Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Аналіз технологій біометричної автентифікації"

Виконав: студент

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Бойко С.С.
підпис (прізвище та ініціали)

Керівник Деркач М.В.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д.І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Луцик Н.С.
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Бойко Степану Степановичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз технологій біометричної автентифікації

Керівник роботи Деркач Марина Володимирівна, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «15» 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Галузь застосування технології біометричної автентифікації та її роль в безпеці збережених даних
Роль технології біометричної автентифікації з точки зору безпеки
Біометрична автентифікація мобільних пристроїв
Основні механізми та їх реалізація
Підвищення рівня безпеки мобільного пристрою за допомогою біометричної автентифікації
Використання багатофакторної автентифікації
Інструменти для реалізації біометричної автентифікації на платформі Android
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1.Титульний слайд, 2.Актуальність біометричної автентифікації, 3.Технології біометричної Автентифікації, 4. Галузі застосування, 5.Інструменти біометричної автентифікації, 6.Біометрична автентифікація у Windows Hello, 7.Візуалізація ознак обличчя, 8.Алгоритм визначення обличчя, 9. Висновки, 10.Методи підвищення безпеки БА.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці			

7. Дата видачі завдання 29.01.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	Виконано
2.	Підбір джерел про види біометричної автентифікації	20.02 – 27.02	Виконано
3.	Опрацювання джерел в галузі мультифакторної автентифікації	28.02 – 16.03	Виконано
4.	Дослідження можливих реалізацій біометричної автентифікації	17.03 – 20.03	Виконано
5.	Тестування налаштування обличчя Windows Hello	20.03-05.04	Виконано
6.	Оформлення розділу «Роль та застосування технології біометричної автентифікації»	06.03 – 17.04	Виконано
7.	Оформлення розділу «Методи та інструменти біометричної автентифікації»	18.04 – 29.04	Виконано
8.	Оформлення розділу «Реалізація методу біометричної автентифікації»	30.04 – 13.05	Виконано
9.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	14.05 – 21.05	Виконано
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	Виконано
11.	Нормоконтроль	06.06 – 12.06	Виконано
12.	Перевірка на плагіат	10.06 – 16.06	Виконано
13.	Попередній захист кваліфікаційної роботи	18.06 – 21.06	Виконано
14.	Захист кваліфікаційної роботи		

Студент _____ Бойко С.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Деркач М.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Аналіз технологій біометричної автентифікації// Кваліфікаційна робота ОР «Бакалавр» //Бойко Степан Степанович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2024 // С. 52, рис. – 21, табл. – __ , кресл. –__ , додат. – ___.

Ключові слова: аналіз, автентифікація, біометрія, безпека даних, Windows Hello.

Кваліфікаційна робота аналізу технологій біометричної автентифікації (БА) та їх ролі у забезпеченні безпеки збережених даних.

У першому розділі кваліфікаційної роботи розглянуто технології біометричної автентифікації (БА), їх роль у забезпеченні безпеки збережених даних, а також у галузі застосування цих технологій.

У другому розділі кваліфікаційної роботи розглянута роль біометричної автентифікації з погляду безпеки, а також методи підвищення безпеки та інструменти біометричної автентифікації.

У третьому розділі кваліфікаційної роботи описано реалізацію методу біометричної автентифікації. Налаштування БА за допомогою розпізнавання обличчя у Windows Hello, а також принцип дії розпізнавання обличчя за допомогою алгоритмів машинного навчання HOG та SVM.

ANNOTATION

Analysis of the Biometric Authentication Technologies// Thesis of educational level "Bachelor" // Boiko Stepan Stepanovych// Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, SB-41 group // Ternopil, 2024 // P. 53, fig. - 21, table. - __ , chair. - ___ , added. -___.

Keywords: analysis, authentication, biometrics, data security, Windows Hello.

The qualification work of biometric authentication (BA) technologies and their role in ensuring the security of stored data.

The first chapter of the qualification work discusses biometric authentication (BA) technologies, their role in ensuring the security of stored data, as well as the application of these technologies.

In the second chapter of the qualification work discusses the role of biometric authentication from a security point of view, as well as methods of increasing security and tools for biometric authentication.

The third chapter of the qualification work describes the implementation of the biometric authentication method. Setting up BA using face recognition in Windows Hello, as well as the principle of face recognition using HOG and SVM machine learning algorithms.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БА – біометрична автентифікація

2FA – двофакторна автентифікація

MFA – багатофакторна автентифікація

ДНК – генетичний код людини

STR – короткі тамдемні повтори

ICAO – Міжнародна організація цивільної авіації

VPN – віртуальна приватна мережа

MFCC – Mel-Frequency Cepstral Coefficients

HOG – Histogram of Oriented Gradients

SVM – Support Vector Machines

ВСТУП

У сучасному світі, де інформаційні технології пронизують усі сфери життя, питання безпеки даних набуває особливої актуальності. Традиційні методи автентифікації, такі як паролі та PIN-коди, все частіше виявляються недостатньо надійними, оскільки їх можна вгадати, зламати, або забути. У цьому контексті біометрична автентифікація (БА) виступає як перспективна альтернатива, що пропонує вищий рівень безпеки та зручності використання.

БА використовує унікальні біологічні або поведінкові характеристики людини для підтвердження її особистості. Ці характеристики, такі як відбитки пальців, риси обличчя, голос, райдужна оболонка ока, геометрія руки, ДНК, або навіть спосіб ходьби, є індивідуальними та важко підроблюваними, що робить біометричну автентифікацію надійним інструментом захисту даних. Це означає, що біометричні ознаки задовольняють трьом критичним властивостям: універсальність, унікальність та сталість.

Дана дипломна робота присвячена аналізу технологій біометричної автентифікації та їх ролі в забезпеченні безпеки збережених даних. У роботі буде розглянуто широкий спектр застосувань біометричної автентифікації, від банківської сфери та мобільних пристроїв до охорони здоров’я та державних установ. Особлива увага буде приділена аналізу різних біометричних характеристик, їх переваг та недоліків, а також методам підвищення безпеки біометричних систем.

1 ГАЛУЗЬ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ ТА ЇЇ РОЛЬ В БЕЗПЕЦІ ЗБЕРЕЖЕНИХ ДАНИХ

1.1 Технології біометричної автентифікації

Біометрична автентифікація (БА) – це сучасний метод підтвердження особистості, який базується на аналізі унікальних фізіологічних або поведінкових особливостей людини. Біометрія дозволяє ідентифікувати та провести верифікацію людини на основі набору специфічних та унікальних рис, властивих їй від народження, які завжди присутні на людині, унікальні та вкрай незмінні у часі.

Відбитки пальців, риси обличчя, голос, райдужна оболонка ока, геометрія руки, ДНК та навіть динаміка рухів – усі ці характеристики є неповторними для кожної людини, на відміну від паролів чи PIN-кодів, такі маркери ідентичності неможливо забути або втратити. Вони завжди з нами, що робить БА зручним та ефективним засобом захисту інформації.

