкових характеристик. На відміну від традиційних методів, таких як паролі чи токени, біометричні дані є природно притаманними людині та практично неможливими для підроблення у звичайних умовах. Саме тому біометричні системи набули широкого поширення у сферах безпеки інформаційних систем, контролю доступу до приміщень, банківських послуг, охорони державних об'єктів, смартфонів та критичної інфраструктури. Проведений аналіз засвідчує, що біометричні технології забезпечують високий рівень точності, швидкість обробки та зручність користування, водночас зменшуючи залежність від знань та матеріальних носіїв. Розвиток технологій 3D-сканування та сенсорних систем сприяє суттєвому підвищенню ефективності розпізнавання та зниженню ймовірності помилок. Водночас, аналіз загроз свідчить, що біометричні системи не є повністю захищеними та залишаються вразливими до широкого спектра атак. Найбільш критичними є:

- атаки на канали передачі даних (перехоплення, MITM, Replay);
- атаки на базу біометричних шаблонів (підміна, викрадення, реконструкція);
- spoofing-атаки за допомогою штучних моделі обличчя, відбитків чи голосу;
- соціальна інженерія та маніпуляції персоналом;
- внутрішні інсайдерські загрози;
- уразливості сенсорів, драйверів і пропрієтарних протоколів.

Особливу небезпеку становить той факт, що біометричні дані є незмінними: якщо шаблон було викрадено або скомпрометовано, його неможливо «замінити» так само, як пароль чи ключ доступу. У зв'язку з цим захист біометричних систем повинен бути багаторівневим та охоплювати всі етапи роботи: від зчитування ознак до зберігання та прийняття рішення.

Ефективна безпека можлива лише за умови інтеграції класичних методів захисту з інноваційними технологіями, а саме: застосування криптографічних протоколів шифрування каналів, цифрових підписів, механізмів перевірки живості (liveness detection), захищених алгоритмів зберігання шаблонів (cancelable biometrics, fuzzy vault, гомоморфне шифрування), багатофакторної автентифікації та контрольованого процесу enrollment.

Важливо також враховувати людський фактор: навчання персоналу, регламентація процедур, контроль доступу до обладнання та аудит усіх операцій з шаблонами.

## 2. Мультимодальна біометрична система доступу

Мультимодальна біометрична система доступу - це комплекс безпеки, який використовує два або більше біометричних ідентифікаторів для встановлення особи. На відміну від одномодальних систем (що базуються лише на одному біометричному параметрі, наприклад відбитку пальця чи обличчі), мультимодальна система об’єднує кілька незалежних або взаємодоповнюючих ознак, що значно підвищує точність і надійність автентифікації.

У таких системах можуть поєднуватися:

- Фізіологічні ознаки: відбитки пальців, райдужна оболонка, геометрія долоні, венозна сітка руки, обличчя, ДНК.

- Поведінкові ознаки: голос, манера ходи, динаміка підпису, клавіатурний почерк, поведінкові профілі користувача.

Система інтегрує кілька алгоритмів обробки даних, створює складний профіль користувача та виконує розпізнавання на основі злиття інформації.

Де використовують мультимодальну біометричну систему :

1. Аеропорти та прикордонний контроль - обличчя + паспорт + відбитки (eGate), райдужка + обличчя.

2. Банківська безпека - голос + обличчя у мобільному банкінгу, відбиток + венозна сітка у фізичних відділеннях.

3. Військові та урядові об’єкти - відбиток + райдужка + геометрія руки , багатофакторні шлюзи.

4. Корпоративні системи доступу - обличчя + RFID ID-карта + відбиток.

5. Смартфони високого класу - Face ID + відбиток (у нових моделях).

6. Судово-криміналістичні бази даних - поєднання відбитків, ДНК та обличчя.

### 2.1Принцип роботи мультимодальної біометричної системи

Захоплення біометричних даних:

- відбитка пальця;
- зображення обличчя;
- райдужної оболонки;
- голосового зразка;
- або інших характеристик.

Попередня обробка:

- нормалізація;
- фільтрація шумів;
- підвищення контрастності;
- вирівнювання;
- сегментація зони інтересу.

Виділення ознак:

- мінуції у відбитку;
- вектори геометрії обличчя;
- текстурні патерни райдужки;
- спектральні характеристики голосу тощо.

## 2.2 Злиття біометричної інформації:

Злиття біометричної інформації може бути реалізовано кількома способами. Загальний підхід полягає в об'єднанні інформації, що надходить з різних модальностей (наприклад, відбитків пальців, обличчя, райдужної оболонки ока і т.д.). Інший тип синтезу інформації в біометрії передбачає поєднання даних, що надходять від однієї біометричної модальності, застосовуючи багато алгоритмічні методи синтезу. У сфері біометрії відбитків пальців є кілька прикладів синтезу інформації, реалізованих за допомогою декількох алгоритмів на різних стадіях процесу розпізнавання. У роботі, представленій М. Ватса (M.Vatsa) використовувалася райдужна оболонка ока як єдина модальність для реалізації мультиалгоритмічного синтезу інформаці. Незалежно від використання однієї

або декількох модальностей, методи синтезу також можуть бути класифіковані щодо їх участі в типових рівнях обробки (модулях), що слідують в режимі біометричного розпізнавання , тобто рівень датчика, рівень функції, рівень оцінки порівняння (або відповідності) та рівень прийняття рішень. Синтез інформації на рівні датчика може бути виконаний за допомогою даних, отриманих різними типами датчиків, наприклад, оптичними і конденсаторами.

Злиття може виконуватися на трьох рівнях:

- На рівні даних (Об’єднання необроблених сигналів) ;
- На рівні ознак; (Комбінація характеристик у спільний вектор ознак) ;
- На рівні рішень (Кожен модуль приймає окреме рішення);

**Зіставлення шаблонів:**

- Об’єднаний або зважений шаблон порівнюється зі зразком користувача з бази.

Прийняття рішення:

- допуск або відмова;
- рівень довіри:
- журнал події.

## 2.3 Переваги мультимодальних біометричних систем:

- Вища точність розпізнавання;
- Стійкість до підробок;
- Підвищена універсальність;
- Оптимізація для різних умов**;**
- Зменшення кількості помилок;
- Високий рівень захисту персональних даних;
- Більша стерильність та чистоти поверхонь.

## 2.4 Недоліки мультимодальних біометричних систем:

- Висока вартість;
- Складність інтеграції;
- Збільшений час автентифікації;
- Можливі проблеми з приватністю;
- Більш складна система адміністрування .

## 2.5 Стандарти мультимодальних біометричних систем :

- ***ISO/IEC 19794*** - Формати біометричних даних :
- 19794-2 - відбитки пальців;
- 19794-5 - зображення обличчя;
- 19794-6 – райдужка;
- 19794-9 - венозні зображення;
- 19794-10 - геометрія руки;
- ***ISO/IEC 30107*** - Стандарти виявлення атак: підробки, муляжі, друковані фото, штучні відбитки, DeepFake-впливи;
- ***ISO/IEC 19792*** - Оцінка безпеки біометричних систем;
- ***ISO/IEC 24745*** - Захист біометричних шаблонів;
- ***ISO/IEC 19989*** - Методи незалежного тестування біометричних систем.

## 2.6 Висновок

Мультимодальні біометричні системи доступу сьогодні посідають ключове місце серед сучасних технологій автентифікації, оскільки вони забезпечують значно вищий рівень надійності, стійкості та точності у порівнянні з традиційними одномодальними системами. Використання двох і більше біометричних ознак – таких як відбитки пальців, розпізнавання обличчя, райдужної оболонки, голосу, вен або поведінкових характеристик – дає змогу компенсувати слабкі сторони кожного окремого методу і мінімізувати ймовірність помилки чи компрометації. Завдяки комбінуванню декількох каналів верифікації мультимодальні системи демонструють підвищену стійкість до фальсифікацій, атак відтворення, шахрайських дій та спроб підробки біометричних характеристик. Вони забезпечують як більш точну ідентифікацію, так і вищий рівень відмовостійкості у випадку, коли одна з модальностей недоступна або пошкоджена. Це особливо важливо у критично важливих сферах: фінансових установах, державних структурах, медичних закладах, системах контролю кордонів і в корпоративних середовищах із підвищеними вимогами до захисту. Крім того, мультимодальні системи дозволяють гнучко налаштовувати рівень безпеки, комбінуючи різні методи автентифікації залежно від загрозового середовища та специфіки об’єкта захисту. Також вони забезпечують більшу доступність для користувачів, оскільки дозволяють вибирати альтернативний канал автентифікації у випадку фізичних чи технічних обмежень.

