

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут телекомунікацій

Кафедра системного аналізу

Пояснювальна записка

до бакалаврської роботи

на ступінь вищої освіти бакалавр

на тему: «**ІНФОРМАЦІЙНА СИСТЕМА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ
НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ**»

Виконав: студент 4 курсу,
групи САД-41, спеціальності

124 Системний аналіз

(шифр і назва спеціальності)

Павлов А.О.

(прізвище та ініціали)

Керівник

Кузьміч М.Ю.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Київ – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут Телекомунікацій

Кафедра _____ Системного аналізу

Ступінь вищої освіти _____ «Бакалавр»

Спеціальність _____ 124 Системний аналіз

ЗАТВЕРДЖУЮ

Завідувач кафедри

Системного аналізу

(ПІБ)

Дата: _____ 2023 року

З А В Д А Н Н Я

НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

(прізвище, ім'я, по батькові)

1. Тема роботи: _____ «Інформаційна система ідентифікації користувачів на основі біометричних даних»

Керівник роботи _____ Кузьміч М.Ю.

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від _____ 2023 року № _____.

2. Строк подання студентом роботи _____

3. Вхідні дані до роботи:

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити).

5. Перелік графічного матеріалу

1) _____

2) _____

3) Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1			
2			
3			
4			
5			
6			
7			
8			
9			

Студент

(підпис)

(прізвище та ініціали)

Керівник роботи

(підпис)

(прізвище та ініціали)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студент Павлов А.О. до захисту бакалаврської роботи
 (прізвище та ініціали)

за спеціальністю 124 Системний аналіз
 (шифр і назва спеціальності)

на тему: «Інформаційна система ідентифікації користувачів на основі біометричних даних»

Бакалаврська робота і рецензія додаються.

Директор інституту Толубко В.Б.
 (підпис)

Довідка про успішність

Павлов А.О. за період навчання в Навчально-науковому інституті Телекомунікації
 (прізвище та ініціали студента)

з 2021 року до 2023 року повністю виконав навчальний план за спеціальністю з таким розподілом оцінок за:

національною шкалою: відмінно ____%; добре ____%; задовільно ____%;

шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Методист факультету:

 (підпис)

 (прізвище та ініціали)

Висновок керівника бакалаврської роботи

Студент Павлов Артем Олексійович

Все це дозволяє оцінити виконану бакалаврську роботу студента Павлова А.О. на оцінку «_____» та присвоїти йому кваліфікацію фахівця з інформаційних технологій.

Керівник роботи

(підпис)

(прізвище та ініціали)

_____ 2023 року

Висновок кафедри про бакалаврську роботу

Бакалаврську роботу розглянуто(а). Студент Павлов А.О. допускається до захисту даної роботи в Державній екзаменаційній комісії.
 (прізвище та ініціали)

Завідувач кафедри Системного аналізу

(підпис)

Гордієнко Т.Б.

(прізвище та ініціали)

РЕФЕРАТ

Оглавление

ВСТУП	9
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ	11
1.1 Біометрія та її роль в житті людини	11
1.2 Історія зародження інформаційних систем ідентифікації користувачів на основі біометричних даних.....	12
1.3 Біометричні данні, методи та їх використання	13
1.4 Біометрична ідентифікація користувача.....	14
1.5 Особливості біометричних даних.....	18
1.6 Переваги ідентифікації по біометричним даним.....	19
1.7 Актуальність та застосування.....	20
2 СИСТЕМНИЙ АНАЛІЗ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ	21
2.1 Системи розпізнавання обличчя	21
2.1.1 OpenCV	22
2.1.2 Amazon Rekognition.....	25
2.1.3 Microsoft Face API	27
2.1.4 FaceSDK	30
2.2 Системи розпізнавання відбитків пальців.....	33
2.2.1 VeriFinger	33
2.2.2 Fingerprint SDK.....	36
2.2.3 DigitalPersona	39
2.2.4 RealScan.....	40
2.3 Системи розпізнавання райдужної оболонки ока.....	42
2.3.1 IrisID	43
3 ТЕНДЕНЦІЇ РОЗВИТКУ ІСУП, ЇХ ПРОБЛЕМАТИКИ І РІШЕННЯ ЦИХ ПРОБЛЕМАТИК	45
ВИСНОВОК.....	60
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ	62

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DNK (ДНК) – означає дезоксирибонуклеїнову кислоту, біомолекулу, яка зберігає генетичну інформацію в клітинах живих організмів.

LBPH (Local Binary Patterns Histograms) – метод комп'ютерного зору та обробки зображень, що використовується для розпізнавання обличчя.

GPU (Graphics Processing Unit) – вид процесорів, призначених для обробки графіки та зображень.

API (Application Programming Interface) – набір інтерфейсів, протоколів та інструментів, що дозволяють різним програмам взаємодіяти між собою.

VPN (Virtual Private Network) – технологія, яка дозволяє забезпечити безпеку та конфіденційність мережевого з'єднання через відкриту мережу, таку як Інтернет. За допомогою VPN створюється зашифрований тунель між двома пристроями, що дозволяє передавати дані безпечно і приватно.

SDK (Software Development Kit) – набір інструментів для розробки програмного забезпечення, який зазвичай включає набір бібліотек, документацію, приклади коду та інші корисні матеріали для розробки програм.

FRS (Facial Recognition System) – система розпізнавання осіб за обличчям.

TPU (Tensor Processing Unit) – спеціалізований процесор, розроблений компанією Google для швидкого виконання обчислень, пов'язаних з машинним навчанням та інтелектуальним аналізом даних.

JPEG, PNG, BMP, AVI, WMV, MOV – це формати файлів для зображень та відео.

LBPH (Local Binary Patterns Histograms) – метод комп'ютерного зору для обробки зображень та розпізнавання облич.

ВСТУП

Інформаційні технології сьогодні відіграють надзвичайно важливу роль у багатьох сферах людської діяльності. Розвиток інтернету, комп'ютерних мереж та технологій зберігання і обробки даних дозволяють створювати різноманітні інформаційні системи для автоматизації процесів в різних галузях, в тому числі й у галузі ідентифікації користувачів.

У світі, де інформація стає все більш цінним ресурсом, захист даних користувачів стає дедалі важливішим завданням. Біометрична ідентифікація є однією з найбільш ефективних методів забезпечення безпеки інформації, оскільки вона базується на унікальних фізіологічних та поведінкових характеристиках кожної людини, такими як відбитки пальців, розміри обличчя, голос, ритм серця та інші. Інформаційна система ідентифікації користувачів на основі біометричних даних є однією з актуальних проблем, яка набуває все більшого значення в контексті захисту особистої інформації та забезпечення безпеки в цифровому просторі.

Ступінь вивченої проблеми вказує на актуальність даної теми і її значимість. Останні роки характеризуються зростанням кількості кібератак, які спрямовані на отримання конфіденційної інформації користувачів, що підкреслює необхідність створення надійних інформаційних систем ідентифікації користувачів на основі біометричних даних.

Об'єктом дослідження є інформаційна система ідентифікації користувачів на основі біометричних даних, аналіз існуючих рішень, розглянуті програмні забезпечення які застосовуються в даній системі чи сфері, основні можливості, проблеми з якими зустрічаються користувачі та відсутність функціоналу який доступний на даний час та може бути впроваджений в їх систему, що зробить їх додаток більш зручнішим та простішим у використанні. Були розглянуті плюси і мінуси даних системи, їх проблематика та методи вирішення.

Предметом дослідження інформаційної системи ідентифікації користувачів на основі біометричних даних є процес розробки та впровадження системи ідентифікації осіб, яка базується на зборі та обробці біометричних даних, таких як

відбитки пальців, обличчя, голос тощо. Дослідження включає в себе аналіз сучасних методів біометричної ідентифікації, а також розробку ефективної системи, яка забезпечує надійний захист особистих даних користувачів та інформаційних ресурсів. Основними складовими предмета дослідження є аналіз вимог до системи, розробка алгоритмів збору та обробки біометричних даних, впровадження системи в практичну діяльність та оцінка її ефективності.

Наукова новизна роботи системи ідентифікації по біометричним даним полягає в розробці та реалізації алгоритмів та моделей, що базуються на біометричних даних, які можуть бути використані для ідентифікації та автентифікації користувачів. Дослідження в цій області спрямовані на розвиток нових технологій та методів, що дозволять забезпечити високий рівень захисту конфіденційної інформації та уникнути можливих порушень безпеки даних. Одним з ключових внесків даної роботи є покращення систем захисту біометричних даних користувачів, що забезпечує їх захист від несанкціонованого доступу та використання.

Отже, розробка та вдосконалення інформаційних систем ідентифікації користувачів на основі біометричних даних є дуже важливим завданням в сучасному світі, оскільки це дозволяє забезпечити безпеку та конфіденційність інформації

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Біометрія та її роль в житті людини

Біометрія – це область науки, яка вивчає фізіологічні та поведінкові характеристики людини для їх використання в ідентифікації особистості. Найпоширеніші приклади біометричних характеристик включають відбитки пальців, райдужну оболонку ока, обличчя, голос та інші.

Роль біометрії у житті може бути різноманітною. Наприклад:

- **Безпека.** Біометрична ідентифікація може бути використана для захисту інформації, відомостей про фінансові транзакції, будівель та багато іншого. Вона може зробити системи безпечнішою та допомогти запобігти злочинам.
- **Охорона здоров'я.** Біометрія може використовуватися в медичних цілях, таких як ідентифікація пацієнтів, автентифікація медичних працівників та забезпечення доступу до медичних даних.
- **Подорожі.** Біометрична ідентифікація може бути використана на кордонах, в аеропортах та інших місцях для ідентифікації пасажирів та перетину кордонів.
- **Зручність.** Біометрична ідентифікація може зробити життя простіше, запобігаючи необхідності запам'ятовування та введення паролів або PIN-кодів.
- **Маркетинг.** Деякі компанії можуть використовувати біометричні дані для аналізу поведінки покупців та покращення досвіду покупок.
- **Ігрова індустрія.** Біометричні технології можуть використовуватися в ігровій індустрії для створення більш реалістичних ігрових персонажів та підвищення залученості гравців.

Крім того, біометричні технології можуть використовуватися в інших галузях, таких як туризм, логістика, спорт і навіть мистецтво. Однак, як і в будь-якій іншій технології, існують певні ризики та обмеження, пов'язані з

використанням біометричних даних, такі як потенційна вразливість для атак хакерів і порушення конфіденційності.

1.2 Історія зародження інформаційних систем ідентифікації користувачів на основі біометричних даних

Історія розвитку інформаційних систем ідентифікації користувачів на основі біометричних даних розпочалася ще наприкінці XIX століття. В 1892 французький антрополог Альфред Біне опублікував свою роботу, в якій запропонував використовувати фотографію особи для ідентифікації злочинців. Протягом наступних десятиліть вчені продовжували досліджувати та розробляти методи ідентифікації, засновані на біометричних даних, таких як відбитки пальців, голос, обличчя та інші.

Перша біометрична система ідентифікації, яка була введена в експлуатацію, була система ідентифікації відбитків пальців, яку у 1896 році запровадили у Франції. З того часу системи ідентифікації на основі біометричних даних продовжують розвиватися та покращуватися.

Одним із ключових етапів у розвитку біометричних систем було створення у 1960-х роках перших автоматичних систем розпізнавання обличчя. Наступним важливим етапом було створення у 1970-х роках систем ідентифікації голосу. У 1990-х роках стали з'являтися перші системи ідентифікації на основі райдужки ока та системи розпізнавання рукописного почерку.

З появою комп'ютерних технологій та розвитком штучного інтелекту, біометричні системи ідентифікації стали більш точними та ефективними. Сьогодні вони широко застосовуються у багатьох галузях, таких як охорона безпеки, медична діагностика, банківські транзакції тощо. Однак, розвиток біометричних технологій також викликає питання безпеки та захисту персональних даних користувачів, що потребує розробки відповідних стандартів та правил їх використання.

1.3 Біометричні дані, методи та їх використання

Ідентифікація – це процес визначення особи чи об'єкта, тобто встановлення його особливостей, які дозволяють розпізнати його серед інших подібних об'єктів чи осіб. В контексті безпеки та захисту даних, ідентифікація зазвичай відбувається за допомогою унікальних ідентифікаторів, таких як номери ID, паролі, біометричні дані тощо, які дозволяють відрізнити конкретну особу чи об'єкт від інших.