Більше того, складність підробки біометричних даних, на відміну від стандартних логіну та паролю, робить такий метод розпізнавання одним із найнадійніших бар’єрів проти несанкціонованого доступу до конфіденційної інформації [1].

На даний момент існують і активно застосовуються в безпеці, системах контролю доступу та запобігання крадіжкам вже 14 типів біометричних пристроїв:

- відбитки пальців - розпізнавання відбитків пальців один із перших біометричних методів, що ґрунтується на визначенні структури ліній на подушечках пальців рук, інакше — папілярних візерунків. Після зчитування сканером унікальний малюнок трансформується на цифровий біометричний шаблон, який потім порівнюється зі зразком, що зберігається в пам'яті пристрою. Такі сканери поділяються на два основні типи: оптичні та кремнієві (теплові та ємнісні).

- рисунок вен на пальцях / руках - цей тип є вдосконаленою версією попереднього. Зламати алгоритм його роботи значно важче, ніж за іншого біометричного сканування, оскільки вени знаходяться глибоко під шкірою. Інфрачервоні промені проходять через поверхню шкіри, де вони поглинаються венозною кров'ю. Спеціальна камера фіксує зображення, оцифровує дані, а потім або зберігає їх або використовує для підтвердження особистості.

- геометрія долонь - визначення геометрії руки відноситься до вимірювання таких характеристик, як довжина та ширина пальців, їх кривизна та відносне розташування. На даний момент цей метод є застарілим і майже не використовується, хоча колись був домінуючим варіантом біометричної ідентифікації.

- райдужна оболонка ока, або кольорова частина ока, складається з товстих ниткоподібних м'язів. Ці м'язи допомагають формувати зіницю, щоб контролювати кількість світла, що потрапляє у око. Вимірюючи унікальні складки та характеристики цих м'язів, тобто унікальність візерунка райдужної оболонки ока людини, інструменти біометричної верифікації можуть підтвердити особу з неймовірною точністю. Оскільки сканер райдужної оболонки ока використовує інфрачервону камеру для захоплення зображення ока, а потім складні алгоритми аналізують візерунок райдужної оболонки для ідентифікації користувача. Технології динамічного сканування (наприклад, сканування того, як людина моргає) додають додатковий рівень точності та безпеки.

- сітківка ока - перевірка сітківки дозволяє відсканувати капіляри глибоко усередині ока за допомогою камер ближнього інфрачервоного діапазону. Зображення спочатку попередньо обробляється для поліпшення його якості, а потім перетворюється на біометричний шаблон для реєстрації нового користувача і для подальшої звірки з еталоном під час спроб розпізнавання користувача.

- технологія розпізнавання обличь, одна з перших та найпоширеніших форм біометричної ідентифікації, аналізує унікальні риси обличчя людини. Спеціалізоване програмне забезпечення вимірює геометричні параметри обличчя, такі як відстань між очима, від підборіддя до чола та інші. Отримані дані

перетворюються на унікальний зашифрований код, або ”підпис обличчя”, який потім порівнюється зі збереженими зразками для верифікації особистості.

Оскільки існують різні підходи:

1) 2D розпізнавання обличчя: цей метод використовує звичайну камеру для захоплення зображення обличчя клієнта. Отримане зображення порівнюється зі збереженим шаблоном обличчя, і якщо збіг достатній, відбувається автентифікація.

2) 3D розпізнавання обличчя: цей метод використовує спеціальні сенсори, такі як інфрачервоні камери та проектори точок, для створення детальної 3D-моделі обличчя клієнта. Цей метод вважається більш безпечним, ніж 2D-розпізнавання, оскільки його важче обдурити підробленими зображеннями.

- форма вушної раковини - біометричні системи, що використовують форму вушної раковини, вимірюють її унікальну акустику за допомогою спеціальних навушників та нечутних звукових хвиль. Мікрофон у навушниках фіксує, як звукові хвилі відбиваються від вушної раковини та розходяться, створюючи індивідуальний акустичний “відбиток” вуха, який потім перетворюється на цифровий шаблон.

- технологія розпізнавання голосу поєднує в собі фізіологічні та поведінкові біометричні дані. З одного боку, вона аналізує форму голосового тракту людини (ніс, рот, горло), що визначає звучання голосу. З іншого боку, вона враховує індивідуальні особливості мовлення, такі як інтонація, темп, акцент тощо. Поєднання цих даних створює унікальний голосовий "підпис". [3].

- термограма – біометрична термографія обличчя фіксує унікальні теплові візерунки, що утворюються внаслідок руху крові під шкірою. Оскільки кровоносна система кожної людини індивідуальна, термограми також є унікальними, навіть у однояйцевих близнюків, що робить цей метод ідентифікації ще точнішим, ніж традиційне розпізнавання обличь.

- ДНК давно використовується для ідентифікації особистості та є єдиним біометричним методом, здатним відстежувати родинні зв'язки. На відміну від відбитків пальців, ДНК неможливо випадково "забути" або втратити, що робить його особливо надійним біометричним ідентифікатором. ДНК містить

послідовності коротких тандемних повторів (STR). З їхньою допомогою можна однозначно підтвердити особистість, порівнюючи їх з іншими STR у базі даних. ДНК вважається ідеальною біометричною характеристикою, але її недолік полягає в тому, що однояйцеві близнюки матимуть одну й ту саму ДНК.

- біометрія ходи - цей метод ідентифікації фіксує унікальні шаблони ходьби людини за допомогою відеозапису, перетворюючи їх на математичне рівняння. Такий підхід є ненав'язливим та непомітним, що робить його ідеальним для спостереження за великими групами людей. Більше того, системи розпізнавання ходи здатні швидко ідентифікувати людей на відстані.

- рух губ - цей новий метод біометричної верифікації аналізує активність м'язів навколо рота під час мовлення, формуючи унікальний шаблон руху губ. Часто такі системи вимагають від користувача повторити пароль, щоб порівняти його з записаним шаблоном та підтвердити особу.

- розпізнавання підпису - ця поведінкова біометрична система вимірює просторові координати, тиск пера, його нахил та інші параметри під час написання підпису. Цифровий планшет фіксує ці дані та створює біометричний профіль для подальшої верифікації.

- натискання клавіш - динаміка натискання клавіш виводить паролі на новий рівень безпеки, відстежуючи індивідуальний ритм їх введення. Датчики фіксують час натискання кожної клавіші, затримки між ними, кількість символів, що вводяться за хвилину, та інші параметри. Шаблони натискання клавіш використовуються разом з паролями та PIN-кодами для підвищення рівня захисту.