Водночас впровадження мультимодальних систем вимагає вирішення низки завдань: підвищення продуктивності алгоритмів обробки даних, забезпечення захищеності біометричних шаблонів, зменшення затримок під час верифікації, а також дотримання етичних і правових стандартів щодо збору та обробки персональних даних. Незважаючи на ці виклики, тенденції розвитку біометричних технологій свідчать про подальше поширення мультимодальних систем як оптимального компромісу між високою точністю, зручністю використання та надійністю.

Отже, мультимодальні біометричні системи становлять сучасний, ефективний та перспективний інструмент забезпечення доступу, який формує новий стандарт у галузі інформаційної безпеки та фізичної охорони. Їхнє використання є ключовим кроком до

підвищення загального рівня кіберзахисту та створення більш стійких і захищених інфраструктур майбутнього.

# 3. Загрози для біометричних систем доступу

У сучасному цифровому середовищі, де обсяг конфіденційних даних зростає щодня, несанкціонований доступ залишається однією з найнебезпечніших загроз для інформаційної безпеки. Це явище включає будь-яке проникнення в систему або мережу без відповідних дозволів, що може призвести до крадіжки даних, пошкодження інформації або навіть повного порушення роботи інфраструктури. На відміну від паролів або токенів, біометрію неможливо «перегенерувати». У разі витоку біометричного шаблону користувач більше не може використовувати певний біометричний метод безпечно. Саме тому формування комплексного захисту є ключовим аспектом побудови таких систем. Наприклад, систему відбитків пальців можна підробити за допомогою підробленого відбитка пальця, сформованого з відбитка пальця користувача, залишеного на поверхні, або систему розпізнавання обличчя можна обдурити за допомогою високоякісної фотографії чи 3D-моделі обличчя авторизованого користувача. Підробка відбитків пальців: Використання підроблених відбитків пальців для імітації характеристик відбитків пальців законного користувача. Зловмисники можуть скопіювати відбитки пальців жертви з поверхні, до якої вони торкалися (наприклад, дверна ручка), а потім створити штучні відбитки пальців за допомогою таких матеріалів, як желатин або силікон. Розширені системи контролю доступу можуть додати додатковий рівень захисту від біометричного спуфінгу. Впровадивши багатофакторну автентифікацію, наприклад сканування відбитків пальців і PIN-код, організації можуть зменшити ймовірність несанкціонованого доступу, навіть якщо один фактор (наприклад, відбиток пальця) підроблено. У біометричних системах автентифікації існує широкий спектр загроз, які можуть бути спрямовані як на фізичні компоненти системи, так і на її логічну архітектуру. Ці атаки класифікують залежно від етапу, на якому вони здійснюються, та характеру дій зловмисника. Основні типи атак включають: спуфінг, повторне відтворення, атаки на канали передавання та маніпуляції з біометричними шаблонами.

## 3.1 Атака типу спуфінга

Атаки спуфінгу передбачають спробу обманути систему шляхом подання штучно створеного або викраденого біометричного зразка, який імітує справжню біометричну ознаку користувача. Наприклад, для зображення обличчя це може бути фотографія, відеозапис або 3D-маска, що репрезентує обличчя зареєстрованої особи.Для поведінкових ознак, таких як клавіатурний почерк, можливим є моделювання характерних патернів натискання клавіш. Цей тип атаки загрожує безпосередньо на етапі захоплення біометричних даних, що ускладнює виявлення, особливо в разі високоякісної імітації. Тобто:

Зловмисник подає на сенсор підроблений біометричний об’єкт:

- Штучний відбиток пальця з гелю/силікону;
- Роздруковане або цифрове фото обличчя;
- 3D-маска;
- Штучний зразок райдужної оболонки;
- Підсвічені підроблені вени.

## 3.2 Атака типу відтворення

Replay-атаки полягають у повторному поданні раніше перехопленого біометричного зразка, з метою аутентифікації в системі без фактичної участі користувача. Такі атаки можуть реалізовуватися шляхом надсилання цифрових копій зображення обличчя або послідовностей таймінгів клавіатурного почерку через неавтентичний інтерфейс введення . Попри простоту реалізації, replay-атаки часто є ефективними проти систем, які не мають механізмів перевірки живості (livenessdetection) або часової узгодженості даних, тобто : замість реального зображення на сенсор подається запис біометрії, наприклад:

- Відео очей під час аналізу живості;
- Аудіозапис голосу замість живого спікера;
- Біометричний сигнал передається у відкритому вигляді;
- Сигнали передаються через уразливу мережу, де зловмисник може виконати MITM

Наслідки успішної атаки типу відтворення :

- Несанкціонований доступ до приміщень або систем, потенційно з високим рівнем секретності;

- Компрометація всіх облікових записів, дані яких потрапили до зловмисника;

- Можливість побудови складніших атак, зокрема MITM, Session Hijacking та підроблення біометричних шаблонів;

- Незворотні втрати безпеки, адже біометричні дані не можна "змінити" як пароль;

### 3.3 Атака на шаблони біометричних ознак та внутрішню структуру системи

Шаблони біометричних ознак, збережені в базі даних системи (наприклад, вектори ознак з обличчя або клавіатурного почерку), можуть стати об’єктом несанкціонованого доступу, модифікації або підміни. Зловмисник, отримавши шаблон, може відтворити біометричні характеристики користувача або створити новий шаблон, що дозволяє проходити аутентифікацію .Оскільки біометричні шаблони не можуть бути "перегенеровані" на відміну від паролів, компрометація таких даних несе довготривалі наслідки. Для захисту шаблонів застосовуються методи біометричного хешування, криптографічного обгортання та шифрування зі збереженням властивості зіставлення. Ці атаки є складнішими та спрямовані на обхід захисту у програмній або мережевій частині.

### 3.4 Атаки на базу біометричних шаблонів

База біометричних шаблонів є критичним компонентом будь-якої біометричної системи доступу. Саме тут зберігаються математичні представлення біометричних ознак (відбитки пальців, геометрія обличчя, райдужка тощо), які використовуються під час процесів автентифікації. Компрометація цієї бази створює серйозні загрози, оскільки біометричні дані є незмінними, на відміну від паролів або токенів.

- Атаки на канали передавання біометричних шаблонів;

- Атаки ін’єкції шаблонів;

- Атаки на структуру бази даних;

- Маніпуляції з метаданими;

- Атаки відновлення - це математичні атаки, що дозволяють реконструювати приблизний біометричний образ на основі векторів ознак.

- Викрадення шаблонів;

- Підмінити шаблон іншим (template injection);

- Відновити вихідний біометричний образ із шаблону (attack inversion).

- Hill-Climbing Algorithm - Зловмисник використовує багаторазові спроби автентифікації та отриманий зворотний зв'язок системи для побудови шаблону, який все ближче наближається до справжнього, поки система не прийме його як валідний.

- Атаки внутрішніх зловмисників;

- Атаки підбору та кореляції шаблонів;

- Атаки через вразливі механізми зберігання;

- Компрометація локального сховища сенсора;

- Ненадійне шифрування або ключі.

## 3.5 Атаки на канали передачі даних

Канал передачі даних у біометричній системі виконує роль сполучної ланки між сенсором (зчитувачем) та центральним модулем, який проводить обробку та порівняння біометричних характеристик. Через високу критичність передаваних даних (сирі біометричні зразки, шаблони, службова інформація автентифікації) цей компонент часто стає основною ціллю атак.

Атаки на канали передачі даних спрямовані на перехоплення, модифікацію, підміну або повторне відтворення інформації, яка циркулює між елементами системи. Вони можуть бути непомітними для системи та користувача, що робить їх особливо небезпечними.