Біометричні дані це унікальні фізіологічні або поведінкові характеристики людини, які можуть бути використані для ідентифікації або аутентифікації особистості. Біометричні розрізняються фізіологічними та поведінковими характеристиками (див.рис.1.3.1).

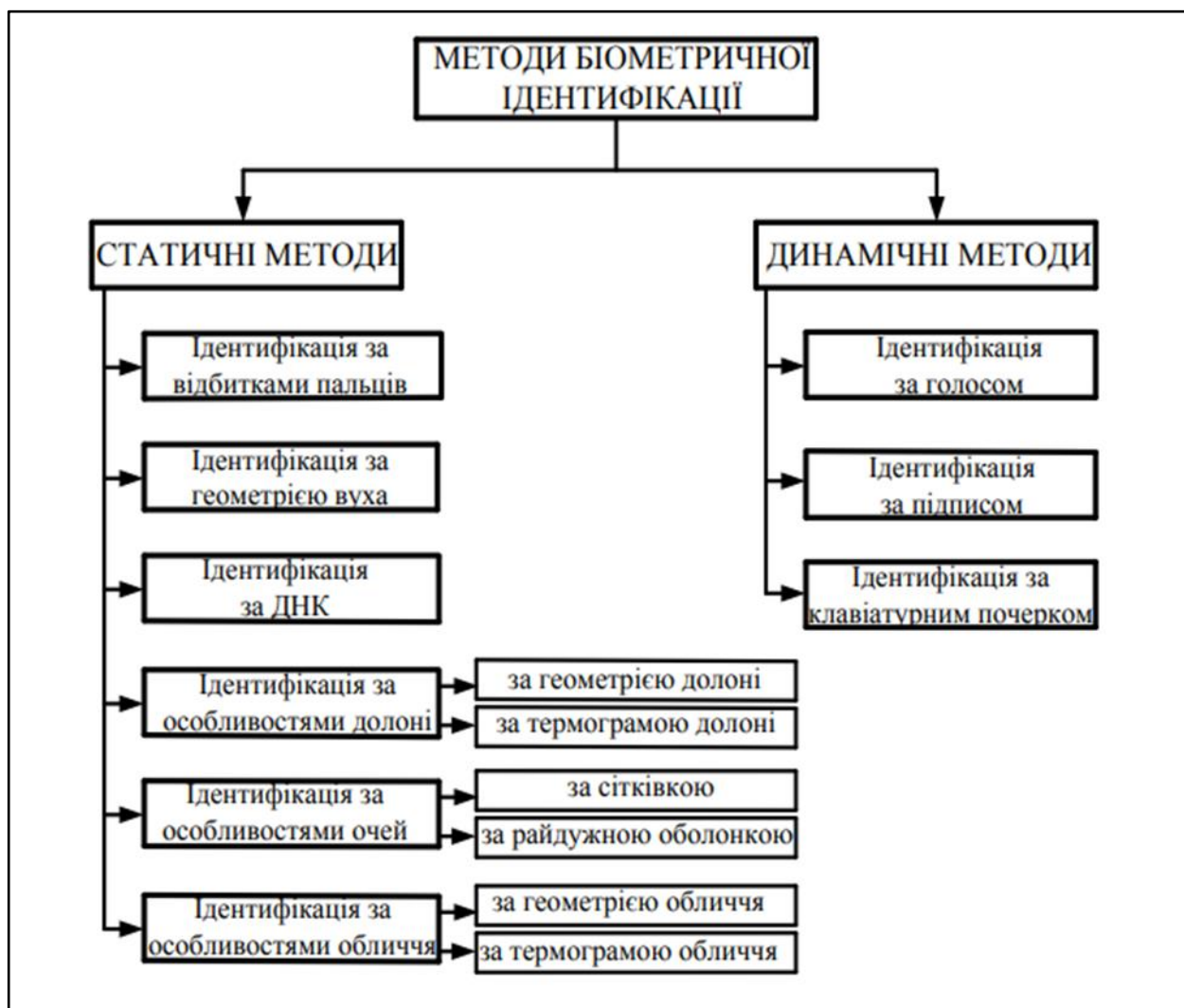


Рисунок 1.3.1 – Методи біометричної ідентифікації

Фізіологічні (статистичні) характеристики включають фізичні риси тіла, такі як відбитки пальців, форма обличчя, розмір і структура очей, голос та ДНК. Ці характеристики унікальні для кожної особи і їх можна використовувати для ідентифікації особи.

Поведінкові (динамічні) характеристики включають особливості поведінки, такі як почерк, голос, походка тощо. Ці характеристики, як фізіологічні є унікальними і можуть бути використані для ідентифікації особи.

В даний час біометричні дані активно використовуються в різних галузях, таких як банківська справа, безпека, державні служби, медична діагностика і т.д. Їхня головна перевага полягає в тому, що вони служать більш надійним способом ідентифікації особистості, ніж традиційні методи, такі як паролі або PIN-коди.

Однак біометричні дані також викликають побоювання щодо безпеки та конфіденційності. У разі витоку біометричних даних їх можна використовувати для підробки або шахрайства. Тому необхідно забезпечувати відповідний захист та зберігання цих даних [1,2].

1.4 Біометрична ідентифікація користувача

Ідентифікація користувача за біометричними даними – це процес використання біометричних характеристик для підтвердження особи користувача. У процесі ідентифікації користувач надає свої біометричні дані, які порівнюються зі збереженими в базі даних.

Процес ідентифікації за біометричними даними може використовуватися для різних цілей, наприклад для забезпечення безпеки, контролю доступу або авторизації транзакцій. Наприклад, при використанні відбитків пальців для ідентифікації користувача сканується відбиток пальця та порівнюється зі збереженим у базі даних відбитком пальця користувача. Якщо дані збігаються, користувач підтверджує свою особистість і отримує доступ до захищених ресурсів або послуг.

Використання біометричних даних для ідентифікації користувачів забезпечує високий рівень безпеки, оскільки біометричні характеристики є

унікальними для кожної людини і не можуть бути підроблені або скомпрометовані без фізичного доступу до користувача. Однак, також існують ризики, пов'язані зі зберіганням та використанням біометричних даних, такі як можливість їх витоку чи зловживання. Тому важливо забезпечувати надійний захист та конфіденційність біометричних даних [2].

Розпізнання голосу. Голос людини містить унікальні фізіологічні та поведінкові ознаки, які можуть бути використані для ідентифікації або верифікації особи. Цей метод використовується для ідентифікації особи на основі її унікальних звуків голосу, таких як тон, інтонація, склад, швидкість мовлення та інших акустичних властивостей. Ці параметри формуються через вібрації голосових зв'язок під час вимовляння звуків та слів. Іншими фізіологічними ознаками голосу є розмір та форма гортані, що впливає на звукові характеристики голосу.

Поведінкові ознаки голосу включають такі параметри, як ритм мовлення, швидкість мовлення, акцент та інші аспекти, які відрізняють голос кожної людини. Ці ознаки формуються через життєвий досвід та навички людини, тому вони є унікальними для кожної особи.

Голосова біометрія застосовується в різних сферах, таких як фінансові установи, урядові органи, технічна підтримка, медичні установи та інші. Наприклад, банки використовують голосову біометрію для ідентифікації клієнтів, щоб запобігти шахрайству та крадіжкам. Урядові органи можуть використовувати голосову біометрію для перевірки осіб на контрольних пунктах або для ідентифікації військовослужбовців.

Розпізнання обличчя. Є одним із методів біометричної ідентифікації, що використовується для автоматичного розпізнавання особи за допомогою візуального аналізу рис обличчя.

Основна ідея розпізнавання обличчя полягає у тому, щоб зіставити біометричні дані, отримані з вхідного зображення обличчя, з біометричними даними, збереженими у базі даних. Для цього використовуються спеціальні алгоритми комп'ютерного зору та машинного навчання, які дозволяють розпізнавати унікальні риси обличчя.

Для забезпечення точності ідентифікації використовуються різноманітні методи обробки зображень, такі як виявлення контурів, виокремлення основних рис обличчя, вимірювання відстаней та кутів між ними, аналіз текстури шкіри та інші.

Є декілька основних застосувань розпізнавання обличчя, такі як контроль доступу, ідентифікація злочинців, відслідковування відвідувань магазинів та інших громадських місць, автоматичне сортування фотографій та відео, інтелектуальні системи безпеки і т.д.

Розпізнавання радужної оболонки. Розпізнавання радужної оболонки ока, також відоме як ірідодіагностика, є одним з методів біометричної ідентифікації людини. Цей метод полягає в аналізі унікальної структури радужки ока, що складається з різних відтінків кольорів, ліній, точок та плям.

Розпізнавання радужки ока відбувається з використанням спеціального обладнання, яке сканує та зберігає унікальну структуру радужки ока. У процесі розпізнавання зібрані дані порівнюються з збереженими у базі даних, що містять інформацію про попередньо зареєстрованих користувачів. Якщо дані збігаються, то користувач отримує доступ до захищеної інформації або системи.

Однією з головних переваг розпізнавання радужки ока є висока точність ідентифікації, оскільки кожна радужка є унікальною для кожної людини і не піддається змінам з часом. Крім того, цей метод біометричної ідентифікації є зручним для використання в умовах, коли не можна здійснювати фізичний контакт з користувачем, наприклад, при віддаленому доступі до систем.

Однак, розпізнавання радужки ока має свої недоліки, включаючи високу вартість обладнання та невисоку швидкість сканування порівняно з іншими методами біометричної ідентифікації, такими як розпізнавання відбитку пальця. Крім того, цей метод може бути неефективним при низькій якості освітлення або при наявності хвороб ока, які можуть змінювати структуру.

Розпізнавання відбитків пальців. Біометричний відбиток пальця – це унікальний шаблон ліній і точок, які утворюються на поверхні пальця і можуть бути використані для ідентифікації особи. Кожна людина має свій власний

індивідуальний біометричний відбиток пальця, і це робить його дуже надійним інструментом для ідентифікації особи.

Для збору біометричних даних про відбитки пальців використовують спеціальні сканери, які зчитують лінії і точки на поверхні пальця. Ці дані потім зберігаються в базі даних і можуть бути використані для порівняння з іншими відбитками пальців для ідентифікації особи.

Біометричні відбитки пальців застосовуються в багатьох сферах, включаючи безпеку, медицину, фінанси та громадські служби. Наприклад, в аеропортах використовують біометричні системи для ідентифікації пасажирів, що дозволяє прискорити процес проходження контролю та забезпечити безпеку польотів. Також, біометричні системи з використанням відбитків пальців можуть бути використані для доступу до робочих місць, офісних приміщень, або навіть до особистих пристроїв, таких як смартфони та планшети.

Хоча біометричні системи з використанням відбитків пальців дуже надійні, вони також можуть мати деякі проблеми, такі як помилки при зчитуванні відбитків пальців через забруднення, зношеність або пошкодження поверхні пальців.

Технологія біометричних відбитків пальців застосовується в різних галузях, де потрібна ідентифікація особи, наприклад:

- для входу до приватних і громадських приміщень та обмеження доступу до окремих зон;
- для аутентифікації користувача на пристроях зберігання даних, таких як смартфони, планшети, ноутбуки та комп'ютери;
- для аутентифікації на робочому місці та обмеження доступу до певних систем або програм;
- для захисту особистих даних та фінансових транзакцій;
- для контролю доступу на виробництві та управлінні персоналом;
- для контролю працівників на будівельних майданчиках та відстеження робочого часу.
- у медицині для ідентифікації пацієнтів та зберігання медичної інформації;

- у системах автоматичної оплати транспорту для швидкого та зручного доступу до транспортних послуг;
- у системах контролю за наявністю та обліку вогнепальної зброї;
- в системах банківської безпеки та фінансових операцій для запобігання шахрайства та використання підроблених документів;
- у системах реєстрації виборців та підтвердження їх особистості на виборчих дільницях.

Також біометричні відбитки пальців використовуються в галузі правоохоронних органів для розкриття злочинів та інших юридичних цілей.