1.2 Галузі застосування технологій біометричної автентифікації

На сьогоднішній день біометричні системи вже звичні кожному, беруть активну участь у нашому житті, поступово приходять на заміну традиційним методам ідентифікації та все частіше проникають у великі бізнеси, такі як банківське обслуговування, роздрібна торгівля (рітейл), фінансові технології (фінтех), автомобільна індустрія. Також технології біометричної автентифікації знайшли своє застосування у безпеці.

1.2.1 Банківська та фінансова сфера

Більшість сучасних банківських додатків, таких як Revolut, Monobank, Privat24, та інші, використовують сканування відбитків пальців для підтвердження транзакцій. Це зручно та безпечно, оскільки відбитки пальців є унікальними для кожної людини та їх важко підробити. Замість введення PIN-коду або пароля, користувач просто прикладає палець до сканера на своєму смартфоні, що забезпечує швидку та безпечну авторизацію платежу (див. рисунок 1.1).

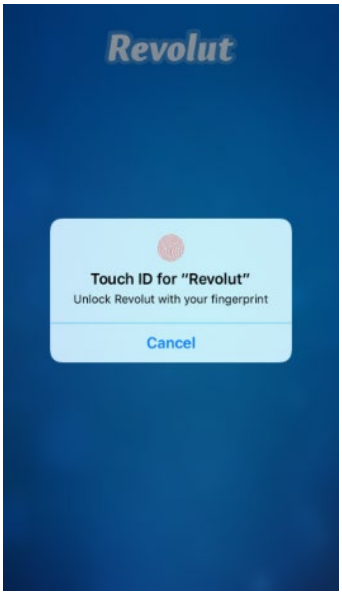

Рисунок 1.1 - “Touch ID” в Revolut.

Деякі банки, особливо ті, що орієнтовані на молоду аудиторію, впроваджують технологію розпізнавання обличчя (наприклад, Face ID від Apple) для авторизації платежів. Це ще більше спрощує процес оплати, оскільки користувачам не потрібно навіть торкатися смартфона. Розпізнавання обличчя у банківській сфері може використовувати різні підходи: 2D та 3D розпізнавання обличчя. Багато банків використовують розпізнавання обличчя для віддаленої ідентифікації клієнтів під час відкриття рахунків, отримання кредитів та інших фінансових послуг. Це дозволяє клієнтам проходити ідентифікацію без

необхідності відвідувати відділення банку, що значно економить час та ресурси. Наприклад, Monobank в Україні використовує розпізнавання обличчя для віддаленої ідентифікації клієнтів під час відкриття рахунку (див. рисунок 1.2).

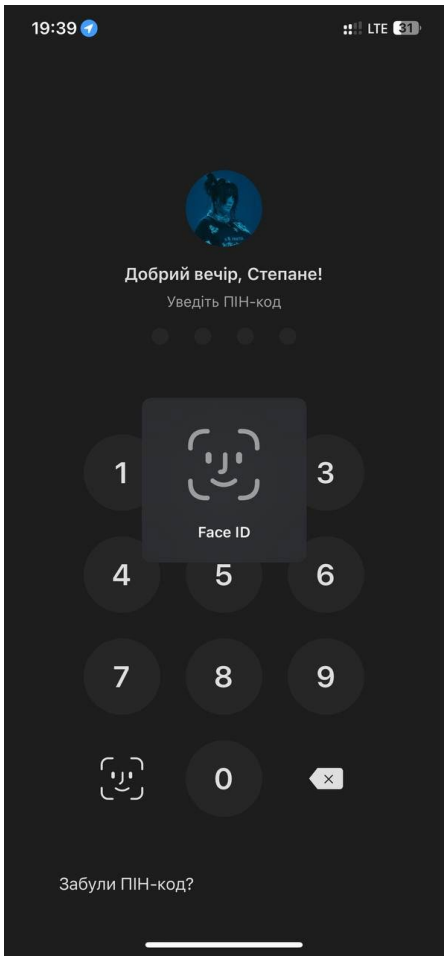

Рисунок 1.2 - Розпізнавання обличчя для авторизації у застосунок Monobank

Також деякі банки вже впроваджують сканування райдужної оболонки ока в банкоматах для ідентифікації клієнтів та надання доступу до їхніх рахунків. Наприклад, NCBA Bank у Кенії використовує сканери райдужної оболонки ока у своїх банкоматах, що дозволяє клієнтам знімати готівку та здійснювати інші операції без використання картки (див. рисунок 1.3). Додатково банки розглядають можливість використання сканування райдужної оболонки ока для автентифікації клієнтів у мобільних додатках та системах онлайн-банкінгу. Це може забезпечити додатковий рівень безпеки та зручності для клієнтів.

Рисунок 1.3 - Використання райдужки ока в банкоматі

1.2.2 Мобільні пристрої

Більшість сучасних смартфонів оснащені сканерами відбитків пальців, які дозволяють користувачам швидко та безпечно розблокувати свої пристрої. Технології, такі як Apple Touch ID та Samsung Fingerprint Scanner, стали стандартом у галузі. Вони використовують ємнісні сенсори для створення зображення відбитка пальця та порівняння його зі зразком, що зберігається в пам'яті пристрою. Ці технології постійно вдосконалюються, стаючи швидшими та точнішими [2].

Багато інших виробників смартфонів, таких як Xiaomi, Huawei, OnePlus та інші, також використовують сканери відбитків пальців, які можуть відрізнятися за типом сенсора (ємнісний, оптичний, ультразвуковий) та місцем розташування.

1.2.3 Охорона здоров’я

В багатьох лікарнях та клініках використовують сканування відбитків пальців для ідентифікації пацієнтів. Це допомагає уникнути помилок при лікуванні, забезпечує правильне ведення медичної документації та запобігає

шахрайству з медичним страхуванням. Наприклад, деякі лікарні використовують сканери відбитків пальців для реєстрації пацієнтів при прийомі, а також для доступу до їхніх електронних медичних карток. Медичні установи використовують сканування райдужної оболонки ока для ідентифікації пацієнтів, особливо в тих випадках, коли відбитки пальців можуть бути пошкоджені або відсутні. Ця технологія особливо корисна в офтальмологічних клініках, де пацієнти часто мають проблеми з відбитками пальців через хвороби очей. Сканування райдужної оболонки ока є безконтактним та гігієнічним методом ідентифікації, що особливо важливо в медичних установах.

1.2.4 Транспорт

Деякі аеропорти використовують сканери відбитків пальців для ідентифікації пасажирів при посадці. Це може бути додатковим заходом безпеки або альтернативою для пасажирів, які не хочуть використовувати розпізнавання обличчя. Також авіакомпанії та залізничні оператори вже використовують розпізнавання обличчя для прискорення процесу посадки. Пасажири можуть просто пройти через спеціальні ворота, які сканують їхнє обличчя та порівнюють його з фотографією в паспорті.