-Перехоплення та модифікація даних між сенсором та сервером;

- MITM (Man-In-The-Middle) атаки;

- Підміна пакету зображення.

**Наслідки:**

- створення точних підробок (спуфінг);

- використання перехоплених пакетів для Replay Attack;

- подальший аналіз протоколу з метою пошуку вразливостей.

### 3.6 Атаки на алгоритми машинного навчання

Фальшивими або штучними атаками називають випадки навмисного пошкодження своїх біометричних даних людиною . Серед наступних проблем із безпекою біометричних документів зазначають відсутність належних методів авторизації на кордоні, та внаслідок цього у світі відбувається зростання кількості злочинців та нелегальних мігрантів на кордоні . З огляду на стрімкий та постійний розвиток біометричних технологій, виникають нові виклики, які спричиняють поширення негативних явищ серед країн.

- **adversarial attacks** (внесення мінімальних змін у зображення обличчя, щоб система не впізнала людину або визнала іншою);

- **poisoning attacks** (завдання шкоди тренувальним даним);

- **model extraction** (викрадення моделі нейромережі через багаторазовий доступ).

- AI-клонування голосу

### 3.7 Соціальна інженерія

- Примушення користувача прикласти палець/подивитися в камеру;

- Фішингові сценарії для отримання зображення обличчя або голосу - користувача обманом змушують надати свої біометричні дані через несправжні інтерфейси чи пристрої;

- Авторитет та помилкове почуття довіри тобто зловмисник може представитися керівником або інженером та домогтися того, щоб користувач сам "підставив палець" або "подивився у камеру".

- Пряме переконання або виманювання доступу - зловмисник може удавати службову особу (адміністратора ІБ, інженера техпідтримки, охоронця), вимагаючи користувача пройти сканування у певному місці або надати можливість використати його біометричні дані;

- Спостереження за процесом автентифікації , тобто зловмисник спостерігає, як користувач проходить біометричну ідентифікацію, і фіксує її прихованою камерою.

- Використання сторонніх технічних пристроїв , для отримання 3Д скану лиця , deepfake-відео, моделей голосу;

- Маніпуляції персоналом, який обслуговує систему з метою отримання доступу ;

- Інсайдерські атаки - співробітник, який має доступ до сенсорів або серверів, може бути підкуплений чи введений в оману

- Підроблений процес реєстрації - користувачу можуть запропонувати «оновити біометрію», що дозволить злочинцю записати її у власний пристрій чи базу.

### 3.8 Стандарти що регулюють захист біометричних систем від атак :

- ***ISO/IEC 30107-1/2/3*** - методи живості (Liveness Detection), вимоги до тестування стійкості.

- ***ISO/IEC 2474***5 - безпечне управління біометричними шаблонами;

- ***ISO/IEC 19792*** = оцінка безпеки біометричних систем;

- ***ISO/IEC 19989-1:2023*** - Інформаційна безпека. Критерії та методологія оцінювання безпеки біометричних систем;

- ***ISO/IEC 19792*** - Оцінка безпеки біометричних систем;

- ***ISO/IEC 30107*** - Стандарти захисту від атак Presentation Attack Detection (PAD)

- ***ISO/IEC 30107-1:2016*** - терміни та моделі атак;

- ***ISO/IEC 30107-2:2017*** - вимоги до систем захисту від атак презентації;

- ***ISO/IEC 30107-3:2017*** - методи тестування PAD-систем.

- ***ISO/IEC 19794*** = Формати біометричних шаблонів;

- ***ISO/IEC 19794-2*** (відбитки пальців),

- ***ISO/IEC 19794-4*** (обличчя),

- ***ISO/IEC 19794-5*** (райдужна оболонка),

- ***ISO/IEC 19794-9*** (динаміка підпису).

## 3.9 Методи захисту від атак у біометричних системах

- Захист на рівні сенсора(перевірка живості) , тобто аналіз текстури шкіри; мікрорухи очей, рефлекс зіниці, 3D-аналіз (глибина, форма). спектральний аналіз (NIR, UV); тепловий профіль.

- Захист біометричних шаблонів - шаблон перетворюється математично, і його неможливо відновити до вихідного образу. key-binding (біометрія прив’язується до криптографічного ключа) або key-generation (з біометрії генерується ключ).

- Гомоморфне шифрування , дозволяє проводити порівняння біометричних ознак у зашифрованому вигляді.

- Захист каналів передачі даних : шифрування TLS 1.3 , цифровий підпис шаблонів.

- Захист алгоритмів машинного навчання - навчання на стійких прикладах, згладження атак, виявлення підроблених даних, захист моделей нейромереж від несанкціонованого доступу.

- Організаційні методи захисту - політика обмеження доступу до біометричних даних; сегментація мережевої інфраструктури; контроль журналів подій; періодичний аудит та тести на «пенетрацію».

## 3.10 Висновок

Біометричні системи доступу стали ключовим елементом сучасної інфраструктури безпеки, оскільки вони забезпечують високий рівень точності, зручності та унікальності автентифікації. Однак разом із широким застосуванням біометрії зростає й кількість загроз, спрямованих на підрив їхньої конфіденційності, цілісності та доступності. Це актуалізує необхідність глибокого розуміння векторів атак і впровадження комплексних механізмів захисту.

Аналіз показує, що біометричні системи піддаються різноманітним видам атак на всіх етапах функціонування: під час збирання біометричних даних, їх передачі, обробки, зберігання та порівняння. Найнебезпечнішими є атаки на сенсори (спуфінг та атаки презентації), маніпуляції каналами передачі інформації, компрометація біометричних шаблонів у базі даних, атакування модулів прийняття рішень, а також шкідливий вплив соціальної інженерії. Особливої уваги заслуговують атаки відтворення, що використовують підроблені фізичні або цифрові біометричні характеристики, оскільки вони дають змогу зловмиснику імітувати користувача без фактичного доступу до його реальних даних.

Сучасні системи захисту пропонують комплексний підхід до протидії таким загрозам. Ключовими механізмами є:

– застосування алгоритмів виявлення живості (Liveness Detection), які дозволяють розрізняти реальну біометрію та підроблені зображення, маски, штучні відбитки чи інші форми спуфінгу;

– криптографічні методи захисту біометричних шаблонів, включаючи хешування, їх біометричну скасованість (cancelable biometrics) і протоколи захищеного порівняння без розкриття даних;

– шифрування каналів передавання даних, що запобігає атакам «людина посередині» та підробці інформаційних потоків;

– багатофакторна та мультимодальна біометрія, що значно знижує ймовірність обходу системи;

– використання стандартів ISO/IEC для оцінки загроз і забезпечення належного тестування стійкості до атак.

Попри наявність розвинених інструментів захисту, повністю усунути ризики практично неможливо. Біометричні дані, на відміну від паролів, не можна змінити у разі їх викрадення, що робить захист шаблонів критично важливим. Крім того, зловмисники постійно вдосконалюють методи атак, зокрема шляхом використання штучного інтелекту для генерації фотореалістичних підробок, що створює нові виклики у сфері безпеки.

Таким чином, забезпечення стійкості біометричних систем доступу потребує системного, багаторівневого підходу, який поєднує технічні, організаційні та криптографічні механізми захисту. Ефективність таких систем прямо залежить від якісної реалізації засобів протидії атакам, постійного оновлення алгоритмів, впровадження міжнародних стандартів і циклічного тестування на проникнення. У міру розвитку технологій біометричні системи залишатимуться одним із ключових інструментів забезпечення безпеки, однак тільки ті рішення, що базуються на комплексному захисті, зможуть відповідати сучасним та майбутнім кіберзагрозам.