У загальному, технологія біометричних відбитків пальців застосовується там, де потрібна швидка та надійна ідентифікація особи, яка забезпечується унікальністю відбитка пальця.

1.5 Особливості біометричних даних

Біометричні дані мають кілька особливостей:

- **Унікальність.** Біометричні дані є унікальними для кожної людини, що дозволяє використовувати їх для ідентифікації або аутентифікації. Навіть якщо дві людини мають схожі властивості, такі як форма особи, їх деталі можуть відрізнятися.
- **Незмінність.** Біометричні дані змінюються дуже повільно чи взагалі змінюються протягом життя. Наприклад, відбитки пальців, форма обличчя та райдужна оболонка ока не зміняться від народження до смерті.
- **Відтворюваність.** Біометричні дані можуть бути відтворені в тому ж вигляді, що і при початковій реєстрації, що дозволяє їх використовувати для повторної аутентифікації.
- **Складність.** Біометричні дані складні для підробки, оскільки вони ґрунтуються на біологічних характеристиках людини.
- **Приватна інформація.** Біометричні дані належать до категорії приватної інформації, тому їх використання має відповідати правилам

конфіденційності та захисту персональних даних [5].

1.6 Переваги ідентифікації по біометричним даним

Конкретні переваги ідентифікації за біометричними даними можуть різнитися залежно від конкретного випадку використання, проте можна виділити такі переваги:

- **Безпека.** Біометричні дані складніше підробити або скопіювати, ніж паролі або пін-коди, які можуть бути вкрадені або вгадані. Це дозволяє підвищити рівень безпеки у системах ідентифікації та авторизації.
- **Зручність.** Біометрична ідентифікація не вимагає запам'ятовування паролів або носіїв (таких як ключі чи карти доступу), що робить її зручною для користувачів.
- **Ефективність.** Ідентифікація за біометричними даними може бути більш швидкою та ефективною, ніж традиційні методи авторизації, такі як введення паролів або презентація карток доступу.
- **Надійність.** Біометричні дані можуть бути використані для точної ідентифікації особи, що дає змогу знизити кількість випадків шахрайства або помилок ідентифікації.
- **Низька вартість.** У деяких випадках використання біометричної ідентифікації може бути дешевшим, ніж традиційні методи, такі як виробництво та розповсюдження носіїв доступу або підтримка інфраструктури для зберігання та керування паролями.
- **Автоматизація.** Вбудовані сканери відбитків пальців або системи розпізнавання облич можуть бути інтегровані в різні пристрої та програмні програми, що дозволяє автоматизувати процеси ідентифікації та авторизації.
- **Незмінність.** Деякі біометричні дані, такі як відбитки пальців, не змінюються протягом життя людини, що дозволяє їх використовувати для постійної ідентифікації користувача.

1.7 Актуальність та застосування

Біометричні дані мають високу актуальність у сучасному світі, де потрібна швидка та надійна ідентифікація особистості. Вони застосовуються у багатьох сферах, включаючи:

- **Безпека.** Біометричні технології широко використовуються у забезпеченні безпеки, наприклад, при доступі до захищених об'єктів, комп'ютерів, мобільних пристроїв тощо;
- **Медична індустрія.** Біометричні дані використовуються в медичній індустрії для ідентифікації пацієнтів, контролю доступу до медичних даних та захисту цих даних.
- **Державні служби.** Біометричні технології використовуються у державних службах для ідентифікації громадян, контролю доступу до державних баз даних та захисту державної інформації.
- **Фінансовий сектор.** Біометричні технології використовуються у фінансовому секторі для ідентифікації клієнтів, захисту банківських рахунків та запобігання шахрайству.
- **Транспорт.** Біометричні технології використовуються в транспортній галузі для ідентифікації пасажирів, керування квитковими системами та підвищення безпеки на транспорті.
- **Роздрібна торгівля.** Біометричні технології використовуються у роздрібній торгівлі для ідентифікації клієнтів, контролю доступу до захищених зон магазину та підвищення рівня безпеки.

Таким чином, біометричні дані відіграють важливу роль у забезпеченні безпеки, зручності та комфорту в житті людей. Вони можуть бути використані в різних сферах діяльності та принести значні переваги в галузі захисту інформації та особистих даних.

2 СИСТЕМНИЙ АНАЛІЗ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Існує безліч систем біометричної ідентифікації, які використовують різні біологічні параметри для ідентифікації особистості. Деякі з найбільш поширених систем біометричної ідентифікації включають:

- системи розпізнавання особи.
- системи розпізнавання відбитків пальців.
- системи розпізнавання райдужної оболонки ока.
- системи розпізнавання голосу
- системи розпізнавання вен.
- системи розпізнавання DNK.
- системи розпізнавання ходи.

2.1 Системи розпізнавання обличчя

Система розпізнавання обличчя (Facial Recognition System) – це технологія комп'ютерного зору, яка використовується для автоматичного розпізнавання та ідентифікації осіб на зображеннях або відеопотоці. Система розпізнавання обличчя працює шляхом аналізу геометричних особливостей обличчя, таких як відстань між очима, форма та розмір губ, носа та інших фізіологічних особливостей, щоб створити унікальний шаблон обличчя, який можна використовувати для ідентифікації людини.

Системи розпізнавання особи використовуються в різних додатках, таких як системи безпеки, автоматичні системи контролю доступу, системи управління мережею та пристроями, системи моніторингу та управління персоналом, системи визначення віку та статі та ін.

Деякі з основних компонентів системи розпізнавання обличчя включають камери або відеокамери для зйомки зображень обличчя, програмне забезпечення для аналізу та обробки зображень, базу даних для зберігання шаблонів осіб і систему зіставлення для ідентифікації осіб.

Проте, слід зазначити, що системи розпізнавання особи викликають певні етичні та правові питання, пов'язані з конфіденційністю та безпекою даних, порушенням прав особистого життя, та можливістю використання для дискримінації та профілювання.

2.1.1 OpenCV

OpenCV – це бібліотека комп'ютерного зору з відкритим вихідним кодом, яка надає широкий спектр функцій обробки зображень і відео, включаючи розпізнавання осіб. OpenCV була створена в 1999 році групою дослідників з Intel, і з того часу стала однією з найпоширеніших та найпопулярніших бібліотек комп'ютерного зору у світі (логотип – див. рис. 2.1.1).

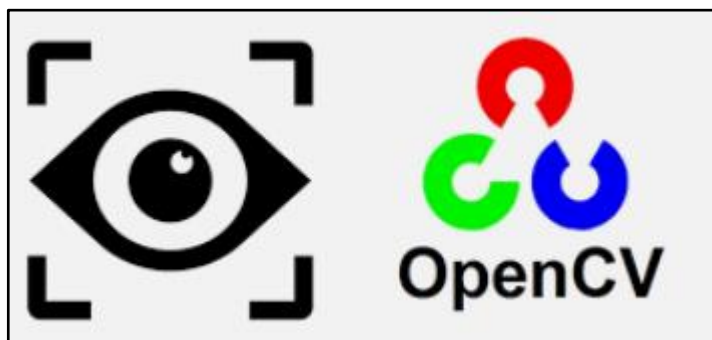


Рисунок 2.1.1 – Логотип «OpenCV»

OpenCV підтримує кілька алгоритмів розпізнавання облич, включаючи Haar Cascade Classifier та Local Binary Patterns Histograms (LBPH). Він також надає можливість для виявлення та отримання ознак обличчя, таких як положення очей, кути губ, форма обличчя та інші.

Однією з головних переваг OpenCV є його безкоштовність та відкритий вихідний код. Це дозволяє розробникам використовувати його для своїх проєктів без необхідності платити за ліцензію. Крім того, OpenCV може працювати на багатьох платформах, включаючи Windows, Linux, MacOS, iOS та Android.

Однак OpenCV має свої недоліки, наприклад, він не завжди дає точний результат при розпізнаванні осіб в умовах з низьким освітленням, або у разі зміни фону або ракурсу зображення. Крім того, OpenCV не має можливості розпізнавати

обличчя в реальному часі на великій кількості камер, що може бути проблемою систем безпеки або управління доступом.

В цілому, OpenCV є потужною та гнучкою бібліотекою комп'ютерного зору, яка може бути використана для реалізації систем розпізнавання облич та інших завдань обробки зображень. Проте, для деяких програм може знадобитися використання більш спеціалізованих програмних рішень.

Бібліотека OpenCV має багато переваг, а також недоліків.

Плюси:

- **Відкритий вихідний код.** Це дозволяє розробникам вивчати, адаптувати та розширювати код бібліотеки під свої потреби, а також ділитися своїми напрацюваннями із спільнотою.
- **Безкоштовність.** OpenCV доступний для використання безкоштовно та не вимагає покупки ліцензій.
- **Кросплатформність.** Бібліотека може працювати на різних платформах, включаючи Windows, Linux, MacOS, iOS та Android.
- **Широкий діапазон функцій.** OpenCV містить велику кількість функцій для обробки зображень та відео, включаючи розпізнавання облич, а також інших завдань комп'ютерного зору, таких як виділення об'єктів, знаходження контурів, визначення кольорів та інших.
- **Швидкість роботи.** OpenCV написана мовою C++, що забезпечує швидкодію та ефективність при обробці великих обсягів даних.

Мінуси:

- **Не завжди точне розпізнавання облич.** OpenCV не завжди дає точний результат при розпізнаванні осіб в умовах з низьким освітленням або у разі зміни фону або ракурсу зображення.
- **Відсутність підтримки GPU.** OpenCV не підтримує розподілені обчислення на графічних процесорах, що може суттєво уповільнювати роботу у разі великих обсягів даних.
- **Недостатня масштабованість.** OpenCV не може розпізнавати обличчя в реальному часі на великій кількості камер, що може бути проблемою

для систем безпеки або управління доступом.

- **Складність використання для новачків.** Для роботи з OpenCV необхідно мати знання мови програмування C++ або Python, що може бути складно для розробників-початківців.

OpenCV також має деякі проблеми, які можуть виникати при її використанні.

Ось деякі з них та можливі шляхи їх вирішення:

- **Необхідність обробки великих обсягів даних.** OpenCV може мати справу з проблемою обробки великих обсягів даних, що може сповільнити роботу програми. Рішення: використання розподілених обчислень на графічних процесорах (GPU), що дозволяють прискорити обробку даних.
- **Низька точність розпізнавання облич в умовах з низьким освітленням або зміненням тлом.** OpenCV не завжди забезпечує точний результат при розпізнаванні осіб в умовах з низьким освітленням або у разі зміни фону або ракурсу зображення. Рішення: використання додаткових алгоритмів обробки зображень, наприклад алгоритмів поліпшення зображення або алгоритмів машинного навчання, для поліпшення точності розпізнавання.
- **Недостатня масштабованість.** OpenCV не може розпізнавати обличчя в реальному часі на великій кількості камер, що може бути проблемою для систем безпеки або управління доступом. Рішення: використання більш потужних обчислювальних систем та/або паралельної обробки даних.
- **Складність використання для новачків.** Для роботи з OpenCV необхідно мати знання мови програмування C++ або Python, що може бути складно для розробників-початківців. Рішення: використання графічних інтерфейсів, які дозволяють працювати з OpenCV без знання мов програмування або навчання мови програмування.
- **Помилки у коді.** При написанні коду на OpenCV можуть бути помилки, що може призвести до неправильної роботи програми. Рішення:

тестування програми на різних умовах та налагодження коду, щоб виявляти та виправляти помилки.

Загалом більшість проблем OpenCV можуть бути вирішені за допомогою використання додаткових алгоритмів обробки зображень, потужніших обчислювальних систем та/або паралельної обробки даних, навчання мови програмування та налагодження коду [6].

2.1.2 Amazon Rekognition

Amazon Rekognition – це хмарний сервіс компанії Amazon для аналізу та обробки зображень та відео. Цей сервіс надає можливості розпізнавання та аналізу осіб, об'єктів і сцен на зображеннях, а також аналізу потоків відео (логотип – див. рис. 2.1.2).



Рисунок 2.1.2 – Логотип «Amazon Rekognition»

Основні можливості Amazon Rekognition включають:

- **Розпізнавання облич:** Amazon Rekognition може розпізнавати та ідентифікувати обличчя на зображеннях та відеофайлах, а також визначати вік, стать та настрій.
- **Розпізнавання об'єктів та сцен:** Amazon Rekognition може розпізнавати об'єкти та сцени на зображеннях та відеофайлах, таких як автомобілі, будівлі та пейзажі.
- **Пошук та індексація зображень:** Amazon Rekognition дозволяє шукати зображення на основі певних критеріїв, таких як особи, об'єкти або сцени.