1.3 Огляд мобільних та десктопних додатків з підтримкою біометричної автентифікації

1.3.1 Apple Touch ID

Технологія Apple, що використовує сканування відбитків пальців. Вона була вперше представлена у 2013 році в iPhone 5s і з тих пір стала невід'ємною частиною багатьох пристроїв Apple, включаючи iPhone, iPad, MacBook Pro та MacBook Air. Touch ID інтегрований в кнопку "Додому" (або кнопку живлення на деяких моделях iPad) і дозволяє користувачам розблоковувати пристрій, авторизувати покупки в App Store та iTunes Store, використовувати Apple Pay, а

також входити в деякі сторонні додатки.

Touch ID використовує ємнісний сенсор, розташований під сапфіровим склом, для сканування відбитка пальця користувача (див. рисунок 1.4). Сенсор створює детальне зображення папілярних ліній на пальці, використовуючи електричне поле. Отримане зображення перетворюється на математичне представлення (шаблон) і зберігається в захищеному анклаві пристрою, Secure Enclave. Під час автентифікації сенсор знову сканує відбиток пальця, створює новий шаблон і порівнює його зі збереженим шаблоном. Якщо шаблони збігаються, автентифікація вважається успішною.

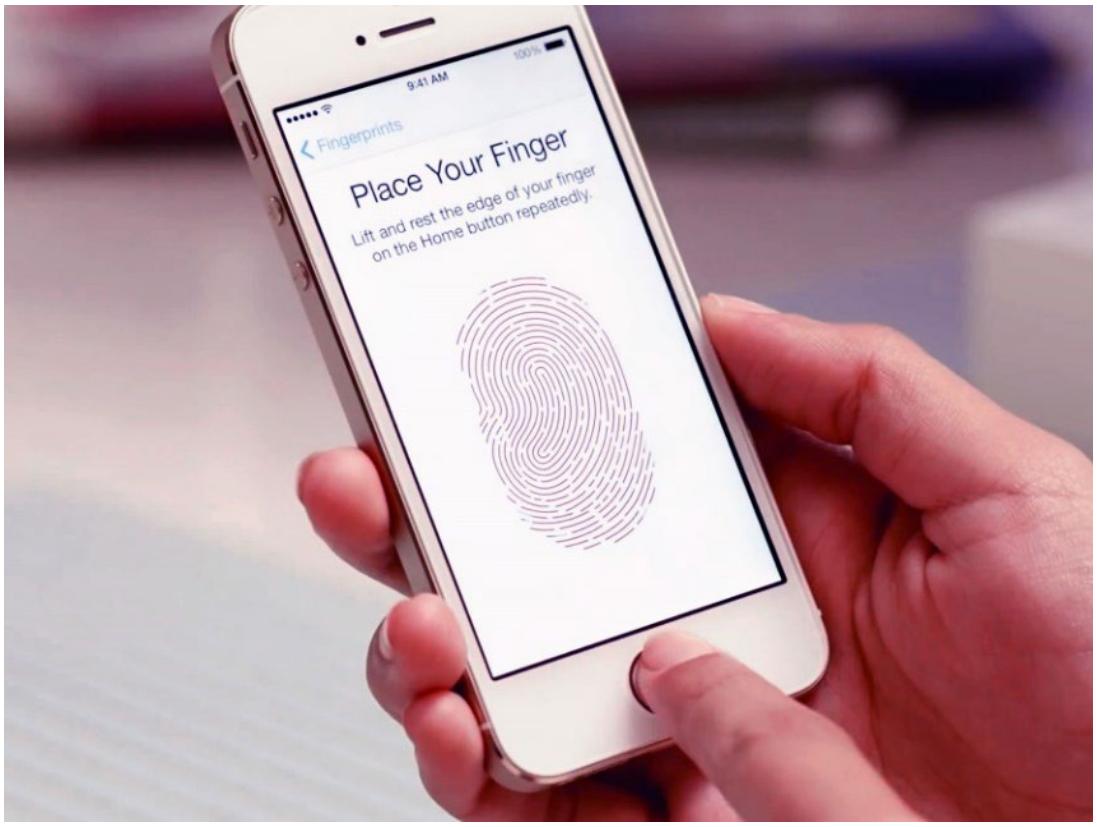

Рисунок 1.4 - Apple Touch ID

Touch ID використовує спеціальний співпроцесор, Secure Enclave, для безпечного зберігання та обробки біометричних даних. Secure Enclave ізольований від основного процесора пристрою, що забезпечує високий рівень захисту від несанкціонованого доступу. Може розпізнавати відбитки пальців незалежно від їхньої орієнтації, що робить його зручним у використанні, дозволяє зберігати до п'яти різних відбитків пальців, що може бути корисним для членів

сім'ї або для використання різних пальців та здатний до адаптивного навчання, що означає, що він з часом покращує свою точність розпізнавання, запам'ятовуючи різні варіанти відбитка пальця користувача.

1.3.2 Samsung Fingerprint Scanner

Технологія Samsung також використовує ємнісний сенсор, але може бути розташована на задній панелі пристрою, під екраном або навіть збоку (див. рисунок 1.5). Технологія базується на унікальності візерунка папілярних ліній на пальцях людини. Сканер створює цифрове зображення відбитка, яке потім порівнюється зі зразком, що зберігається в пам'яті пристрою.

Рисунок 1.5 - Ємнісний сканер відпечатку пальця на задній кришці телефону

Samsung використовує різні типи сканерів відбитків пальців у своїх пристроях.

- Ємнісні сканери: це найпоширеніший тип сканерів, які використовуються в більшості смартфонів Samsung Galaxy. Вони розташовані під

екраном, на задній панелі пристрою або інтегровані в кнопку живлення. Ємнісні сканери використовують електричний струм для виявлення папілярних ліній на пальці та створення цифрового зображення відбитка.

- Ультразвукові сканери: ця технологія є більш новою та передовою. Вона використовує ультразвукові хвилі для створення 3D-моделі відбитка пальця, що робить його більш точним та безпечним, ніж ємнісні сканери. Ультразвукові сканери також можуть працювати через скло або метал, що дозволяє розміщувати їх під екраном смартфона (див. рисунок 1.6). Samsung вперше представила ультразвуковий сканер відбитків пальців у Galaxy S10 та S10+.

Рисунок 1.6 - Ультразвуковий сканер вбудований у екран

1.3.3 Apple Face ID

Face ID використовує TrueDepth камеру, що складається з кількох компонентів, інфрачервоний випромінювач (Flood Illuminator), що проектує рівномірне інфрачервоне світло на обличчя користувача, навіть в умовах низької освітленості. Точковий проектор (Dot Projector) проектує понад 30 000 невидимих інфрачервоних точок на обличчя, створюючи унікальну карту глибини обличчя (див. рисунок 1.7).