### 3.1.2 Штучний інтелект в біометричних системах доступу

Штучний інтелект (ШІ) став фундаментальним компонентом сучасних біометричних систем контролю доступу, трансформуючи як процеси розпізнавання, так і механізми захисту персональних даних. Інтелектуальні моделі машинного навчання дають змогу підвищити точність, надійність та адаптивність біометричних технологій порівняно з традиційними алгоритмічними підходами. Використання ШІ дозволяє не тільки оптимізувати обробку біометричних ознак, але й забезпечити проактивний захист від атак, сталий контроль якості та підвищений рівень ідентифікації. технологія IoT (Internet of Things) передбачає об'єднання фізичних пристроїв: сенсорів, контролерів, виконавчих механізмів в єдину мережу, здатну до автоматичного збору, передачі та обробки даних. Інтернет речей дає змогу розширити функціональні можливості цифрових систем, дозволяючи їм працювати у фізичному світі: реагувати на події, змінювати середовище, вести облік тощо. Поєднання біометричної ідентифікації з інфраструктурою IoT створює передумови для формування нових типів «розумних» систем. Наприклад, двері, які автоматично відкриваються лише при розпізнаванні авторизованого обличчя, або система відвідування, що фіксує присутність працівників без потреби у паперовому обліку чи використанні RFID-карт. Слід зазначити, що поняття «смарт-система біометричної ідентифікації» не обмежується лише апаратною частиною. Вона включає програмні алгоритми машинного навчання, мережеві протоколи, системи управління базами даних, елементи інтерфейсу користувача та засоби кібербезпеки. Таким чином, вона перетворюється на багаторівневу інформаційно-технічну систему, здатну до адаптування, масштабування та інтеграції у різні цифрові платформи. Варто наголосити, що біометрична ідентифікація та IoT-технології – це не окремі напрямки, а взаємопов'язані складові одного цілого, це не лише покращує якіс 1.4 Методи та алгоритми біометричної ідентифікації на IoTплатформах Використання алгоритмічних методів у біометричних системах, що функціонують у межах IoT-інфраструктури, передбачає поєднання двох принципово різних вимог: високої точності розпізнавання та обмеженості ресурсів. Цей баланс вимагає адаптації або навіть спрощення традиційних алгоритмів комп'ютерного зору, не жертвуючи при цьому базовими показниками надійності. Розуміння, які саме методи доцільні в умовах IoT, потребує критичного переосмислення класичних підходів

до біометрії. На сьогодні більшість рішень, що працюють з розпізнаванням облич, ґрунтуються на багатоступеневому процесі, який включає: виявлення обличчя у зображенні, вилучення унікальних ознак, побудову векторного представлення (ембедінгу) та порівняння з існуючими шаблонами у базі. У кожному з цих кроків можливе застосування різних алгоритмів, вибір яких значною мірою залежить від обчислювальних можливостей пристрою. Умовно, всі методи можна поділити на традиційні, на основі ознак, та сучасні, на основі глибинного навчання.ть цифрової взаємодії, а й дозволяє побудову безпечних, автономних і зручних середовищ у сфері освіти, охорони здоров’я, промисловості та міського управління. У певних сценаріях, зокрема в біометричному контролі доступу, доречним є застосування комбінованих моделей, наприклад, об'єднання детектора обличчя  на основі HOG з класифікатором, що працює на CNN. Це дозволяє досягти прийнятного компромісу між продуктивністю і точністю. Сучасні фреймворки, як-от TensorFlow Lite, OpenVINO чи MediaPipe, дають змогу запускати такі моделі навіть на пристроях із мінімальними ресурсами (Raspberry Pi, Jetson Nano).

**Випадки** використання :

Залучення клієнтів : Зацікавлені сторони можуть використовувати механізми зворотного зв'язку для підвищення задоволеності та лояльності клієнтів. Наприклад, компанії можуть впроваджувати опитування для збору інформації про вподобання клієнтів, яку Rapid Innovation може аналізувати за допомогою інструментів на базі штучного інтелекту, щоб отримати практичну інформацію. Це відповідає стратегії залучення зацікавлених сторін та плану комунікації із зацікавленими сторонами.

Розробка продукту : Залучення зацікавлених сторін до процесу розробки продукту може призвести до інновацій, які відповідають потребам ринку. Наприклад, технологічні компанії часто залучають користувачів до бета-тестування для вдосконалення своїх продуктів. Швидкі інновації можуть сприяти цьому процесу, використовуючи алгоритми штучного інтелекту для аналізу відгуків користувачів та покращення функцій продукту, що є частиною плану залучення зацікавлених сторін.

Дотримання нормативних вимог : Зацікавлені сторони, такі як регуляторні органи, забезпечують відповідність проектів правовим стандартам. Це особливо важливо в таких галузях, як охорона здоров'я та фінанси, де дотримання вимог є критично важливим. Швидкі інновації можуть допомогти клієнтам впоратися з цими складнощами,

впроваджуючи блокчейн-рішення, що підвищують прозорість та відстежуваність, як зазначено в плані управління зацікавленими сторонами.

Алгоритми комп'ютерного зору визначають:

-розташування обличчя на зображенні;

- межі райдужної оболонки;

- контури руки чи пальця;

--структуру вен;

- артикуляцію при голосовій біометрії.

Виділення та нормалізація ознак:

ШІ-моделі автоматично обирають такі найбільш інформативні характеристики глибинні ознаки обличчя (deep facial embeddings), унікальні патерни частотних спектрів голосу, неявні мікроскопічні структури райдужки ,топологічні особливості вен (vascular network embeddings), поведінкові патерни клавіатурного ритму чи рухів миші. Завдяки цьому значно зростає точність розпізнавання та стійкість до шуму.

Класифікація та зіставлення ШІ моделі, зокрема:

**-CNN**,

**- Siamese Networks**,

**- RNN**,

**- Transformer-архітектури**,

Здійснюють ідентифікацію та верифікацію біометричного зразка. У порівнянні з класичними методами (наприклад, алгоритмами геометричних ознак), ШІ-системи демонструють вищий рівень точності та меншу чутливість до відхилень.

Виявлення атак ШІ дозволяє ідентифікувати спроби підробок:

- маски обличчя;

- фотографії;

- відео атаки (deepfake attacks);

- штучні пальці;

- друковані чи 3D-моделі кисті руки;

- аудіосинтез голосу.

Методи глибокого аналізу текстур, динамічних характеристик та мікродеталей дають змогу розпізнати навіть високоякісні підробки.

### 3.1.3 Адаптивне навчання (Adaptive Learning) ШІ дозволяє:

Важливим методом підвищення ефективності, надійності та зручності біометричних систем доступу в умовах мінливого середовища проти загроз, що розвиваються, є адаптивне навчання штучного інтелекту. Ідея адаптивного навчання полягає в тому, що алгоритми здатні автоматично реорганізовувати свої параметри у відповідь на нову інформацію, при цьому система залишається безпечною та цілісною.

Системи на основі адаптивного навчання дозволяють покращити якість біометричного розпізнавання в довгостроковій перспективі. Біометричні характеристики людини можуть змінюватися залежно від віку, фізичної підготовки, погодних умов або через проблеми зі скануванням. Ці зміни можуть бути вивчені за допомогою адаптивних моделей, які оновлюють свої біометричні шаблони та зменшують ймовірність відмови особі в доступі до системи (коефіцієнт помилкових відхилень) при відносно постійній ймовірності дозволу особі отримати доступ (коефіцієнт помилкових прийнять).

Використання адаптивного навчання робить систему набагато стійкішою до атак. Воно дозволяє алгоритмам розпізнавати дивні моделі поведінки, незрозумілі біометричні зразки або підозрілі входи. На основі цього система може автоматично змінювати свою чутливість, запитувати додаткову перевірку або перемикатися в режим підвищеної безпеки. Це особливо корисно проти атак повторного відтворення, спуфінгу та біометричних підробок, згенерованих штучним інтелектом.

По-третє, адаптивне навчання дозволяє покращити використання інших біометричних систем. Інтелектуальні алгоритми можуть змінювати значення кожного біометричного елемента залежно від того, наскільки він хороший та надійний у певний час. Наприклад, коли освітлення тьмяне, система може зменшити розпізнавання обличчя та посилити використання відбитків пальців або голосу. Це робить систему надійнішою та продовжує забезпечувати доступ.