- **Аналіз потоків відео:** Amazon Rekognition може аналізувати потоки відео в реальному часі для розпізнавання облич і об'єктів, а також для виявлення порушень безпеки.
- **Інтеграція з іншими сервісами Amazon:** Amazon Rekognition може інтегруватися з іншими хмарними сервісами Amazon, такими як Amazon S3 та Amazon Kinesis, для забезпечення ширших можливостей аналізу даних.

Переваги:

- **Висока точність розпізнавання.** Amazon Rekognition використовує технології машинного навчання, щоб забезпечити високу точність розпізнавання об'єктів на зображеннях та відео.
- **Масштабованість.** Сервіс може масштабуватися залежно від потреб клієнта, тому він може бути використаний як невеликими, так і великими компаніями.
- **Розпізнавання облич.** Amazon Rekognition надає можливість розпізнавати обличчя на зображеннях та відео, а також проводити пошук по базі даних облич.
- **Різноманітність функцій.** Сервіс забезпечує виявлення тексту, зображень, різних об'єктів і навіть настрої людей зображення та відео.

Недоліки:

- **Ціни:** Amazon Rekognition може бути дорогим для малих та середніх компаній. Він працює за моделлю оплати за використання, що може стати проблемою для організацій, які працюють з обмеженим бюджетом.
- **Приватність:** Можливість розпізнавання осіб може спричинити проблеми з приватністю, оскільки це може призвести до витоку особистих даних людей.
- **Недостатня якість даних:** Якість зображень та відео може сильно впливати на точність розпізнавання, і якщо зображення не є чіткими та

добре освітленими, це може призвести до неправильного розпізнавання об'єктів та облич.

- **Залежність від хмарної інфраструктури:** Amazon Rekognition є хмарним сервісом, що означає, що він залежить від хмарної інфраструктури Amazon, і це може викликати проблеми, якщо клієнт не має доступу до інтернету або хмарної платформи.

Проблематика Amazon Rekognition полягає в деяких недоліках та обмеженнях, які можуть вплинути на його ефективність та безпеку використання.

Однією з проблем є можливість помилок у розпізнаванні осіб, особливо у випадках, коли зображення є недостатньо чіткими або коли на фотографії присутні кілька людей. Це може призвести до неправильної ідентифікації або відмови у доступі для легітимних користувачів.

Ще однією проблемою є можливість використання технології розпізнавання осіб для незаконних чи шкідливих цілей, таких як стеження, дискримінація чи порушення приватності. Крім того, можливість зберігання та використання великої кількості особистих даних може викликати побоювання щодо безпеки та конфіденційності.

Також важливо враховувати обмеження Amazon Rekognition, пов'язані з доступністю технології в різних країнах та регіонах, а також обмеження на використання в деяких галузях, таких як медицина та правоохоронні органи.

Зрештою, варто враховувати можливі проблеми з етикою та моральністю при використанні технології розпізнавання осіб, особливо якщо вона використовується для контролю та моніторингу громадян. Це може викликати питання щодо порушення прав та свобод людини, а також можливих негативних соціальних та політичних наслідків [7].

2.1.3 Microsoft Face API

Microsoft Face API – це високорівневий сервіс розпізнавання облич, що надається Microsoft Azure. Він використовує комплексні алгоритми машинного навчання та глибокого навчання для аналізу зображень та розпізнавання осіб на

фотографіях та відео. Цей сервіс дозволяє розробникам швидко та легко інтегрувати функції розпізнавання осіб у свої програми та послуги (логотип – див. рис. 2.1.3).

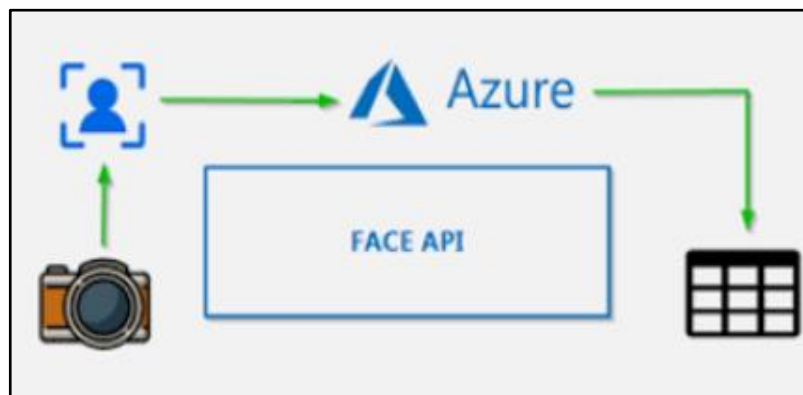


Рисунок 2.1.3 – Логотип «Microsoft Face API»

Основні можливості Microsoft Face API включають:

- Розпізнавання облич: Microsoft Face API може розпізнавати обличчя на зображеннях та відео та аналізувати їх характеристики, такі як вік, стать, настрій та аксесуари.
- Ідентифікація осіб: Сервіс також дозволяє ідентифікувати особи та зіставляти їх із заздалегідь визначеними базами даних осіб. Це може бути корисним, наприклад, для систем контролю доступу, систем управління рекламою та багато інших.
- Визначення розташування осіб: Microsoft Face API може визначати розташування обличчя на зображенні та вказувати його точні координати.
- Аналіз зображень: Сервіс дозволяє аналізувати фотографії та відео на наявність різних об'єктів та ознак, таких як наявність людей, настрій, вік та стать.
- Інтеграція з Azure: Microsoft Face API може бути легко інтегрована з іншими сервісами Azure, такими як Azure Cognitive Services та Azure Machine Learning.

Крім того, Microsoft Face API забезпечує високу точність та швидкість розпізнавання, підтримку кількох мов програмування та платформ, а також високий рівень безпеки та конфіденційності.

Плюси:

- Висока точність розпізнавання облич, особливо у випадках із низькою якістю зображень чи відео.
- Підтримує розпізнавання кількох облич на одному зображенні.
- Має API, який дозволяє розробникам інтегрувати його у свої програми та послуги.
- Підтримує різні мови програмування, такі як C#, Java, Python та інші.
- Має можливість визначення віку, статі, настрою та інших характеристик особи.
- Надає можливість створення власних баз даних для розпізнавання.
- Мінуси:
- Платний сервіс, хоча є безкоштовний період для тестування.
- Працює лише у хмарному середовищі, що може бути небажаним для деяких користувачів через потенційні проблеми з конфіденційністю даних.
- Не підтримує розпізнавання реального часу на пристроях з обмеженими обчислювальними потужностями.

Проблематика:

- Деякі користувачі можуть побоюватися, що використання хмарних сервісів може призвести до витоку конфіденційних даних.
- Можливі помилки при розпізнаванні облич, особливо при сильній зміні зовнішності або освітлення на зображенні.
- Деякі функції можуть бути недоступні в деяких регіонах через обмеження урядових органів.

Вирішення проблем:

- Щоб зменшити побоювання щодо конфіденційності даних, можна

використовувати методи шифрування та анонімізації даних перед надсиланням їх на сервери Microsoft.

- Для покращення точності розпізнавання можна використовувати додаткові алгоритми та методи, такі як глибоке навчання та машинне навчання.
- Для доступу до деяких функцій в обмежених регіонах можна використовувати VPN або інші технології обходу блокування.

2.1.4 FaceSDK

FaceSDK – це набір інструментів для розробки програм, які використовують біометричне розпізнавання облич. Він розроблений компанією Luxand Inc. та дозволяє виконувати такі завдання, як ідентифікація осіб, розпізнавання емоцій, визначення віку та статі, а також створення 3D-моделей осіб (логотип – див. рис. 2.1.4).



Рисунок 2.1.4 – Логотип « FaceSDK »

Деякі можливості, що надаються FaceSDK, включають:

- Розпізнавання облич на зображеннях та відео
- Визначення статі та віку особи
- Визначення настрою та емоцій
- Розпізнавання унікальних характеристик, таких як вуса, борода, окуляри, волосся.

Ідентифікація особи у базі даних

FaceSDK має високу точність розпізнавання та працює з різними форматами зображень та відео, такими як JPEG, PNG, BMP, AVI, WMV, MOV та інші. SDK також підтримує різні мови програмування, такі як C++, .NET, Java, Python та інші.

Крім того, FaceSDK надає додаткові функції, такі як порівняння осіб, пошук найбільш схожих осіб, автоматичну обробку та вирівнювання зображень для покращення точності розпізнавання.

Загалом, FaceSDK є гнучким інструментом для роботи із зображеннями та відео, пов'язаними з особами, який може використовуватись у широкому спектрі додатків, включаючи безпеку, моніторинг та управління контентом.

FaceSDK має такі переваги:

- **Висока точність розпізнавання:** FaceSDK забезпечує високу точність розпізнавання обличчя завдяки використанню сучасних алгоритмів машинного навчання.
- **Багатий набір функцій:** FaceSDK пропонує широкий спектр функцій, включаючи розпізнавання осіб, визначення віку та статі, розпізнавання емоцій, визначення наявності та розташування очей та багато інших.
- **Гнучкість і налаштуваність:** FaceSDK має гнучку і конфігурацію, що налаштовується, що дозволяє налаштовувати параметри алгоритмів розпізнавання для отримання максимальної точності і швидкості.
- **Кросплатформенність:** FaceSDK може бути використаний на різних платформах, включаючи Windows, Linux, MacOS, iOS та Android.
- **Легкість використання:** FaceSDK має простий і інтуїтивно зрозумілий інтерфейс програмування додатків (API), що полегшує розробку додатків, що використовують функціональність біометричної ідентифікації.

Однак, у FaceSDK також є деякі недоліки:

- **Висока вартість:** FaceSDK є комерційним продуктом і його використання вимагає оплати ліцензійних платежів.
- **Вимоги до ресурсів:** FaceSDK споживає значні ресурси комп'ютера, особливо при роботі з великими обсягами даних або додатками з

високим навантаженням.

- **Необхідність навчання моделі:** для досягнення найкращих результатів необхідно навчити модель на конкретних даних, що може вимагати додаткових витрат часу та ресурсів.

Проблематика FaceSDK полягає в тому, що він є комерційним продуктом, який вимагає ліцензування для використання, а також вимогливий до ресурсів комп'ютера. Однак ці проблеми можуть бути вирішені шляхом оптимізації роботи з ресурсами та покращення алгоритмів розпізнавання. Крім того, для покращення точності розпізнавання необхідно навчати модель на конкретних даних.

Для вирішення проблем, пов'язаних з використанням FaceSDK, можна запропонувати кілька способів:

1. **Оптимізація продуктивності:** для покращення швидкості обробки зображень та зниження навантаження на процесор можна використовувати спеціалізовані процесори, такі як графічні процесори (GPU) або процесори для машинного навчання (TPU).
2. **Поліпшення точності розпізнавання:** для збільшення точності розпізнавання можна використовувати комбінацію кількох методів, таких як використання кількох моделей навчання, покращення якості вихідних зображень, а також обробку більшої кількості даних під час навчання моделі.
3. **Розробка нових алгоритмів:** для вирішення проблем, пов'язаних із розпізнаванням осіб в умовах поганого висвітлення, зміни положення голови та інших факторів, можна розробляти нові алгоритми, які ефективно працюватимуть в таких умовах.
4. **Підвищення безпеки:** для захисту даних користувачів та запобігання можливості використання розпізнавання осіб для незаконних цілей необхідно забезпечити надійну аутентифікацію та авторизацію користувачів при доступі до системи. Також можна використовувати алгоритми, які не зберігають зображення користувачів на сервері та запобігають можливості їх крадіжки або використання в незаконних

цілях.

5. **Вирішення проблем із конфіденційністю:** для покращення захисту конфіденційності користувачів можна використовувати методи анонімізації даних, такі як заміна ідентифікаційних номерів випадковими значеннями або використання методів шифрування при передачі даних. Також важливо дотримуватись вимог до захисту персональних даних відповідно до законодавства [8].