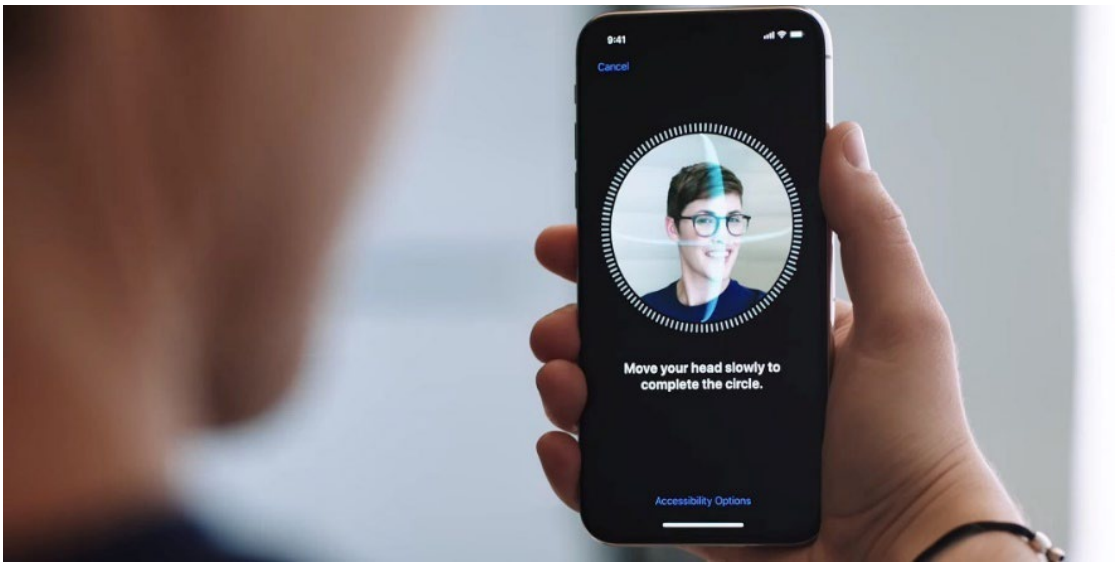

Рисунок 1.7 - Налаштування Face ID

Ці дані передаються до нейронного двигуна (Neural Engine), який аналізує карту глибини обличчя та порівнює її зі збереженим шаблоном обличчя користувача. Якщо збіг достатній, відбувається автентифікація. Face ID використовує спеціальний співпроцесор, Secure Enclave, для безпечного зберігання та обробки біометричних даних. Secure Enclave ізольований від основного процесора пристрою, що забезпечує високий рівень захисту від несанкціонованого доступу. Алгоритми машинного навчання для адаптації до змін зовнішності користувача, таких як носіння окулярів, головного убору, макіяжу або зміни зачіски. Також Face ID вимагає від користувача звернути увагу на пристрій та мати намір розблокувати його. Це робить його більш безпечним, ніж системи, які розпізнають обличчя на фотографії.

1.3.4 Windows Hello

Windows Hello – це технологія біометричної автентифікації, вбудована в операційну систему Windows 10 та 11, яка дозволяє користувачам входити в систему, розблоковувати пристрої та авторизувати покупки за допомогою розпізнавання обличчя, відбитків пальців або PIN-коду. Розпізнавання обличчя в Windows Hello є одним з найпопулярніших та зручних методів біометричної

автентифікації на ПК та ноутбуках (див. рисунок 1.8).

Рисунок 1.8 - Налаштування розпізнавання обличчя у Windows

Windows Hello використовує спеціальну інфрачервону (ІЧ) камеру, яка проектує невидиме ІЧ-світло на обличчя користувача та захоплює його відображення. Це дозволяє створити детальну карту глибини обличчя, яка потім аналізується за допомогою алгоритмів машинного навчання для підтвердження особистості користувача.

1.3.5 Google Face Unlock

Google Face Unlock - це технологія біометричної автентифікації, розроблена компанією Google, яка використовує фронтальну камеру смартфона та алгоритми машинного навчання для розпізнавання обличчя користувача (див. рисунок 1.9). Ця технологія дозволяє швидко та зручно розблоковувати пристрій, авторизувати покупки та входити в додатки. Face Unlock використовує фронтальну камеру смартфона для захоплення зображення обличчя користувача. Потім це зображення обробляється за допомогою алгоритмів машинного навчання, які

аналізують унікальні риси обличчя, такі як відстань між очима, форма носа та інші. Система порівнює отримані дані зі збереженим шаблоном обличчя користувача, і якщо збіг достатній, відбувається автентифікація.

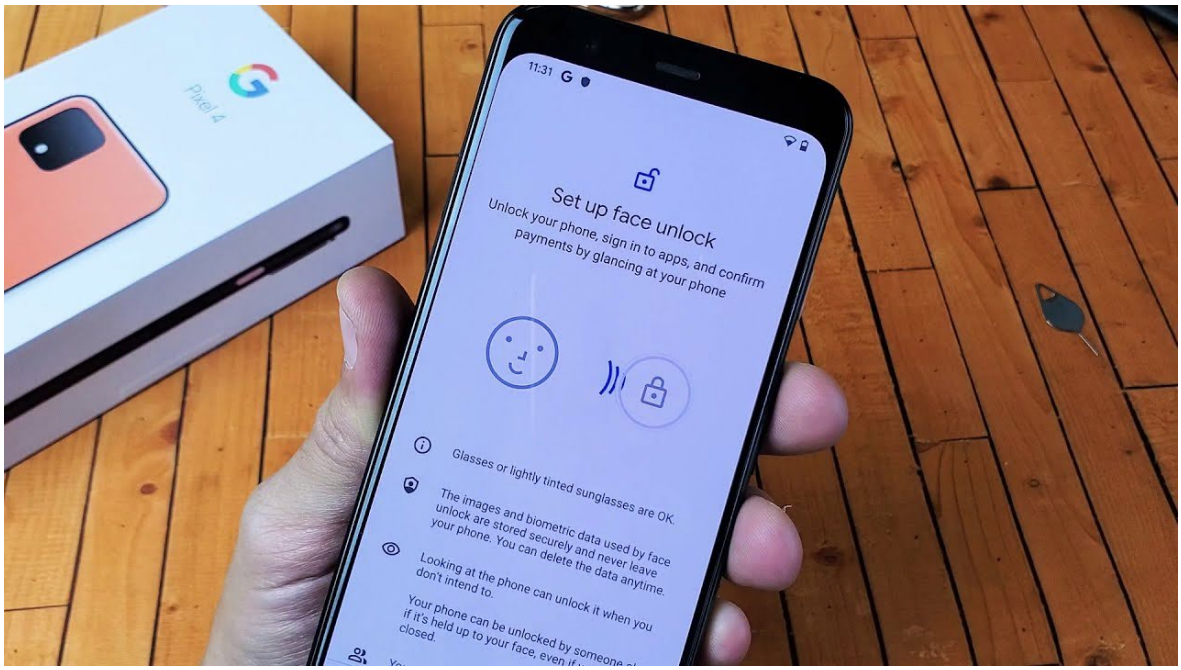

Рисунок 1.9 - Google Face Unlock

На відміну від Apple Face ID, Google Face Unlock не використовує спеціальні ІЧ-сенсори та проектори точок. Замість цього, він покладається на фронтальну камеру смартфона, що робить його більш доступним для різних пристроїв. На деяких пристроях Google Pixel, біометричні дані, включаючи дані Face Unlock, зберігаються в окремому безпечному чіпі Titan M, що забезпечує їх захист від несанкціонованого доступу.