Використання адаптивних програм навчання мінімізує помилки, пов'язані з людиною, а також допомагає системам працювати незалежно. Системи самонавчання

зменшують потребу в людському втручанні під час зміни параметрів та оновлення моделей, а також участі адміністратора. Це особливо корисно у великих системах з високим рівнем доступу, тисячами користувачів та мінливим трафіком. Отже, адаптивне навчання ШІ дозволяє біометричним системам доступу бути більш точними, гнучкими та стійкими до сучасних і перспективних загроз. За умови коректної реалізації та інтеграції з механізмами захисту, цей підхід формує основу для створення інтелектуальних, саморегульованих і надійних систем доступу нового покоління.

Тобто :

- підлаштовувати систему під зміни зовнішності користувача;
- оновлювати шаблони без повторної реєстрації;
- коригувати поведінкові біометричні моделі;
-знижувати рівень помилок FAR/FRR.

**Переваги використання штучного інтелекту в біометричних системах доступу**

.

Інтеграція штучного інтелекту в біометричні системи доступу стала одним із визначальних факторів їх розвитку . Алгоритми машинного навчання та глибоких нейронних мереж дозволили суттєво підвищити точність ідентифікації, стійкість до атак та адаптивність систем у складних і динамічних умовах експлуатації. На відміну від класичних алгоритмів , ШІ-засоби здатні аналізувати великі обсяги даних, виявляти приховані закономірності та самостійно оптимізувати процес автентифікації. Штучний інтелект значно підвищує ефективність виявлення спуфінг-атак та атак презентації. Алгоритми ШІ аналізують мікротекстури шкіри, природні рухи, поведінкові патерни, теплові характеристики або тимчасові зміни сигналу, які складно відтворити за допомогою фотографій, відео, масок чи штучних відбитків. Завдяки цьому системи з ШІ здатні ефективно відрізняти «живу» біометрію від синтетичної або відтвореної, навіть у випадку використання високоякісних підробок. Біометричні ознаки людини з часом змінюються під впливом віку, стану здоров’я, фізичних навантажень або зовнішніх факторів. Алгоритми адаптивного навчання дозволяють системі поступово оновлювати біометричні моделі без необхідності повторної реєстрації користувача.
Це забезпечує стабільну роботу системи у довгостроковій перспективі та зменшує

кількість помилкових відмов у доступі. ШІ відіграє ключову роль у мультимодальних біометричних системах, де використовується кілька різних ознак. Інтелектуальні алгоритми здатні динамічно визначати вагу кожної модальності залежно від її якості та контексту використання. Наприклад, за поганого освітлення система може знищити значущість розпізнавання обличчя та підвищити роль голосової або дактилоскопічної біометрії, що суттєво підвищує загальну надійність автентифікації. Штучний інтелект легко інтегрується з іншими засобами захисту: системами відеоспостереження, SIEM, контролю доступу, кібербезпеки та управління ризиками. Це дозволяє створювати комплексні інтелектуальні системи безпеки з централізованим аналізом подій та реагуванням на загрози в реальному часі. Штучний інтелект дозволяє аналізувати не лише статичні біометричні характеристики, поведінкові патерни користувача: темп мовлення, динаміку підпису, ритм натискання клавіш, частоту та послідовність спроб входу. На основі цього система може виявляти аномалії або підозрілі дії, які свідчать про можливу атаку, і автоматично активувати додаткові механізми захисту. Алгоритми ШІ добре масштабуються та ефективно працюють у системах із великою кількістю користувачів. Використання оптимізованих нейронних мереж і апаратного прискорення (GPU, CPU) дозволяє обробляти біометричні дані в реальному часі без суттєвих затримок. Це робить ШІ-рішення придатними для великих підприємств, транспортних вузлів, банківських систем і державних сервісів. Автоматизація процесів аналізу та прийняття рішень зменшує залежність системи від суб’єктивних рішень операторів або адміністраторів. ШІ здатний забезпечити стабільну якість автентифікації та однаковий рівень безпеки незалежно від умов експлуатації та навантаження.

Недоліки та ризики використання ШІ в біометричних системах

Незважаючи на суттєві переваги, інтеграція штучного інтелекту в біометричні системи супроводжується низкою технічних, безпекових, етичних та організаційних ризиків. Складність моделей машинного навчання, залежність від якості даних та висока вартість впровадження створюють нові вектори загроз, які необхідно враховувати час проєктування та експлуатації таких систем. Алгоритми машинного навчання самі по собі можуть бути об’єктом атак. Зловмисники здатні здійснювати:

- таки отруєння даних - навмисне внесення спотворених або шкідливих біометричних зразків у навчальні або адаптивні набори даних;

**- Adversarial-атаки** - створення спеціально модифікованих біометричних зразків, які для людини виглядають коректними, але призводять до помилкових рішень моделі;

**- model inversion та model extraction** - відновлення біометричних характеристик або логіки роботи моделі через багаторазові запити.

Ефективність ШІ безпосередньо залежить від якості навчальних даних , потрібно повні данні, незастарілими, та презентабельними модель демонструватиме знижену точність та нестабільну поведінку. У біометричних системах це може призводити до підвищення кількості помилкових відмов або допусків для окремих груп користувачів. Одним із найсерйозніших соціальних ризиків є наявність упередженості в алгоритмах ШІ. Якщо навчальні вибірки не охоплюють достатньо різноманітних біометричних характеристик, система скоріше за все може працювати з різною точністю для різних демографічних груп. ШІ-моделі, особливо глибокі нейронні мережі, потребують значних обчислювальних ресурсів для навчання та виконання. Це ускладнює їх використання в: вбудованих системах, мобільних пристроях, розподілених системах доступу з обмеженим апаратним забезпеченням. Високі апаратні вимоги також підвищують вартість впровадження та експлуатації.


Рис.14 біометричний термінал з ШІ

## 3.12 Вдосконалення біометричної системи контролю доступу розпізнавання обличчя

Сучасні біометричні системи контролю доступу, зокрема системи на основі розпізнавання обличчя, широко застосовуються у корпоративних, банківських, державних та критично важливих інформаційних інфраструктура. Вони забезпечують зручну та швидку ідентифікацію користувачів без необхідності використання фізичних носіїв або запам’ятовування паролів. Водночас одномодальні біометричні системи мають достатньо багато суттєвих недоліків, серед яких уразливість до атак підміни біометричних ознак, зниження точності за неправильних умов зйомки, обмежена адаптивність до зміни зовнішнього вигляду користувачів та підвищені ризики компрометації персональних даних. Це обумовлює необхідність їх подальшого покращення з урахуванням сучасних потреб інформаційної безпеки.

Загальна ідея вдосконалення полягає у переході від традиційної одномодальної системи біометричного доступу до інтелектуальної адаптивної системи, що поєднує методи штучного інтелекту, елементи мультимодальної біометрії та сучасні механізми захисту персональних даних. Основна задумка робиться не лише на підвищенні точності ідентифікації, а й на забезпеченні стійкості системи до сучасних атак, таких як : атака першого дня (spoofing), deepfake-загроз та атак на біометричні шаблони. Запропоноване вдосконалення передбачає інтеграцію інтелектуальних алгоритмів аналізу живості об’єкта , які дозволяють відрізняти реальну присутність користувача від використання підроблених зображень, відеозаписів або тривимірних масок. На відміну від класичних методів, ці алгоритми базуються на аналізі мікро динамічних характеристик, зокрема мікроміміків , рухів очей, реакції зіниць на зміну освітлення та просторової структури обличчя. Застосування таких методів значно підвищує рівень захисту системи від нелегального доступу.

Додатковим елементом вдосконалення є використання поведінкових біометричних характеристик як допоміжного фактора автентифікації. Аналіз характерних рухів голови, часових затримок реакції та індивідуальних моделей поведінки дозволяє сформувати більш повний біометричний профіль користувача. Такий підхід підвищує надійність системи без суттєвого зниження зручності використання та дозволяє реалізувати гнучку

адаптацію рівня безпеки залежно від контексту доступу. Важливим аспектом загальної ідеї вдосконалення є забезпечення захисту біометричних шаблонів на всіх етапах їх життєвого циклу. Для цього пропонується застосування методів перетворюваної біометрії (cancelable biometrics) та локальної обробки даних без передачі біометричної інформації у зовнішні хмарні сервіси. Такий підхід знижує ризик витоку персональних даних та забезпечує відповідність міжнародним стандартам інформаційної безпеки та вимогам захисту персональних даних.