2.2 Системи розпізнавання відбитків пальців

Системи розпізнавання відбитків пальців (Fingerprint Recognition Systems) використовуються для ідентифікації та автентифікації особи на основі унікальних фізіологічних характеристик відбитків пальців. Ці системи використовуються для різних цілей, таких як доступ до комп'ютерів, мобільних пристроїв, будівель, сейфів і т.д.

Основними компонентами системи розпізнавання відбитків пальців є сенсор, який захоплює зображення відбитка пальця, та програмне забезпечення, яке обробляє зображення та визначає, чи відповідає відбиток пальця відомому шаблону чи ні.

2.2.1 VeriFinger

VeriFinger – це програмне забезпечення для розпізнавання відбитків пальців, розроблене компанією Neurotechnology. Воно дозволяє швидко і точно ідентифікувати людину за її унікальним відбитком пальця і може використовуватися для автоматичної ідентифікації на підприємствах, в урядових установах, на кордонах та інших областях, де потрібний високий ступінь безпеки (логотип – див. рис. 2.2.1).



Рисунок 2.2.1 – Логотип « VeriFinger »

VeriFinger використовує найсучасніші алгоритми для обробки відбитків пальців та має високу швидкість та точність розпізнавання. Він може працювати з різними типами сканерів відбитків пальців та підтримує широкий діапазон форматів зображень.

- Серед можливостей VeriFinger можна виділити:
- Висока точність розпізнавання відбитків пальців;
- Підтримка великої кількості сканерів відбитків пальців;
- Робота із широким діапазоном форматів зображень;
- Підтримка 1:1 та 1:N зіставлення відбитків пальців;
- Швидке та ефективне зіставлення великих баз даних відбитків пальців.

Незважаючи на те, що VeriFinger є досить надійною системою для розпізнавання відбитків пальців, у неї все ж таки є кілька проблем, які можуть вплинути на її роботу:

- **Якість відбитків пальців:** VeriFinger вимагає високої якості відбитків пальців для надійного розпізнавання, що може бути проблемою, якщо відбиток пальця був пошкоджений або засмічений.
- **Неоднорідність відбитків пальців:** у різних людей відбитки пальців можуть мати різну форму, розмір та структуру, що може знизити точність розпізнавання.
- **Інтеграція з іншими системами:** для використання VeriFinger разом з іншими системами можуть бути потрібні додаткові налаштування, що може зайняти деякий час і вимагати додаткових ресурсів.

- **Вартість:** VeriFinger є платним програмним забезпеченням, що може бути проблемою для компаній з обмеженим бюджетом.
- **Конфіденційність даних:** при використанні VeriFinger для збору та зберігання біометричних даних може бути проблема з конфіденційністю та безпекою цих даних.

Для вирішення цих проблем рекомендується забезпечити високу якість збору відбитків пальців, використовувати додаткові методи аутентифікації, такі як паролі або PIN-коди, а також забезпечити безпеку та конфіденційність даних при збиранні та зберіганні біометричних даних. Також можна розглянути використання інших систем розпізнавання відбитків пальців із покращеною точністю та швидкістю роботи.

Розглянемо кілька можливих способів вирішення проблем, пов'язаних із VeriFinger:

- Використання якісніших сенсорів відбитків пальців. Однією з основних проблем VeriFinger є низька якість сканування відбитків пальців, що може призвести до помилок у процесі ідентифікації. Встановлення більш якісних сенсорів дозволить отримувати чіткіші зображення відбитків пальців, що покращить точність ідентифікації.
- Поліпшення алгоритмів обробки даних. Однією з основних проблем, пов'язаних з VeriFinger є висока ймовірність помилок при обробці даних. Для поліпшення точності ідентифікації необхідно розробити точніші алгоритми обробки даних, які будуть здатні визначати відбитки пальців з більшою точністю.
- Використання додаткових методів ідентифікації. Якщо точність ідентифікації за допомогою VeriFinger залишає бажати кращого, можна використовувати додаткові методи ідентифікації, наприклад, розпізнавання обличчя або голосу. Це дозволить підвищити точність ідентифікації, зменшити ймовірність помилок та знизити кількість помилкових спрацьовувань.
- Використання досконаліших систем розпізнавання. В даний час

існують більш досконалі системи розпізнавання відбитків пальців, наприклад AFIS (Automated Fingerprint Identification System). AFIS використовує точніші алгоритми обробки даних і дозволяє ідентифікувати відбитки пальців з більшою точністю, ніж VeriFinger. Перехід на AFIS може бути одним із способів вирішення проблем, пов'язаних із VeriFinger.

Для підвищення безпеки використання VeriFinger рекомендується застосовувати сучасні методи шифрування для захисту даних під час зберігання та передачі, а також забезпечувати фізичну безпеку обладнання, на якому запущено VeriFinger. Також важливо проводити навчання користувачів правилам безпечного використання системи та біометричних даних загалом [9].

2.2.2 Fingerprint SDK

BioEnable – це компанія, яка розробляє та постачає технології біометричної ідентифікації, такі як системи розпізнавання відбитків пальців, осіб, судин пальців тощо. Компанія була створена в 2001 році в Індії та має широкий спектр продуктів та рішень, пов'язаних з біометричною ідентифікацією.

Один із продуктів BioEnable – це програмне забезпечення для збору та аналізу відбитків пальців під назвою "Fingerprint SDK".

Fingerprint SDK – це програмне забезпечення, розроблене для систем біометричної ідентифікації на основі відбитків пальців. Fingerprint SDK надає розробникам API для інтеграції системи розпізнавання відбитків пальців у їхні програми (логотип – див. рис. 2.2.2).



Рисунок 2.2.2 – Логотип « Fingerprint SDK »

Основні можливості Fingerprint SDK включають:

- Розпізнавання відбитків пальців у режимі реального часу
- Ідентифікація кількох користувачів одночасно
- Підтримка різних типів сканерів відбитків пальців
- Зберігання відбитків пальців у зашифрованому вигляді
- Підтримка кількох мов програмування, як-от C++, C#, Java, VB.NET

Його основними перевагами є:

Плюси:

- **Висока точність розпізнавання.** Fingerprint SDK використовує алгоритми, які дозволяють досягти високої точності розпізнавання відбитків пальців.
- **Гнучкість та налаштовуваність.** ПЗ дозволяє налаштовувати різні параметри розпізнавання, що робить його гнучким та здатним працювати з різними типами сенсорів.
- **Широкий спектр застосування:** Fingerprint SDK може використовуватися в різних галузях, включаючи керування доступом, системи контролю часу та присутності, онлайн-платежі тощо.
- **Простота у використанні:** Fingerprint SDK має зручний інтерфейс і простий у використанні, що дозволяє розробникам швидко створювати програми, що використовують біометричну ідентифікацію.

Мінуси:

- **Обмежені можливості аналізу відбитків пальців.** незважаючи на те, що Fingerprint SDK може зчитувати відбитки пальців, він може мати труднощі при роботі з нестандартними відбитками або відбитками, отриманими в умовах, відмінних від стандартних.
- **Низька точність розпізнавання:** у деяких випадках Fingerprint SDK може припускатися помилок у розпізнаванні відбитків пальців. Це може призвести до того, що система розпізнає невірну особу та допустить несанкціонований доступ.
- **Неповний захист від шахрайства:** деякі користувачі можуть спробувати обдурити систему, представивши нереальний відбиток пальця або за допомогою інших методів обману. Fingerprint SDK не завжди може виявляти такі спроби шахрайства.
- **Проблеми сумісності:** Fingerprint SDK може мати проблеми сумісності з деякими пристроями та операційними системами, що може зробити його марним у деяких ситуаціях.
- **Обмежена функціональність:** Fingerprint SDK має обмежений функціонал у порівнянні з іншими системами розпізнавання відбитків пальців. Це може обмежити можливості використання системи в деяких програмах.

Для вирішення цих проблем можна використовувати такі підходи:

1. Використання більш просунутих алгоритмів аналізу відбитків пальців збільшення точності розпізнавання.
2. Розробка методів додаткової аутентифікації, які можуть бути використані для підвищення безпеки системи та запобігання спробам шахрайства.
3. Проводить більш ретельне тестування системи на різних пристроях та операційних системах для забезпечення сумісності.
4. Додавання нових функцій та можливостей у Fingerprint SDK, щоб збільшити його функціональність та забезпечити його використання у ширшому діапазоні додатків.

2.2.3 DigitalPersona

DigitalPersona – це програмне забезпечення для біометричної аутентифікації, яке дозволяє розпізнавати відбитки пальців і використовувати їх для ідентифікації користувачів. DigitalPersona була заснована в 1996 році і на даний момент є однією з найбільш відомих та застосовуваних систем у світі.

DigitalPersona надає ряд функцій, включаючи:

- Реєстрація користувачів та їх відбитків пальців;
- Зберігання відбитків пальців у базі даних для подальшої ідентифікації;
- Ідентифікація користувачів на основі їх відбитків пальців у режимі реального часу;
- Аутентифікація користувачів на основі їх відбитків пальців у системах безпеки та контролю доступу.

DigitalPersona має такі переваги:

- Висока точність розпізнавання відбитків пальців;
- Підтримка множини алгоритмів розпізнавання відбитків пальців;
- використання захищених протоколів зв'язку для передачі даних;
- Можливість інтеграції з іншими системами безпеки та контролю доступу.

Однак у DigitalPersona є й недоліки:

- Вимогливість до апаратного забезпечення;
- Обмеженість у можливості працювати з великою кількістю користувачів;
- Необхідність наявності високошвидкісного інтернет-з'єднання для обміну даними;
- Висока вартість.

Проблематика DigitalPersona пов'язана з обмеженнями, які є у поточній версії системи. Наприклад, неможливість роботи з великою кількістю користувачів або недостатня точність розпізнавання відбитків пальців за певних умов. Для вирішення цих проблем можна застосовувати такі способи:

- використання більш сучасних алгоритмів розпізнавання відбитків пальців;
- Поліпшення апаратної частини системи для підвищення точності та швидкості роботи;
- Впровадження додаткових методів ідентифікації, наприклад, розпізнавання голосу чи сканування особи;
- Підвищення рівня безпеки системи за рахунок використання криптографічних протоколів та захищених каналів передачі даних.

2.2.4 RealScan

RealScan – це біометрична система, призначена для збирання та аналізу відбитків пальців. Вона була розроблена компанією Suprema, яка є одним із лідерів у галузі біометричних технологій (логотип – див. рис. 2.2.4).



Рисунок 2.2.4 – Логотип «RealScan»

Основні можливості RealScan включають:

- швидке та точне сканування відбитків пальців;
- високу швидкість обробки та зіставлення даних;
- підтримку стандартних протоколів та інтерфейсів для інтеграції з іншими системами;
- можливість використання у різних секторах, включаючи державні установи, фінансові установи, компанії тощо.

Система також забезпечує високий рівень безпеки та захисту даних, що робить її привабливою для використання в критичних програмах, таких як контроль доступу або автентифікація користувачів.

Одним із недоліків RealScan є його вартість, яка може бути значно вищою, ніж у інших систем розпізнавання відбитків пальців. Крім того, для роботи системи необхідна наявність спеціалізованого обладнання, що може бути проблематичним у випадку, якщо потрібно використовувати систему на великій кількості пристроїв.

RealScan, як і будь-яка технологія, має свої проблеми та обмеження. Деякі з них включають:

- **Якість відбитків пальців.** Якість відбитків пальців може змінюватись в залежності від умов збору, таких як погане освітлення, вологість, відбитки пальців, що затверділи і т.д. Це може призвести до того, що сканер не зможе розпізнати відбитки пальців або помилковий результат.
- **Проблеми з чутливістю сканера:** Деякі сканери відбитків пальців можуть не бути достатньо чутливими для збирання відбитків пальців у деяких людей. Це може призвести до того, що сканер не зможе зібрати якісний відбиток пальця для розпізнавання.
- **Сумісність з програмним забезпеченням:** Деякі сканери відбитків пальців можуть мати проблеми із сумісністю з певним програмним забезпеченням, що може призвести до проблем при використанні сканера разом з цим програмним забезпеченням.
- **Захист від шахрайства:** Сканери відбитків пальців можуть бути обдурені під час використання липких папірців, латексних поверхонь або інших матеріалів для створення підроблених відбитків пальців. Це може призвести до шахрайства в системах, які використовують сканери відбитків пальців.
- **Приватність та безпека:** Збирання та зберігання відбитків пальців може бути ризикованим у сенсі приватності та безпеки. У разі витоку або несанкціонованого доступу до цієї інформації може статися витік

конфіденційних даних та порушення правил конфіденційності.