1.3.6 Samsung Iris Scanner

Samsung Iris Scanner – це інноваційна технологія біометричної автентифікації, розроблена компанією Samsung, яка використовує сканування райдужної оболонки ока для ідентифікації користувача (див. рисунок 1.10). Ця технологія була вперше представлена в смартфоні Samsung Galaxy Note 7 у 2016 році і пізніше була включена до деяких моделей Galaxy S8, S8+, S8+, S9 та S9+.

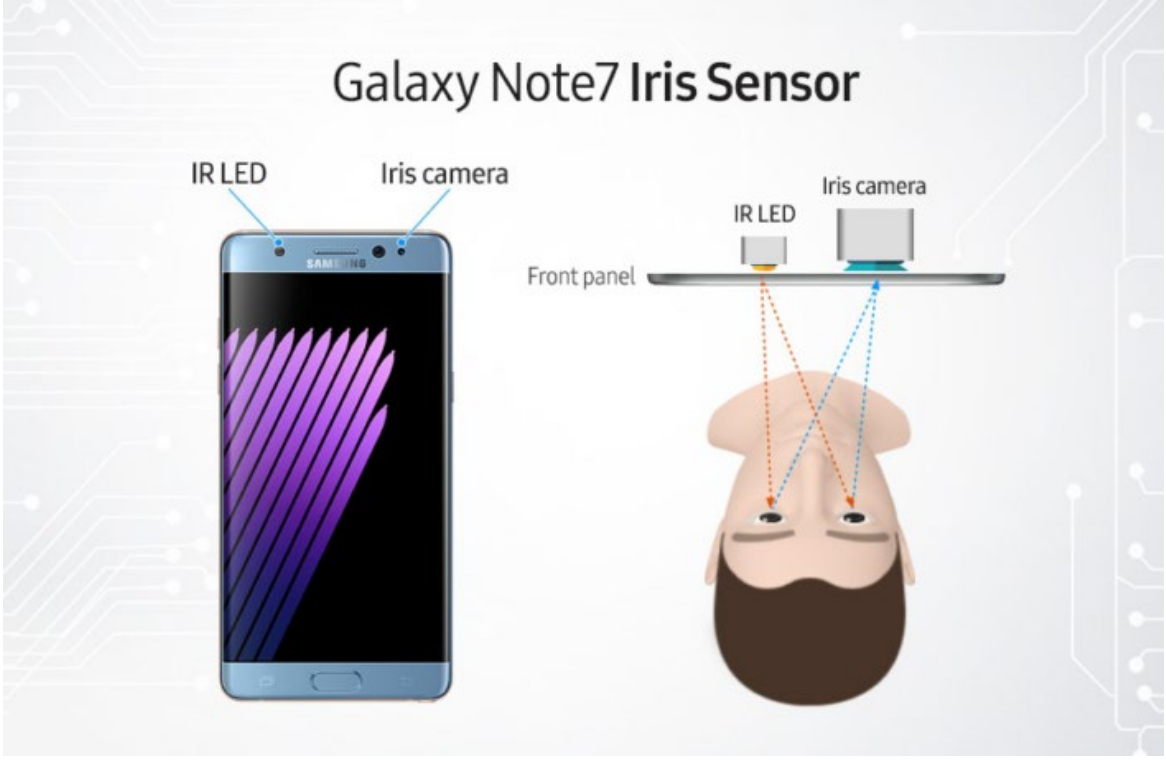

Рисунок 1.10 - Samsung Iris Scanner

1.4 Постановка завдання на розробку

Актуальність даної роботи обумовлена зростаючим значенням біометричної автентифікації в сучасному світі. З кожним роком все більше організацій та приватних осіб використовують біометричні дані для захисту своїх даних та систем. Розуміння принципів роботи біометричної автентифікації, її переваг та недоліків є важливим для прийняття обґрунтованих рішень щодо її впровадження та використання.

Метою даної роботи є проведення комплексного аналізу технологій та реалізація методу біометричної автентифікації для захисту облікових записів від несанкціонованого доступу.

Для досягнення цієї мети будуть вирішені наступні завдання:

1. Аналіз існуючих технологій біометричної автентифікації.
2. Аналіз галузей застосування технологій біометричної автентифікації.
3. Аналіз методів підвищення безпеки облікових записів від несанкціонованого доступу.

4. Реалізація методу біометричної автентифікації на ПК та ноутбуках.

1.5 Висновки до першого розділу

Технології біометричної автентифікації мають великий потенціал у забезпеченні безпеки збережених даних та пропонують ряд переваг порівняно з традиційними методами автентифікації. Вони знаходять все ширше застосування в різних сферах життя, від банківської справи до охорони здоров'я. Однак, для ефективного використання цих технологій необхідно враховувати їх переваги та недоліки, а також використовувати комплексний підхід до забезпечення безпеки, включаючи комбінування біометричної автентифікації з іншими методами захисту.

2 МЕТОДИ ТА ІНСТРУМЕНТИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

2.1 Роль технології біометричної автентифікації з точки зору безпеки

Мобільні пристрої, такі як смартфони та планшети, та навіть ПК та ноутбуки стали невід'ємною частиною нашого життя. Вони зберігають величезну кількість особистої та конфіденційної інформації, включаючи контакти, повідомлення, фотографії, фінансові дані та багато іншого. Тому захист цих пристроїв від несанкціонованого доступу є надзвичайно важливим. Біометрична автентифікація відіграє ключову роль у забезпеченні безпеки даних та систем, пропонуючи зручний та надійний спосіб підтвердження особистості користувача і надаючи ряд істотних переваг порівняно з традиційними методами автентифікації [1]:

– Захист від шахрайства та крадіжок: біометричні дані, такі як відбитки пальців або риси обличчя, є унікальними для кожної людини та важко підроблюваними. Це робить біометричну автентифікацію ефективним інструментом захисту від шахрайства та крадіжок особистих даних. Наприклад, відбитки пальців мають унікальний візерунок, який формується ще до народження і залишається незмінним протягом усього життя, що робить їх надійним засобом ідентифікації.