Локальна обробка біометричних даних із застосуванням технологій Edge AI є одним із ключових напрямів вдосконалення. . Вона передбачає виконання основних обчислень безпосередньо на кінцевому пристрої, що зменшує потребу у передачі даних до центрального серверу чи хмарної платформи. Такий підхід суттєво підвищує безпеку персональних даних, прискорює обробку біометричних сигналів та забезпечує низьку затримку у процесі автентифікації. Локальна обробка передбачає інтеграцію на пристрої потужних обчислювальних модулів, на графічному процесорі або Tensor Processing Unit (інтегральна схема специфічного застосування), які здатні обробляти алгоритми глибинного навчання та нейронні мережі в реальному часі. Завдяки цьому на Edge-пристрої можна виконувати всі основні операції біометричної системи: детекцію та сегментацію об’єкта, виділення ознак, формування біометричного шаблону, аналіз живості та поведінкових параметрів користувача. Таким чином, передача чутливих біометричних даних у мережу або хмару зводиться до мінімуму, що значно знижує ризик їх перехоплення або компрометації. Особливо ефективною локальна обробка стає у випадках мультимодальної біометрії, де одночасно аналізуються фізіологічні та поведінкові характеристики користувача. Edge AI дозволяє об’єднати дані з камер, сенсорів глибини, інфрачервоних датчиків та пристроїв для зчитування поведінкових патернів у єдину систему обробки. Це забезпечує високоточне та швидке прийняття рішень щодо автентифікації без необхідності передачі великих обсягів даних у центральну систему. Крім підвищення безпеки, локальна обробка дозволяє значно зменшити час автентифікації, що є критично важливим у сценаріях з високою пропускною здатністю користувачів, таких як офісні та промислові комплекси, аеропорти та інші об’єкти з інтенсивним потоком людей. Edge AI забезпечує мінімальну затримку у прийнятті рішень, що підвищує зручність користувачів та ефективність контролю доступу.

Отже, загальна ідея вдосконалення біометричної системи контролю доступу на основі розпізнавання облич полягає у створенні комплексного покращення моделі , яке поєднує високоточну біометричну ідентифікацію, адаптивні механізми аналізу ризиків і сучасні методи захисту даних. Ключову роль у процесі ідентифікації відіграє **модуль виділення глибинних ознак**, який формує компактний та унікальний біометричний шаблон користувача. Для цього застосовуються сіамські нейронні мережі або глибинні ембединг-моделі, які навчаються мінімізувати відстань між зразками одного користувача та максимізувати її між різними особами. Такий підхід забезпечує високу точність зіставлення та зменшує ймовірність помилкових рішень навіть у разі часткових змін зовнішності користувача.

Для підвищення надійності системи програмний рівень також включає модуль поведінкової біометрії, який аналізує динамічність характеристики взаємодії користувача з системою. До таких характеристик належать характерні рухи голови, затримки реакцій , рухи очей , рухи губ та індивідуальні патерни поведінки. Інтеграція цього модуля дозволяє сформувати більш розширений біометричний профіль та значно ускладнює реалізацію складних атак, зокрема із застосуванням Deep Fake відео або імітації зовнішності.

Завершальним елементом програмного рівня є інтелектуальний модуль прийняття рішень, який об’єднує результати роботи всіх AI-модулів та формує фінальне рішення щодо надавання або відмови у доступі. Цей модуль реалізує адаптивну логіку, що враховує рівень довіри до кожного біометричного параметра, історію попередніх спроб автентифікації. Такий підхід дозволяє гнучко змінювати рівень безпеки системи залежно від поточної загрози та умов експлуатації.

### 3.1.4 Висновок по використання штучного інтелекту в біометричних системах

Використання штучного інтелекту в біометричних системах контролю доступу є одним із найважливіших напрямів розвитку сучасних технологій безпеки. Поєднання біометрії з алгоритмами машинного навчання та глибоких нейронних мереж дозволило перейти від класичних, статичних методів автентифікації до інтелектуальних, адаптивних систем, здатних ефективно працювати в умовах змінного середовища та зростаючих кіберзагроз. Проведений аналіз свідчить, що застосування ШІ суттєво підвищує

функціональні можливості біометричних систем, водночас створюючи нові виклики та ризики, які потребують системного підходу до управління безпекою.

До основних переваг використання штучного інтелекту належить значне підвищення точності та надійності ідентифікації користувачів. Алгоритми глибокого навчання здатні формувати складні багатовимірні представлення біометричних ознак, що забезпечує стійкість до шумів, спотворень і змін умов зчитування. Це дозволяє зменшити кількість помилкових допусків і відмов, що є критично важливим для систем контролю доступу з високими вимогами до безпеки. Крім того, ШІ значно підвищує ефективність виявлення атак презентації та спуфінгу, аналізуючи мікродинамічні та поведінкові характеристики, які практично неможливо точно відтворити за допомогою підроблених зразків.

Важливою перевагою є адаптивність біометричних систем на основі ШІ. Завдяки механізмам адаптивного навчання системи можуть враховувати поступові зміни біометричних характеристик користувачів, пов’язані з віком, фізичним станом або зовнішніми факторами. Це забезпечує довготривалу стабільність роботи системи без необхідності частого повторного запису біометричних шаблонів. У мультимодальних системах ШІ дозволяє динамічно керувати вагами різних біометричних ознак, підвищуючи надійність автентифікації навіть у несприятливих умовах.

Окремо слід відзначити здатність інтелектуальних систем до виявлення аномальної поведінки та потенційних загроз у режимі реального часу. Аналіз шаблонів доступу, частоти спроб автентифікації та поведінкових характеристик користувачів дозволяє системам контролю доступу своєчасно реагувати на підозрілі дії, активувати додаткові рівні перевірки або тимчасово обмежувати доступ. Таким чином, біометричні системи з елементами ШІ поступово трансформуються з інструментів ідентифікації в комплексні інтелектуальні платформи безпеки.

Водночас результати аналізу демонструють, що використання штучного інтелекту в біометричних системах пов’язане з низкою суттєвих недоліків і ризиків. Однією з ключових проблем є вразливість моделей машинного навчання до спеціалізованих атак, зокрема отруєння даних, adversarial-атак та спроб відновлення біометричних характеристик через аналіз поведінки моделі. Такі атаки можуть бути складними для

виявлення та призводити до поступового зниження рівня безпеки системи без явних ознак компрометації.

Серйозним ризиком є залежність ефективності ШІ від якості та репрезентативності навчальних даних. Недостатньо збалансовані або застарілі набори даних можуть призводити до системних перекосів у роботі системи, зниження точності для окремих категорій користувачів та виникнення дискримінаційних ефектів. У контексті систем контролю доступу це може спричиняти як неправомірні відмови, так і порушення прав користувачів, що має не лише технічні, а й правові та етичні наслідки.

Додатковим недоліком є висока складність і непрозорість алгоритмів глибокого навчання. Неможливість чітко пояснити причини прийняття конкретного рішення ускладнює аудит безпеки, сертифікацію систем та розслідування інцидентів. Це особливо критично для об’єктів критичної інфраструктури, де кожне рішення системи доступу повинно бути обґрунтованим і відтворюваним.

Також варто враховувати підвищені вимоги до обчислювальних ресурсів та інфраструктури, що збільшує вартість впровадження й експлуатації таких систем. Крім того, збирання та обробка великих обсягів біометричних даних створює значні ризики для конфіденційності, адже компрометація біометричної інформації має незворотний характер.

Отже, використання штучного інтелекту в біометричних системах контролю доступу є водночас потужним інструментом підвищення безпеки та джерелом нових ризиків. Ефективне впровадження таких систем можливе лише за умови комплексного підходу, що поєднує сучасні алгоритми ШІ з криптографічним захистом, суворими політиками управління даними, регулярним аудитом, відповідністю міжнародним стандартам і врахуванням етичних та правових аспектів. Саме баланс між технологічними можливостями та ризиками визначатиме доцільність і безпечність застосування інтелектуальних біометричних систем контролю доступу в майбутньому.