Загалом ці проблеми можуть обмежити ефективність та безпеку систем розпізнавання відбитків пальців, тому розробники та виробники постійно працюють над покращенням технології та вирішенням цих проблем.

2.3 Системи розпізнавання райдужної оболонки ока

Системи розпізнавання райдужної оболонки ока – це технологія біометричної ідентифікації, яка заснована на аналізі унікальних фізіологічних характеристик райдужної оболонки ока, таких як її текстура, колір, шаблон вен. Ці характеристики є унікальними для кожної людини і можуть бути використані для створення унікального біометричного шаблону, який може бути використаний для ідентифікації особистості.

Система має досить високу точність ідентифікації особистості, швидкий процес ідентифікації, унікальність фізіологічних характеристик райдужки ока. Але при всіх цих плюсах для системи потрібне спеціальне обладнання для сканування, потрібна близька відстань сканування між пристроєм та оком, що може викликати дискомфорт користувачу. Також ця система має недолік що до можливих фізіологічних змін користувача, при захворюваннях ока або старінні.

Проблематика, пов'язана з використанням технології розпізнавання райдужки ока, включає можливість виникнення помилок при зборі зображень райдужки ока, а також можливість обману системи при використанні фотографій або інших підроблених зображень. Для вирішення цих проблем можуть бути використані методи біометричної автентифікації на основі мультимодальних систем, що комбінують кілька методів ідентифікації, таких як райдужка ока та відбиток пальця. Крім того, такі системи можуть бути покращені шляхом використання алгоритмів

2.3.1 IrisID

Одним з найбільш відомих програм для розпізнавання райдужки ока є IrisID. Це програмне забезпечення використовується для розпізнавання райдужки ока в різних областях, таких як безпека, контроль доступу та державні служби.

IrisID – це технологічна компанія, що спеціалізується на системах біометричної ідентифікації на основі розпізнавання райдужної оболонки ока. Компанія була заснована в 1997 році і з тих пір є одним з провідних виробників технології розпізнавання райдужної оболонки ока (логотип – див. рис. 2.3.1).



Рисунок 2.3.1 – Логотип «IrisID»

Одним з найбільш популярних продуктів IrisID є система iCAM, яка включає в себе апаратне забезпечення та програмне забезпечення для збору зображень райдужної оболонки ока та проведення ідентифікації. Система iCAM складається з камери, плати захоплення зображення, програмного забезпечення та алгоритмів зіставлення, які використовуються для порівняння зображення райдужної оболонки ока з попередньо збереженими шаблонами. Камера iCAM використовує інфрачервоне освітлення для отримання зображення райдужки ока без використання флеш-освітлення, що робить процедуру комфортнішою для користувача. iCAM підтримує кілька режимів роботи, включаючи одиночне захоплення зображення, безперервний режим та режим сканування, що дозволяє сканувати групи людей з метою ідентифікації.

Однією з переваг iCAM є висока точність розпізнавання райдужки ока. Крім того, система може працювати в широкому діапазоні умов освітлення і навіть в

умовах поганої видимості, наприклад, при носінні окулярів, контактних лінз або наявності ушкоджень ока. Вона також має швидкий час відповіді, що дозволяє швидко перевіряти особистість у реальному часі. Система iCAM зараз використовується в багатьох галузях, включаючи державні установи, банківську сферу, промисловість та транспорт.

Незважаючи на те, що системи розпізнавання райдужки ока, такі як IrisID, мають високу точність і надійність, вони також стикаються з низкою проблем.

Однією з головних проблем є складність використання системи. Для розпізнавання райдужної оболонки очі потрібне гарне освітлення, правильна відстань від пристрою та стійка поза голови. Це може бути проблематичним для користувачів, особливо якщо система використовується в мобільних пристроях.

Крім того, в деяких випадках система може не розпізнати райдужку ока, що призводить до помилкових негативних результатів. Це може бути пов'язане з температурою, освітленням або станом ока (наприклад, при наявності контактних лінз або запалення ока).

Іншою проблемою може бути приватність даних. Оскільки система використовує біометричні дані користувача для розпізнавання, можливо, що дані можуть бути скомпрометовані або використані без дозволу користувача.

Нарешті, вартість системи розпізнавання райдужної оболонки ока також може бути проблемою, особливо для малих і середніх компаній або для приватних осіб.

Однак, багато з цих проблем можуть бути вирішені шляхом покращення технології, розробки нових методів розпізнавання та захисту даних користувачів[10].

3 ВИРІШЕННЯ ПРОБЛЕМ І ПОКАЩЕННЯ СИСТЕМИ ІДЕНТИФІКАЦІЇ ТА БЕЗПЕКИ ЗБЕРІГАННЯ БІОМЕТРИЧНИХ ДАНИХ

Проаналізувавши системи та програмні засоби біометричної ідентифікації, головною проблемою є можливість зламування та крадіжки цих даних. Збереження біометричних даних потребує високого рівня захисту, оскільки якщо такі дані потраплять у руки зловмисників, то користувач може стати жертвою шахрайства, викрадення особистості та інших злочинів. Крім того, існує ризик того, що система ідентифікації може неправильно ідентифікувати особу через технічні проблеми з читанням біометричних даних, таких як помилки в розпізнаванні обличчя, відбитку пальця або розпізнаванні голосу. Крім того, відсутність стандартизації біометричних даних може стати перешкодою в інтеграції різних систем ідентифікації та породити технічні проблеми при їх використанні.

3.1 IDEF0 діаграми та її використання

IDEF0 (Integration Definition for Function Modeling) – це методологія моделювання бізнес-процесів, яка використовується для аналізу та проектування інформаційних систем та бізнес-процесів. IDEF0 була розроблена у 1981 році як частина програми CALS (Computer-Aided Acquisition and Logistics Support), яка мала на меті покращення процесу придбання та логістики військової техніки.

IDEF0 була розроблена з метою спрощення та стандартизації процесу аналізу та проектування бізнес-процесів. Вона дозволяє створювати графічні моделі, що зображають функції, що виконуються в процесі, та їх взаємодію.

IDEF0 стала популярною в управлінні бізнесом та проектуванні інформаційних систем, оскільки дозволяє спростити складні процеси та зменшити кількість помилок в проектуванні. Вона використовується у великих компаніях та урядових структурах для аналізу бізнес-процесів та проектування нових інформаційних систем.

Застосування IDEF0 діаграм допомагає визначити області для подальшого удосконалення, відслідковувати процес взаємодії компонентів системи і зрозуміти, які елементи можуть бути оптимізовані. Ці діаграми часто використовуються в

інженерній діяльності для моделювання різних процесів, включаючи технічне проектування, управління проектами, бізнес-аналіз і т.д.

Однією з головних переваг IDEF0 діаграм є те, що вона дозволяє детально вивчити процес взаємодії елементів системи, відображає їх ієрархічну структуру, а також чітко показує вхідні та вихідні дані для кожної операції. Крім того, ця діаграма дозволяє легко ідентифікувати недоліки та слабкі місця в процесах системи та пропонувати варіанти їх вирішення.

Іншим важливим перевагою IDEF0 є те, що вона є стандартизованою діаграмою, що дозволяє її легко інтерпретувати та використовувати для комунікації між різними відділами та експертами.

Нарешті, IDEF0 діаграми дозволяють використовувати різні рівні деталізації для різних аудиторій. Наприклад, вони можуть використовуватися для забезпечення загального уявлення про процес для керівництва компанії або детальніше вивчити процес для інженерів та технічного персоналу.

3.2 Безпека зберігання біометричних даних та її покращення

Щоб уникнути крадіжки або неправильного сканування біометричних даних користувачів, розглянутих ПЗ та наведених систем біометрії на момент аналізу теми ідентифікації, треба розробити нову систему яка покращить сканування, захист та зберігання інформації в базі даних, поліпшить та зробить роботу приборів сканування більш чіткішим та швидким.

Отже, розглядаючи дані системи, проблематику, враховуючи всі недоліки та переваги програмних пристроїв, додатків та засобів зберігання інформації, була створена модель (інструкція) в форматі IDEF0 діаграми з чіткими та доцільними методами та засобами покращення системи зберігання даних.

В ході дослідження та детального аналізу біометричної ідентифікації було створено опис системи посилення безпеки зберігання біометричних даних користувачів використовуючи вхідні та вихідні данні, функції та механізми (див.рис.3.3.1).

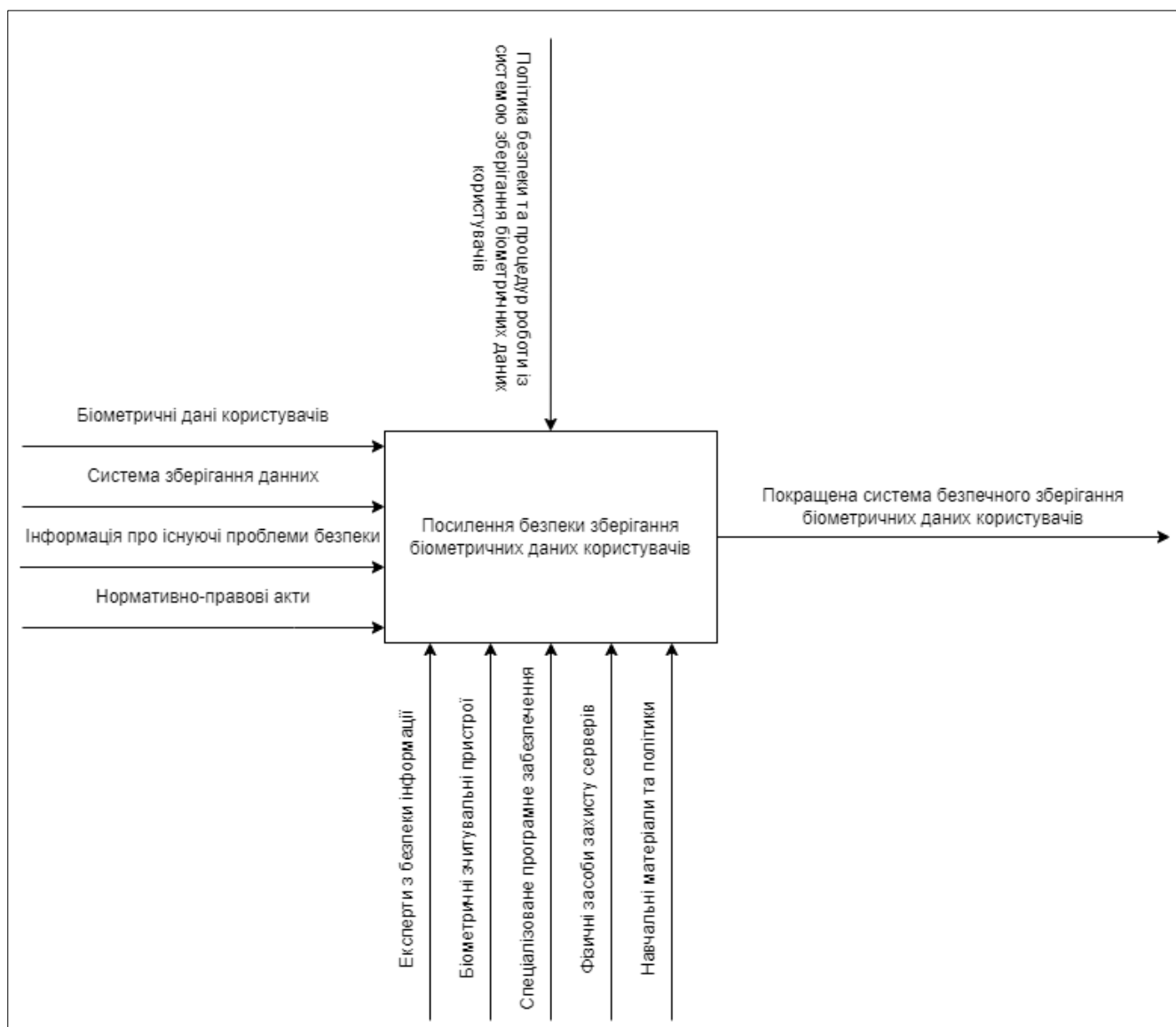


Рисунок 3.3.1 – Модель «Посилення безпеки зберігання біометричних даних користувачів»

A0:Посилення безпеки зберігання біометричних даних користувачів

Комірка IDEF0 діаграми описує загальну мету процесу з удосконалення безпеки зберігання біометричних даних користувачів. У контексті цієї комірки, під посиленням безпеки розуміється вдосконалення існуючої системи зберігання біометричних даних шляхом впровадження додаткових заходів захисту, які зменшують ймовірність несанкціонованого доступу до цих даних та забезпечать їх безпеку та конфіденційність. Крім того, в процесі удосконалення безпеки зберігання біометричних даних користувачів, можуть бути визначені додаткові вимоги до зберігання та передачі цих даних, а також можуть бути внесені зміни до

процедур їх обробки та використання. Кінцевою метою процесу є підвищення рівня безпеки та довіри користувачів до системи зберігання їх біометричних даних.