– Підвищення рівня безпеки: біометрична автентифікація додає додатковий рівень захисту до традиційних методів, таких як паролі та PIN-коди, які можуть бути забуті, втрачені або вгадані. Біометричні дані не можна забути або передати іншій особі, що робить їх більш безпечними, ніж традиційні методи автентифікації.

– Зручність і простота використання: біометричні дані завжди з нами – їх неможливо забути або втратити. Це робить біометричну автентифікацію зручним та простим у використанні методом підтвердження особистості. Наприклад, для розблокування смартфона за допомогою відбитка пальця потрібно лише доторкнутися до сканера, що набагато швидше та зручніше, ніж вводити пароль.

– Моніторинг і контроль доступу: біометричні системи дозволяють точно відстежувати, хто і коли отримував доступ до певних ресурсів або приміщень. Це допомагає виявляти підозрілу активність та запобігати несанкціонованому доступу. Наприклад, компанії можуть використовувати біометричні системи контролю доступу для відстеження того, які співробітники та коли входили до певних приміщень, що допомагає забезпечити безпеку конфіденційних даних.

– Підвищення довіри та відповідності вимогам: використання біометричної автентифікації сприяє підвищенню довіри до систем та послуг, оскільки вона вважається більш надійним методом підтвердження особистості. Більше того, біометрична автентифікація допомагає організаціям відповідати вимогам регуляторних органів щодо захисту даних. Наприклад, використання біометричних паспортів допомагає країнам відповідати вимогам Міжнародної організації цивільної авіації (ICAO) щодо безпеки документів.

– Розпізнавання та реагування на загрози: біометричні системи можуть бути інтегровані з іншими засобами безпеки, такими як системи відеоспостереження або аналізу поведінки користувачів, для своєчасного виявлення та реагування на потенційні загрози. Наприклад, система розпізнавання обличчя може бути використана для ідентифікації підозрілих осіб у натовпі, що дозволяє правоохоронним органам швидко вжити заходів [4].

2.2 Методи підвищення безпеки

Біометрична автентифікація сама по собі є значним кроком у підвищенні безпеки пристроїв та додатків, але її можна зробити ще надійнішою за допомогою наступних методів:

1. Використання багатофакторної автентифікації (MFA): MFA передбачає використання декількох факторів автентифікації для підтвердження особистості користувача. Це може бути комбінація біометричних даних (наприклад, відбиток пальця) та знання (наприклад, пароль) або володіння (наприклад, смартфон). MFA значно ускладнює завдання зловмисникам, оскільки

їм потрібно буде отримати доступ до декількох факторів, щоб розблокувати пристрій або отримати доступ до даних [5].

2. Використання безпечних методів зберігання біометричних даних: біометричні дані повинні зберігатися в зашифрованому вигляді та захищатися від несанкціонованого доступу. Сучасні мобільні пристрої використовують апаратні засоби шифрування, такі як Secure Enclave від Apple або TrustZone від ARM, для захисту біометричних даних. Більше того, біометричні шаблони (математичні представлення біометричних даних) не повинні зберігатися в відкритому вигляді, а повинні бути захищені незворотнім шифруванням, щоб їх не можна було відновити навіть у разі витоку даних.

3. Налаштування блокування пристрою: користувачі повинні налаштовувати автоматичне блокування пристрою після певного періоду неактивності. Це запобігає несанкціонованому доступу до пристрою, якщо він буде загублений або вкрадений. Більшість мобільних пристроїв дозволяють користувачам налаштувати час автоматичного блокування, а також вибрати, які дії потрібно виконати для розблокування (наприклад, введення PIN-коду, використання відбитка пальця або розпізнавання обличчя).

4. Відстеження та управління пристроями: сервіси, такі як Find My iPhone від Apple або Find My Device від Google, дозволяють користувачам відстежувати місцезнаходження своїх пристроїв, віддалено блокувати їх або навіть стирати дані у разі втрати або крадіжки. Це значно знижує ризик несанкціонованого доступу до даних на загубленому або вкраденому пристрої.

5. Використання додаткових засобів захисту - крім біометричної автентифікації, користувачі повинні використовувати інші засоби захисту своїх мобільних пристроїв, такі як:

– Антивірусні програми та фаєрволи: допомагають захистити пристрій від шкідливого програмного забезпечення, яке може бути використане для крадіжки даних або отримання несанкціонованого доступу.

– VPN (Virtual Private Network): VPN шифрує весь трафік між пристроєм та Інтернетом, що робить його більш безпечним для передачі конфіденційної інформації, такої як дані банківських карток або паролі.

– Двофакторна автентифікація (2FA): 2FA додає додатковий рівень безпеки, вимагаючи від користувача не тільки біометричних даних, але й одноразового коду, що надсилається на телефон або електронну пошту.

– Регулярне оновлення програмного забезпечення: оновлення програмного забезпечення часто містять виправлення вразливостей безпеки, тому важливо встановлювати їх своєчасно.

2.3 Інструменти біометричної автентифікації

2.3.1 Бібліотека Dlib

Розпізнавання обличчя є однією з найпопулярніших та активно досліджуваних областей біометрії. Python пропонує декілька бібліотек, які дозволяють розробникам створювати власні системи розпізнавання обличчя або інтегрувати їх у вже існуючі проекти.

Dlib – це універсальна бібліотека з відкритим кодом, яка надає широкий спектр інструментів для машинного навчання та комп'ютерного зору. Написана на C++, вона має зручні обгортки для Python, що робить її доступною для широкого кола розробників. Dlib знаходить застосування в різних галузях, включаючи біометричну автентифікацію, де її потужні алгоритми та висока точність роблять її незамінним інструментом.

Однією з ключових переваг Dlib є її потужний функціонал для обробки зображень. Бібліотека надає інструменти для завантаження, відображення, маніпулювання та аналізу зображень різних форматів. Завдяки цьому, Dlib може бути використана для попередньої обробки зображень перед їх передачею до алгоритмів розпізнавання, що значно підвищує точність та ефективність біометричних систем.

Особливо важливою є вбудована підтримка розпізнавання обличчя. Dlib використовує передові алгоритми машинного навчання, такі як HOG (Histogram of Oriented Gradients) (див. рис. 2.1) та deep metric learning, для виявлення та розпізнавання обличь на зображеннях. HOG дозволяє виявляти обличчя на

зображенні незалежно від їхнього положення та розміру, а deep metric learning дозволяє створювати компактні вектори, які описують унікальні риси обличчя, що спрощує процес порівняння та ідентифікації.