### 3.15 Висновок

Був проведений аналіз біометричної системи з урахуваннями її недоліків та переваг , після чого був обраний шлях вдосконалення через переход від традиційної

одномодальної системи біометричного доступу до інтелектуальної адаптивної системи, що поєднує методи штучного інтелекту, елементи мультимодальної біометрії, та перехід до локальної обробки даних , та інтеграції AI-моделей в систему для зменшення ризиків та автономної роботи . Реалізація запропонованого вдосконалення дозволяє досягти значних результатів підвищення точності ідентифікації користувачів, зниження ймовірності помилкових рішень. Забезпечуючи відповідність сучасним стандартам безпеки та ефективний захист персональної інформації користувачів.

# ВИСНОВКИ ПО РОБОТІ

У магістерській кваліфікаційній роботі вирішено актуальне науково-практичне завдання щодо підвищення рівня захисту персональних даних у системах контролю та управління доступом на основі інтелектуальних біометричних технологій. Встановлено, що традиційні засоби автентифікації, зокрема паролі, картки та фізичні ключі, не забезпечують достатньої стійкості до втрати, передавання стороннім особам, підроблення або компрометації. Біометрична автентифікація дає змогу пов’язати процедуру надання доступу з фізіологічними чи поведінковими характеристиками користувача, зменшити вплив людського фактора та підвищити достовірність ідентифікації. Водночас біометричні дані є особливо чутливою категорією персональної інформації, тому потребують комплексного захисту.

У першому розділі систематизовано основні види біометричних систем і проаналізовано принципи їх функціонування. Розглянуто контактні та безконтактні сканери відбитків пальців, технології розпізнавання обличчя, райдужної оболонки ока, геометрії долоні, венозної сітки руки, ДНК, а також поведінкові характеристики. Визначено переваги, недоліки та експлуатаційні обмеження кожного підходу. Показано, що точність розпізнавання залежить від якості сенсора, стану біометричної ознаки, умов освітлення, правильності позиціонування користувача та стійкості до підроблення. Проаналізовано стандарти ISO/IEC, які регламентують формати біометричних даних, оцінювання якості зразків, обмін шаблонами та захист від атак.

У другому розділі досліджено мультимодальні біометричні системи, що поєднують дві або більше незалежних ознак. Встановлено, що злиття біометричної інформації дає змогу зменшити ймовірність помилкового допуску, компенсувати нестабільність окремої модальності та підвищити надійність ідентифікації. Доцільним є поєднання взаємодоповнювальних характеристик, наприклад розпізнавання обличчя з перевіркою відбитка пальця, венозної сітки або поведінкової ознаки. Разом із тим мультимодальність збільшує складність системи, обсяг оброблюваних персональних даних і вимоги до продуктивності, тому вибір модальностей має ґрунтуватися на оцінці ризиків, категорії об’єкта та принципі мінімізації даних.

У третьому розділі класифіковано актуальні загрози для біометричних систем контролю доступу. До них віднесено спуфінг із використанням фотографій, відеозаписів,

масок або штучно відтворених ознак; повторне відтворення перехоплених даних; атаки на біометричні шаблони, внутрішні модулі, бази даних і канали передавання; атаки на алгоритми машинного навчання; соціальну інженерію та зловживання привілеями. Обґрунтовано необхідність комплексного захисту, що включає перевірку живості, мультимодальну або багатофакторну автентифікацію, шифрування шаблонів і каналів зв'язку, розмежування прав доступу, контроль цілісності, захищене журналювання, регулярне оновлення та тестування системи.

Обґрунтовано доцільність використання штучного інтелекту та адаптивного навчання для підвищення точності й стійкості біометричної ідентифікації. Інтелектуальні алгоритми здатні враховувати поступові зміни зовнішності користувача, покращувати розпізнавання за складних умов, виявляти аномальні сценарії та ознаки deepfake або спуфінгу. Водночас адаптивне оновлення моделей повинно виконуватися лише після надійного підтвердження особи, із контролем довіри, перевіркою якості нових зразків, журналюванням змін і можливістю повернення до попередньої версії моделі.

Практичним результатом роботи є концепція вдосконаленої системи розпізнавання обличчя, яка передбачає оцінювання якості зображення, перевірку живості, виявлення спуфінгу та deepfake-ознак, формування захищеного біометричного шаблону, аналіз контексту доступу та ризик-орієнтоване прийняття рішення. Для критичних операцій або сумнівних результатів доцільно залучати додаткову біометричну ознаку чи інший фактор автентифікації. Біометричні шаблони необхідно зберігати у захищеному вигляді із застосуванням шифрування, токенізації або скасованої біометрії, а оброблення даних здійснювати відповідно до принципів законності, визначеної мети, мінімізації та обмеження строку зберігання.

Таким чином, мету магістерської роботи досягнуто, а поставлені завдання виконано. Досліджено основні біометричні технології, визначено переваги мультимодального підходу, проаналізовано актуальні загрози та сформовано пропозиції щодо вдосконалення системи контролю доступу на основі розпізнавання обличчя. Запропоновані рішення можуть бути використані під час проєктування або модернізації систем контролю доступу на підприємствах, у державних установах, банківській сфері та на об'єктах критичної інфраструктури. Подальші дослідження доцільно спрямувати на експериментальне оцінювання показників FAR, FRR та EER, перевірку стійкості до presentation attacks і

deepfake-атак, а також розроблення засобів захисту моделей машинного навчання та біометричних шаблонів.

# ПЕРЕЛІК ПОСИЛАНЬ

1https://ela.kpi.ua/server/api/core/bitstreams/2770e38c-c7f1-4d2d-9a2e-8c010a4f87ad/content

2 https://scispace.com/pdf/biomet-a-multimodal-biometric-authentication-system-for-1vgjvtdj6f.pdf

3https://ela.kpi.ua/server/api/core/bitstreams/b212eee5-a059-4bb2-a39e-8d1946f4c0f4/content

4 https://re.kpi.ua/wp-content/uploads/2023/01/dyplom-kyrylenko.pdf

5https://duikt.edu.ua/repozitorii/%D0%9A%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B0%20%D0%A2%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83/2020/%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC%20%D0%91%D0%BE%D0%BD%D0%B4%D0%B0%D1%80%D1%8C%20%D0%A1%D0%97%D0%94%D0%9C-61.pdf

6 https://duikt.edu.ua/repozitorii/%D0%9A%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B0%20%D0%A2%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83/2020/%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC%20%D0%91%D0%BE%D0%BD%D0%B4%D0%B0%D1%80%D1%8C%20%D0%A1%D0%97%D0%94%D0%9C-61.pdf

7 file:///D:/%D1%81%D0%BA%D0%B0%D1%87%D0%B0%D0%BD%D0%BE%D0%B5/cyril,+6.pdf

8 https://www.infocom.zp.ua/wp-content/uploads/2020/07/Bio_Business.pdf

9 https://www.neurotechnology.com/megamatcher-abis.html?gad_source=1&gad_campaignid=962911673&gbraid=0AAAAAD_Q61BVle6G46E

3KHygtJ1skWMuj&gclid=CjwKCAiA3fnJBhAgEiwAyqmY5WUeGgU1KyUjEu908W6xexFjFRYzHOCSiaYufqQno6zR9nYc6-sBJxoC9bIQAvD_BwE

10 https://vario.com.ua/biometricheskaya-sistema-kontrolya-dostupa-po-venam-paltsa-zkteco-fv350/?srsltid=AfmBOoqGHVe9gGygZoktnmSBOaskkaJrPEnbx3b4z_IFUX3vyy0pnM9B

11 https://habr.com/ru/companies/otus/articles/787116/

12 https://op.edu.ua/sites/default/files/publicFiles/dissphd/robota_phd_shamanina_t.v.pdf

13 https://itzo-book.at.ua/load/disciplina/lekcijni_zanjattja/tema_9_biometrichni_sistemi_rozpiznannja_ljudini/2-1-0-12

14 https://yur-gazeta.com/publications/practice/inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html

15 https://journal.comp-sc.if.ua/test/index.php/ITCM/article/view/627/648

16 https://iq.vntu.edu.ua/repository/getfile.php/6093.pdf

17 https://itez.com.ua/blog/social-engineering-vishing-smishing-deepfake-protection.html