Вхід:

1. **Біометричні дані користувачів.** Включає унікальні біологічні характеристики або особисті ідентифікатори, такі як відбитки пальців, розпізнавання обличчя, голосові зразки тощо. Ці дані використовуються для ідентифікації та аутентифікації користувачів.
2. **Система зберігання даних.** Включає апаратне та програмне забезпечення, що використовується для зберігання біометричних даних користувачів. Ця система може включати базу даних, сервери, системи шифрування та інші технології для забезпечення безпеки та цілісності даних.
3. **Інформація про існуючі проблеми безпеки.** Вона включає в себе докладні відомості про поточні загрози, ризики та вразливості, пов'язані зі зберіганням біометричних даних. Ця інформація може бути отримана шляхом аналізу попередніх інцидентів, досліджень безпеки або відповідних статистичних даних.
4. **Нормативно-правові акти.** Включає законодавчі та регуляторні вимоги, які стосуються зберігання біометричних даних. Ці нормативно-правові акти є як правила про конфіденційність даних, захист персональних даних, обов'язкові вимоги щодо безпеки тощо.

Вихід:

Покращена система зберігання даних. Вдосконалення апаратного та програмного забезпечення, що використовується для зберігання біометричних даних користувачів. Можуть бути внесені зміни до системи баз даних, серверів, методів шифрування, механізмів аутентифікації та інших технологій для поліпшення безпеки та надійності збереження даних.

Механізми A0:

- **Експерти з безпеки інформації.** Фахівці з безпеки, які володіють знаннями та досвідом у галузі захисту даних. Вони виконують аналіз загроз, розробляють стратегії безпеки, проводять аудит безпеки та надають рекомендації щодо покращення системи зберігання біометричних даних.
- **Біометричні зчитувальні пристрої.** Це пристрої, які використовуються для збору біометричних даних користувачів. Вони можуть включати сканери відбитків пальців, камери для розпізнавання обличчя, пристрої для голосового визнання тощо. Ці зчитувальні пристрої забезпечують точність та надійність збору біометричних даних.
- **Спеціалізоване програмне забезпечення.** Програми, розроблені для забезпечення безпеки та ефективного управління біометричними даними. Вони можуть включати модулі шифрування, автентифікації, контролю доступу, моніторингу безпеки та аудиту. Це програмне забезпечення допомагає забезпечити конфіденційність та цілісність біометричних даних.
- **Фізичні засоби захисту серверів.** Призначені для забезпечення фізичної безпеки серверів, на яких зберігаються біометричні дані. Це можуть бути спеціально обладнані серверні приміщення з контролем доступу, системи пожежної безпеки, системи контролю температури та вологості, фізичні заходи для захисту від несанкціонованого доступу, такі як замки, сейфи тощо.
- **Навчальні матеріали та політики:** Це документи та матеріали, які надають інструкції та рекомендації щодо безпеки зберігання біометричних даних. Навчальні матеріали можуть включати посібники, курси навчання, тренінги, які надають персоналу інформацію про найкращі практики безпеки та процедури реагування на потенційні загрози. Політики встановлюють правила та стандарти щодо безпеки,

включаючи правила паролів, обмеження доступу, шифрування даних та інші безпечні практики, які повинні дотримуватись.

Управління A0:

Визначення політики безпеки. Це процес формулювання документів, які встановлюють правила, процедури і вимоги щодо безпеки зберігання біометричних даних. В цих документах можуть бути визначені положення про доступ до системи, рівні авторизації, вимоги до паролів, обмеження доступу, зберігання резервних копій, політика використання шифрування та інші безпечні практики.

Розробка процедур роботи. Це встановлення чітких і докладних інструкцій та процедур для роботи з системою зберігання біометричних даних. Ці процедури можуть включати створення облікових записів користувачів, управління доступом до даних, аудит безпеки, моніторинг і виявлення потенційних загроз, реагування на інциденти безпеки та інші процеси, які сприяють безпеці даних.

Застосування політики та процедур. Це виконання встановлених політик та процедур безпеки зберігання біометричних даних. Це включає навчання персоналу, щоб вони були ознайомлені з політиками та процедурами, регулярне оновлення політик та процедур з урахуванням змін в технологіях та загрозах безпеки, а також контроль і виконання вимог безпеки.

2.2.4 Декомпозиція моделі IDEF0 діаграми

До даної моделі «Посилення безпеки зберігання біометричних даних користувачів», була створена детальна декомпозиція в форматі IDEF0 діаграми, в якій детально розглядені та описані функції, вхідні та вихідні дані, механізми, етапи розвитку та створення покращеної системи (див.рис.3.3.2).

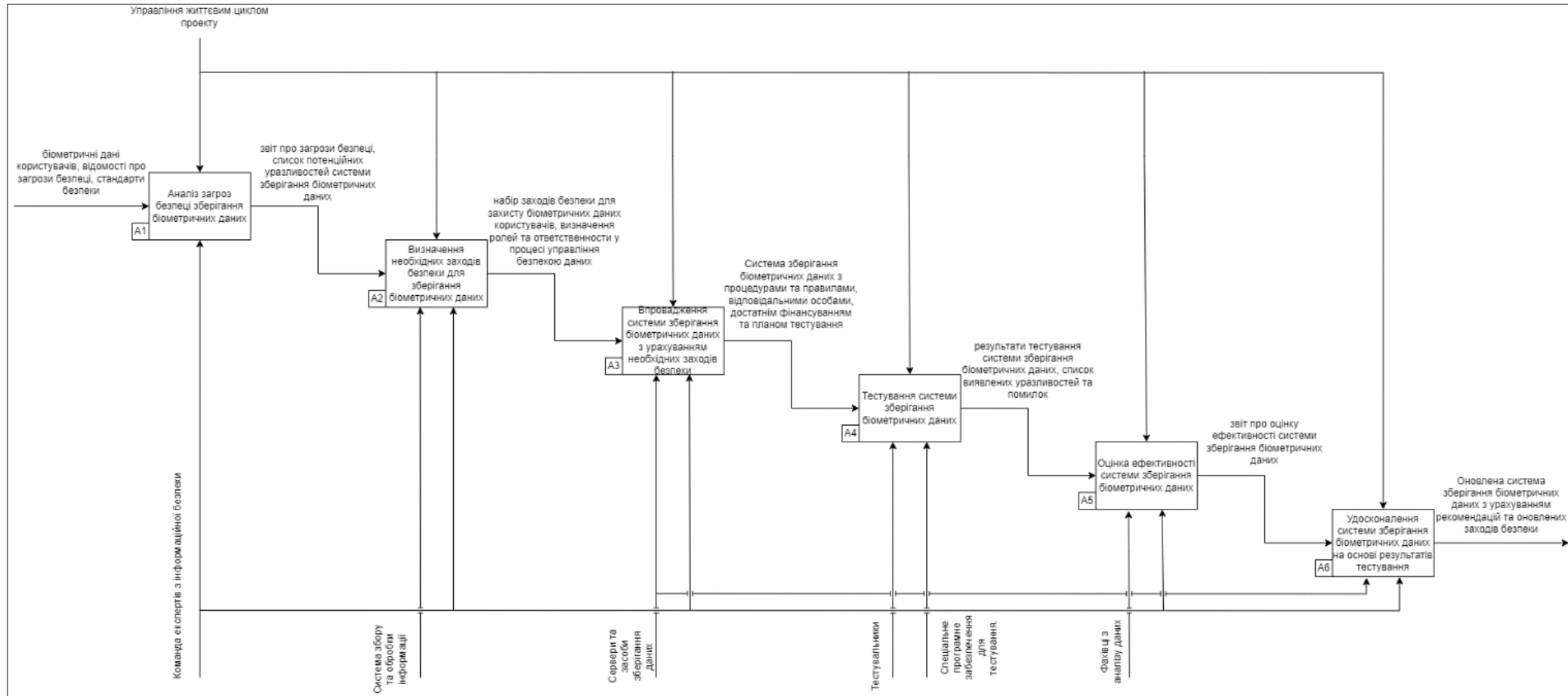


Рисунок 3.3.2 – Декомпозиція моделі «Посилення безпеки зберігання біометричних даних користувачів»

A1: Аналіз загроз безпеці зберігання біометричних даних

Описується перший крок процесу з посилення безпеки зберігання біометричних даних користувачів. Цей крок передбачає аналіз потенційних загроз безпеці зберігання біометричних даних та визначення можливих наслідків їх реалізації. У цьому кроці важливо зрозуміти, які загрози можуть настати та які можливі шляхи їх уникнення. Наприклад, можуть бути загрози такі, як несанкціонований доступ до баз даних, атаки з використанням вірусів або іншого шкідливого програмного забезпечення, псування даних тощо.

У комірці описується процес збору та аналізу інформації щодо потенційних загроз та їх наслідків для зберігання біометричних даних. В результаті цього аналізу визначаються можливі шляхи запобігання загрозам та заходи для підвищення безпеки зберігання біометричних даних.

Вхід:

Біометричні дані користувачів. Це інформація, яка ідентифікує користувачів на основі їх біологічних характеристик, таких як відбитки пальців, райдужна оболонка ока, голос та інші.

Вихід:

Список потенційних уразливостей системи зберігання біометричних даних. Це перелік можливих уразливостей, які можуть бути виявлені в системі зберігання біометричних даних. Вразливості можуть стосуватися програмного забезпечення, апаратного забезпечення, процедур безпеки або інших аспектів системи.

A2: Визначення необхідних заходів безпеки для зберігання біометричних даних

Описано процес визначення заходів безпеки, необхідних для забезпечення безпечного зберігання біометричних даних користувачів. У цьому процесі враховується аналіз загроз безпеці зберігання біометричних даних (який описаний в комірці A1), а також інформація про сучасні методи захисту даних. На основі цього аналізу визначаються необхідні заходи безпеки, наприклад, шифрування даних, контроль доступу до них, резервне копіювання тощо.

Вихід:

Набір заходів безпеки. Це список конкретних заходів, що необхідно вжити для захисту біометричних даних користувачів. Ці заходи можуть включати технічні, організаційні та процедурні заходи, які спрямовані на забезпечення конфіденційності, цілісності та доступності даних.

Визначення ролей та відповідальності. Визначення конкретних ролей і обов'язків, пов'язаних з управлінням безпекою даних. Це можуть бути ролі внутрішніх або зовнішніх сторін, які мають відповідальність за забезпечення безпеки біометричних даних. Визначення ролей та відповідальності допомагає забезпечити чітку структуру управління безпекою даних та уникнути пропусків у захисті.

A3: Впровадження системи зберігання біометричних даних з урахуванням необхідних заходів безпеки

Описується процес впровадження системи зберігання біометричних даних з урахуванням необхідних заходів безпеки. Цей процес включає в себе наступні етапи:

- Визначення вимог до системи зберігання біометричних даних з урахуванням необхідних заходів безпеки.
- Вибір технології для системи зберігання біометричних даних.
- Розробка дизайну системи зберігання біометричних даних з урахуванням вимог до безпеки.
- Розробка програмного забезпечення для системи зберігання біометричних даних.
- Розгортання системи зберігання біометричних даних на обраному сервері або в хмарному сервісі.
- Налаштування системи зберігання біометричних даних з урахуванням необхідних заходів безпеки.
- Тестування системи зберігання біометричних даних на відповідність вимогам до безпеки.
- Впровадження системи зберігання біометричних даних з урахуванням

необхідних заходів безпеки.