18 https://csecurity.kubg.edu.ua/index.php/journal/article/view/670/547

19 https://elartu.tntu.edu.ua/bitstream/lib/48666/1/Mag_2025_SNnm_61_Savchyshyn_Y_S.pdf

20 https://online.budstandart.com/ua/catalog/doc-page?id_doc=104379

21 https://www.rapidinnovation.io/post/ai-agents-for-biometric-authentication

22 https://www.zen.com/ua/blog/personal-finance-uk/features-of-biometric-identification-in-the-financial-sphere/

23 https://journals.dut.edu.ua/index.php/dataprotect/article/view/3235.com

24 https://www.iso.org/standard/83828.html?utm.com

25 https://en.wikipedia.org/wiki/Main_Page

26 https://arxiv.org/abs/2007.11318

27 https://tst.stu.cn.ua/article/view/215780

28 https://automation.honeywell.com/us/en/campaigns/hts/thermal-iq?utm_source=google&utm_medium=cpc&utm_campaign=25-sets-hts-npi-thermalsolutions_thermaliq-google_ad&gad_source=1&gad_campaignid=23246714046&gbraid=0AAAAAqCsnWtzjPQu0U5qdxup81qhRhmVW&gclid=CjwKCAiA3fnJBhAgEiwAyqmY5UzG4y3VwOpj18aRPPtoZNQkR0FEfqpIZIZuFAkLyZIbYSjC8FFy5BoCUrsQAvD_BwE

29 https://www.redhat.com/en/engage/improve-security-compliance-ebook?sc_cid=7013a000002w17SAAQ&gclsrc=aw.ds&gad_source=1&gad_campaignid=22032471047&gbraid=0AAAADsbVMSxw98UhjHRPwAvVaXIY-NTS&gclid=CjwKCAiA3fnJBhAgEiwAyqmY5TVeDdEIdBkO79wLvihgtBZNsmHOvC_yUvFt4ZrM3McJPA-IlNOOkxoCF3MQAvD_BwE

30 https://neurotechnology.com/megamatcher-biometric-identity-registration-system.html?gad_source=1&gad_campaignid=20701797293&gbraid=0AAAAAD_Q61DA2ocNKNUT71HtqibOkvzHU&gclid=CjwKCAiA3fnJBhAgEiwAyqmY5ViW0bg8dlvWFGtcU71RnfAXPFKZ1J9LhlKi10NoI7yClv65up6_IhoCiCwQAvD_BwE

# ДОДАТКИ



## Захист персональних даних інтелектуальною біометричною системою контролю доступом

- Магістерська робота: Роман ЧЕЧКО
- Спеціальність 125 «Кібербезпека та захист інформації»
- Керівник: Юрій ПЕПА, к.т.н., доцент
- Фокус: біометричні системи доступу, персональні дані, штучний інтелект, контроль доступу





## Актуальність дослідження

- Зростання обсягів персональних даних потребує надійних механізмів контролю доступу.
- Традиційні паролі та картки можуть бути втрачені, підроблені або передані стороннім особам.
- Інтелектуальні біометричні системи підвищують точність ідентифікації та знижують ризик НСД.

## Мета, об’єкт і предмет роботи

- Мета: дослідити інтелектуальну біометричну систему контролю доступу з метою підвищення рівня захисту персональних даних.
- Об’єкт: процес забезпечення інформаційної безпеки та захисту персональних даних у системах контролю доступу.
- Предмет: методи, алгоритми та технології захисту персональних даних у біометричних системах контролю доступу.





## Основні завдання дослідження

- Проаналізувати існуючі біометричні системи доступу та принципи їх роботи.
- Дослідити мультимодальну біометричну систему доступу.
- Визначити основні загрози для біометричних систем і методи протидії.
- Обґрунтувати напрями вдосконалення біометричної моделі доступу із застосуванням ШІ.

## Структура магістерської роботи

- Розділ 1 - біометричні системи доступу та їх класифікація.
- Розділ 2 - мультимодальна біометрична система доступу.
- Розділ 3 - загрози для біометричних систем, методи захисту та використання ШІ.
- У роботі розглянуто фізіологічні, поведінкові та комбіновані біометричні характеристики.





## Біометрична система доступу

- Біометрична система доступу використовує унікальні фізіологічні або поведінкові характеристики людини.
- Процес включає зчитування ознаки, попередню обробку, формування шаблону та порівняння з еталонними даними.
- Після успішної ідентифікації або верифікації користувачу надається доступ до захищеного ресурсу.

## Фізіологічні біометричні характеристики

- До фізіологічних ознак належать відбитки пальців, обличчя, райдужна оболонка ока, геометрія долоні та венозна сітка руки.
- Такі ознаки є відносно стабільними та складними для випадкового відтворення.
- Ефективність залежить від якості сенсора, стану біометричної ознаки та умов зчитування.





## Контактні та безконтактні сканери відбитків пальців

- Контактні оптичні сканери мають просту конструкцію, невисоку вартість і високу точність у стандартних умовах.
- Недоліки контактних сканерів: зношення поверхні, забруднення, залишкові відбитки та нижча гігієнічність.
- Безконтактні сканери зменшують фізичний контакт, але потребують точнішого позиціонування та якісної оптики.

## Розпізнавання обличчя

- Технологія розпізнавання обличчя забезпечує зручну та швидку ідентифікацію користувача.
- Основні етапи: виявлення обличчя, виділення ознак, формування шаблону та зіставлення з базою.
- Система потребує захисту від фотографій, відеозаписів, масок і deepfake-атак.





## Інші біометричні технології

- Сканування райдужної оболонки забезпечує високу точність, але потребує спеціалізованого обладнання.
- Геометрія долоні та венозна сітка руки придатні для контрольованих зон і корпоративних систем доступу.
- ДНК-біометрія має високу ідентифікаційну цінність, але є складною, повільною та непридатною для оперативного доступу.

## Поведінкові біометричні характеристики

- Поведінкові ознаки включають голос, почерк, клавіатурний почерк та інші динамічні характеристики користувача.
- Такі системи можуть працювати як додатковий фактор безперервної автентифікації.
- Недоліки: залежність від емоційного стану, умов середовища, обладнання та зміни поведінки користувача.





## Мультимодальна біометрична система доступу

- Мультимодальна система поєднує дві або більше біометричних ознак для підвищення надійності контролю доступу.
- Злиття даних може виконуватися на рівні сенсорів, ознак, оцінок відповідності або остаточних рішень.
- Переваги: менша ймовірність помилкового допуску, вища стійкість до підроблення та відмов окремої модальності.

## Загрози для біометричних систем

- Ключові загрози: спуфінг, атаки відтворення, компрометація шаблонів, атаки на бази даних і канали передавання.
- Окрему небезпеку становлять атаки на алгоритми машинного навчання та соціальна інженерія.
- Компрометація біометричного шаблону є критичною, оскільки біометричну ознаку неможливо швидко замінити як пароль.





## Методи захисту біометричних систем

- Необхідні механізми: перевірка живості, антиспуфінг, багатофакторна автентифікація та контроль цілісності.
- Біометричні шаблони потрібно зберігати у захищеному вигляді із застосуванням шифрування, токенізації або скасованої біометрії.
- Важливими є розмежування прав доступу, журналювання подій, аудит і захищені канали передавання.

## Штучний інтелект у біометричних системах

- ШІ підвищує точність розпізнавання, дозволяє аналізувати складні ознаки та виявляти підозрілу активність.
- Адаптивне навчання дає змогу враховувати поступові зміни зовнішності або поведінки користувача.
- Оновлення моделей має виконуватися контрольовано, щоб уникнути отруєння даних і викривлення біометричного профілю.





## Висновки

- Досліджено основні біометричні системи доступу, їх переваги, недоліки та стандарти застосування.
- Визначено доцільність мультимодального підходу для підвищення надійності ідентифікації.
- Проаналізовано загрози біометричним системам та запропоновано напрями захисту персональних даних.
- Обґрунтовано використання інтелектуальної адаптивної біометричної системи контролю доступу.