Вихід:

Система зберігання біометричних даних з процедурами та правилами.

Вказує на наявність розробленої та впровадженої системи зберігання біометричних даних. Вона повинна включати процедури та правила, які забезпечують безпеку даних від несанкціонованого доступу, змін та втрати.

Відповідальні особи. Вказує на наявність призначених осіб, які мають відповідальність за управління та забезпечення безпеки системи зберігання біометричних даних. Ці особи можуть бути внутрішніми чи зовнішніми спеціалістами, які відповідають за виконання встановлених процедур та правил.

Достатнє фінансування. Вказує на наявність достатніх фінансових ресурсів для впровадження та підтримки системи зберігання біометричних даних з урахуванням необхідних заходів безпеки. Це може включати витрати на обладнання, програмне забезпечення, навчання персоналу та інші витрати, пов'язані з забезпеченням безпеки даних.

План тестування. Вказує на наявність розробленого плану тестування системи зберігання біометричних даних. План тестування включає процедури, методи та критерії для перевірки ефективності та правильності роботи системи зберігання даних. Він дозволяє перевірити, чи задовольняє система встановлені вимоги безпеки та функціональності.

A4: Тестування системи зберігання біометричних даних

Передбачено проведення тестування розробленої системи зберігання біометричних даних. Цей етап є дуже важливим, оскільки під час тестування можуть виявитися помилки та недоліки системи, які не були виявлені на попередніх етапах.

На цьому етапі будуть розроблені тестові плани та проведені відповідні тести, які дозволять перевірити роботу системи зберігання біометричних даних. Результати тестів будуть детально проаналізовані та використані для вдосконалення системи на наступному етапі.

У разі виявлення помилок та недоліків на цьому етапі, необхідно буде повернутися на попередні етапи та внести відповідні зміни в розроблену систему. Таким чином, тестування є важливим етапом у процесі розробки та вдосконалення системи зберігання біометричних даних.

Вихід:

Результати тестування системи зберігання біометричних даних. Це включає результати проведених тестів, які були здійснені для оцінки функціональності, безпеки та ефективності системи зберігання біометричних даних. Результати можуть містити інформацію про успішність системи, проблеми, виявлені уразливості або помилки.

Список виявлених уразливостей та помилок. Це вказує на наявність документованого списку виявлених уразливостей та помилок під час тестування системи зберігання біометричних даних. Цей список може містити опис кожної уразливості або помилки, їх вплив на безпеку та функціональність системи, а також рекомендації щодо виправлення або підвищення безпеки.

A5: Оцінка ефективності системи зберігання біометричних даних

Описується процес оцінки результатів впровадження системи зберігання біометричних даних. Цей процес включає наступні етапи:

- **Зібрання даних про роботу системи зберігання біометричних даних.** В цьому етапі проводиться аналіз різних параметрів системи, таких як швидкість доступу до даних, частота помилок, стійкість до атак і т.д.
- **Аналіз даних і порівняння зі стандартами.** У цьому етапі проводиться порівняння результатів з встановленими стандартами і вимогами до зберігання біометричних даних.
- **Визначення ефективності системи.** У цьому етапі оцінюється ефективність системи зберігання біометричних даних з точки зору безпеки, швидкодії та зручності використання.
- **Визначення потреб у вдосконаленні системи.** У цьому етапі визначаються потреби у вдосконаленні системи зберігання біометричних даних з урахуванням результатів оцінки ефективності.

- **Розробка плану вдосконалення системи.** У цьому етапі розробляється план вдосконалення системи зберігання біометричних даних з урахуванням виявлених потреб.
- **Впровадження плану вдосконалення системи.** У цьому етапі впроваджується план вдосконалення системи зберігання біометричних даних з метою поліпшення безпеки, швидкодії та зручності використання.

Вихід:

Висновки щодо функціональності. Описується, наскільки добре система виконує свої функції зберігання біометричних даних. Це може включати оцінку швидкості, точності та доступності системи.

Оцінка безпеки. Аналізується рівень безпеки системи зберігання біометричних даних. Оцінка може включати перевірку використання захисту даних, контролю доступу, шифрування та інших заходів безпеки.

Виявлені проблеми або слабкі місця. Звіт може вказувати на будь-які виявлені проблеми, помилки або слабкі місця системи зберігання біометричних даних, які потребують уваги та виправлення.

Рекомендації щодо вдосконалення. Звіт може містити рекомендації та пропозиції щодо подальшого удосконалення системи зберігання біометричних даних. Це може включати пропозиції щодо покращення безпеки, функціональності та швидкості системи.

А6: Удосконалення системи зберігання біометричних даних на основі результатів тестування

Описується процес вдосконалення системи зберігання біометричних даних на основі отриманих результатів тестування. Для досягнення цієї мети виконуються наступні дії:

- Оцінка результатів тестування системи зберігання біометричних даних.
- Виявлення проблем і недоліків у роботі системи зберігання біометричних даних.
- Розробка плану вдосконалення системи зберігання біометричних даних

з урахуванням виявлених проблем і недоліків.

- Впровадження запропонованих заходів вдосконалення системи зберігання біометричних даних.
- Перевірка результатів вдосконалення системи зберігання біометричних даних.
- Повторення циклу випробування та оцінки системи зберігання біометричних даних з урахуванням внесених змін.

Цей процес дозволяє забезпечити постійне вдосконалення системи зберігання біометричних даних, що є необхідною умовою для забезпечення безпеки та надійності її роботи.

Вихід:

Оновлені заходи безпеки. Система вдосконалюється шляхом впровадження нових або вдосконалення існуючих заходів безпеки. Це може включати усунення виявлених уразливостей, вдосконалення контролю доступу, шифрування даних тощо.

Виконані рекомендації: Система зберігання біометричних даних оновлюється відповідно до рекомендацій, які були сформульовані під час оцінки та тестування системи. Це можуть бути рекомендації щодо покращення функціональності, безпеки, продуктивності або ефективності системи.

Оновлена система. Після впровадження рекомендацій та заходів безпеки система зберігання біометричних даних оновлюється і готова до подальшого використання. Це може включати оновлене програмне забезпечення, налаштування інфраструктури, оновлені політики безпеки тощо.

Механізми декомпозиції моделі IDEF0 діаграми

Команда експертів з інформаційної безпеки. Це група фахівців, які спеціалізуються на аналізі та захисті інформації. Вони володіють глибокими знаннями про загрози, ризики та заходи безпеки і використовують свої навички для забезпечення безпеки системи зберігання біометричних даних.

Система збору та обробки інформації. Це інфраструктура, яка включає різні компоненти для збору, передачі та обробки біометричних даних користувачів. Ця система може включати різні пристрої, датчики, мережеві з'єднання та програмне забезпечення для збору, передачі та обробки даних.

Сервери та засоби зберігання даних. Це фізичні пристрої, які використовуються для зберігання біометричних даних користувачів. Це можуть бути сервери, бази даних, сховища даних та інші засоби зберігання, які забезпечують безпечну та надійну збереження і доступ до даних.

Тестувальники. Це спеціалісти, які виконують тестування системи зберігання біометричних даних з метою виявлення потенційних проблем, помилок та уразливостей. Вони проводять різні види тестувань, включаючи функціональне тестування, витривалість, безпеку, навантаження тощо.

Спеціальне програмне забезпечення для тестування. Це набір програмних інструментів і ресурсів, що використовуються для проведення тестування системи зберігання біометричних даних. Це може включати різноманітні програми для автоматизації тестування, генерації тестових даних, виявлення уразливостей та аналізу безпеки.

Управління життєвим циклом проекту.

Це процес планування, виконання, контролю та оцінки проекту на протязі всього його існування. Управління життєвим циклом проекту забезпечує організацію, керування та координацію всіх етапів проекту з метою досягнення поставленої мети.

Цей процес включає в себе такі етапи:

- **Планування:** Визначення цілей проекту, складання робочого плану, розподіл ресурсів та визначення вимог проекту.
- **Виконання:** Реалізація робочого плану, виконання завдань, координація роботи команди, вирішення проблем та управління змінами.
- **Контроль:** Моніторинг виконання проекту, порівняння фактичних результатів з планованими, виявлення відхилень, вирішення проблем

та коригування плану.

- Оцінка: Аналіз результатів проекту, оцінка досягнутих цілей, вивчення навчальних висновків та рекомендацій для майбутніх проектів.

ВИСНОВОК

Проаналізувавши і дослідивши питання ідентифікації користувачів на основі біометричних даних, можна зробити висновок, що розробка інформаційної системи ідентифікації користувачів на основі біометричних даних є актуальною та перспективною задачею, оскільки це дозволить підвищити рівень безпеки та захисту конфіденційної інформації.

У даній дипломній роботі було проведено аналіз наукової літератури та практичних реалізацій інформаційних систем, що використовують біометричні дані для ідентифікації користувачів. Було визначено основні види біометричних даних та їх переваги та недоліки.

Окрему увагу було приділено безпеці збереження біометричних даних користувачів. У дипломній роботі було запропоновано підвищення безпеки збереження біометричних даних шляхом розробки архітектури інформаційної системи на основі методології IDEF0. За допомогою IDEF0 було показано, що безпека збереження біометричних даних може бути покращена завдяки використанню спеціальних механізмів захисту даних та резервного збереження.

Таким чином, можна зробити висновок, що розробка інформаційної системи ідентифікації користувачів на основі біометричних даних є актуальною та перспективною задачею, а розроблена в дипломній роботі архітектура системи на основі IDEF0 може покращити безпеку збереження біометричних даних користувачів.

Пропонуються додаткові дослідження та розробки у галузі біометричної ідентифікації користувачів, зокрема, удосконалення алгоритмів обробки та порівняння біометричних даних, введення нових типів біометричних параметрів, розробка систем забезпечення захисту від злому та фальсифікації, а також дослідження масштабування та впровадження систем ідентифікації в реальних умовах.

Для практичного використання розробленої інформаційної системи ідентифікації користувачів на основі біометричних даних, необхідні додаткові

заходи забезпечення безпеки і захисту персональних даних користувачів. Також слід враховувати вимоги законодавства про захист персональних даних та відповідні міжнародні стандарти у галузі біометричних технологій.

Варто зазначити, що система поліпшення захисту біометричних даних потребує практичної апробації в реальних умовах щоб напевно дізнатися як саме і на скільки вона вплине на ефективність та захист в цілому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Сучасні методи біометричної ідентифікації [Електронний ресурс]: [Веб-сайт]. Режим доступу: www.ela.kpi.ua (дата звернення 23.04.2023).
2. Біометрична ідентифікація [Електронний ресурс]: [Веб-сайт]. Режим доступу: sites.google.com (дата звернення 27.04.2023).
3. Методи біометричної ідентифікації [Електронний ресурс]: [Веб-сайт]. Режим доступу: www.ela.kpi.ua (дата звернення 27.04.2023).
4. Біометрична ідентифікація за відбитками пальців [Електронний ресурс]: [Веб-сайт]. Режим доступу: www.tech.vernadskyjournals.in.ua (дата звернення 28.04.2023).
5. Біометричні особливості [Електронний ресурс]: [Веб-сайт]. Режим доступу: www.ela.kpi.ua (дата звернення 26.04.2023).
6. What is OpenCV <https://viso.ai> [Електронний ресурс]: [Веб-сайт]. Режим доступу: studfile.net (дата звернення 10.05.2023).
7. Amazon Rekognition [Електронний ресурс]: [Веб-сайт]. Режим доступу: aws.amazon.com (дата звернення 26.04.2023).
8. FaceSDK [Електронний ресурс]: [Веб-сайт]. Режим доступу: www.luxand.com (дата звернення 26.04.2023).
9. VeryFinger [Електронний ресурс]: [Веб-сайт]. Режим доступу: www.neurotechnology.com (дата звернення 26.04.2023).
10. IRIS ID [Електронний ресурс]: [Веб-сайт]. Режим доступу: www.irisid.com (дата звернення 26.04.2023).