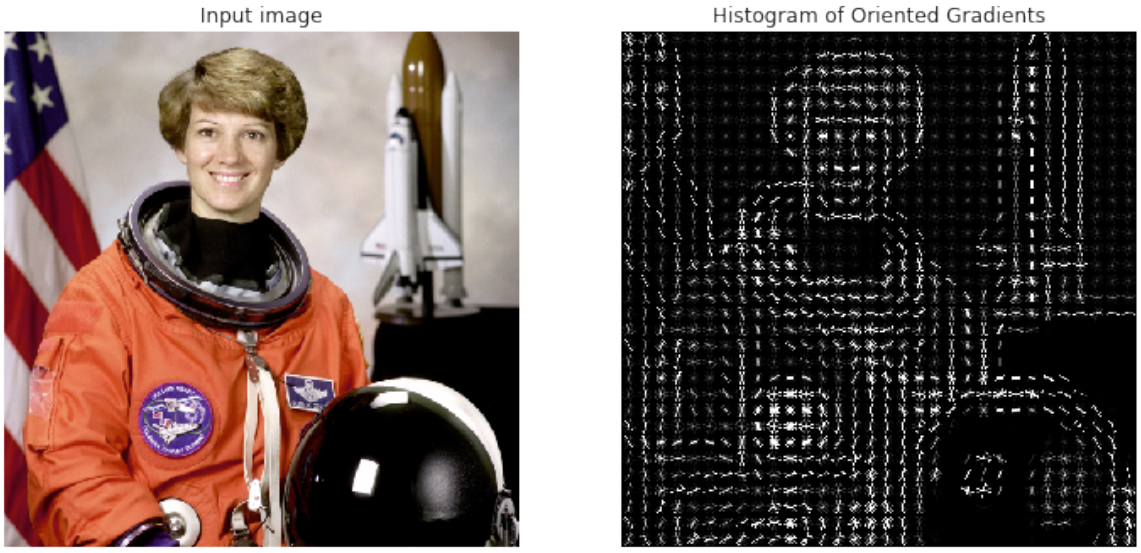

Рисунок 2.1 - Гістограма орієнтованих градієнтів

Dlib пропонує потужну модель виявлення обличчя, яка не лише визначає їх наявність на зображенні, але й точно локалізує ключові точки, такі як очі, ніс та рот [6]. Ця функціональність зробила Dlib незамінним інструментом у багатьох застосунках комп'ютерного зору та розпізнавання обличчя.

2.3.2 Face Recognition

Це бібліотека з відкритим кодом, яка спрощує процес розпізнавання обличчя за допомогою Python. Вона побудована на основі бібліотеки Dlib для досягнення високої точності розпізнавання. Однією з ключових переваг Face Recognition є її простота використання. Бібліотека абстрагує складні деталі реалізації алгоритмів розпізнавання обличчя, дозволяючи розробникам зосередитися на вирішенні конкретних завдань. За допомогою лише кількох рядків коду можна створити систему, яка здатна виявляти та розпізнавати обличчя на зображеннях та відео. Проте, незважаючи на свою простоту, Face Recognition забезпечує високу точність розпізнавання завдяки використанню передових

методів машинного навчання, таких як deep metric learning. Цей алгоритм дозволяє створювати компактні вектори, які описують унікальні риси обличчя, що полегшує процес порівняння та ідентифікації (див. рисунок 2.3). Завдяки цьому, Face Recognition може досягати точності розпізнавання, порівнянної з більш складними бібліотеками, такими як Dlib.

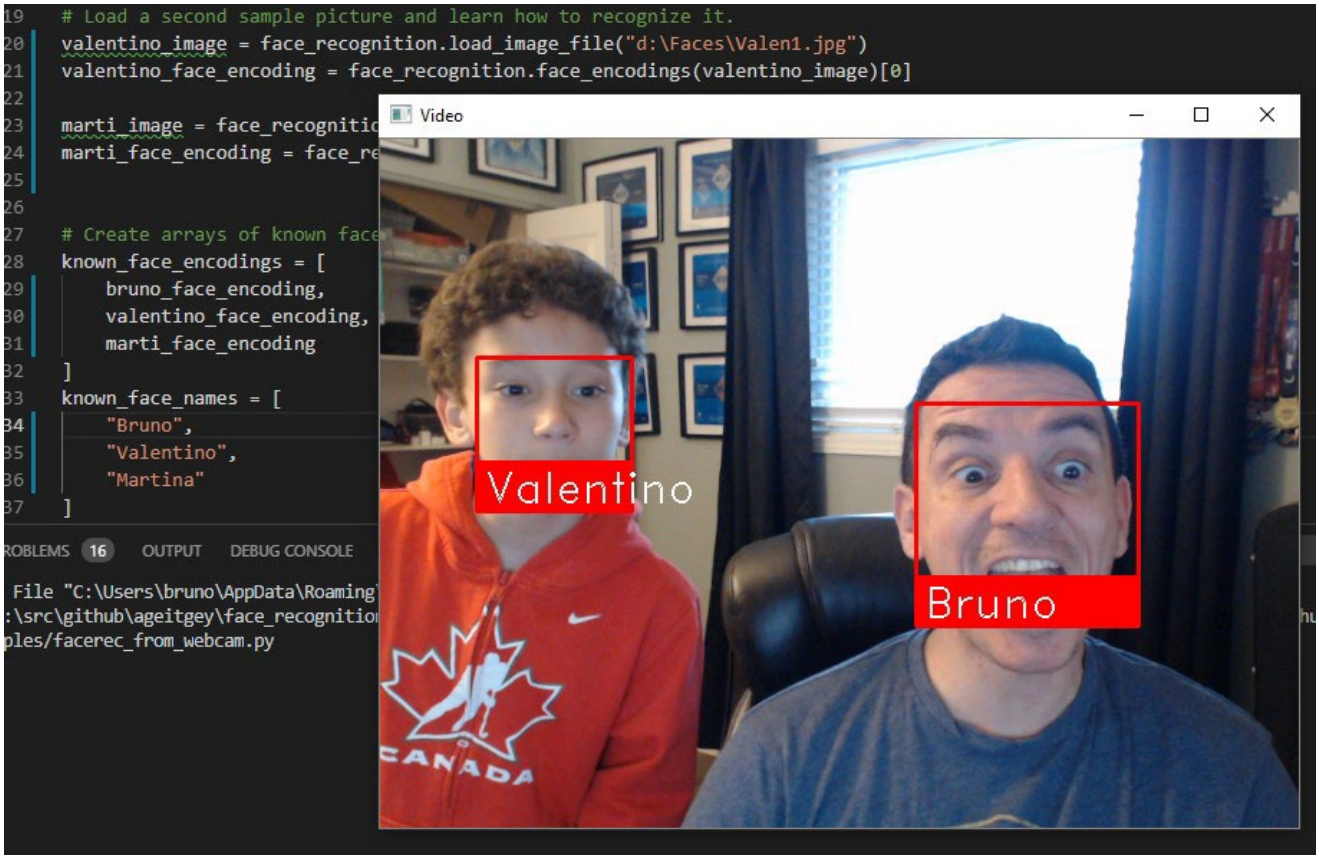

Рисунок 2.3 - Face Recognition

2.3.3 Бібліотека Librosa

Аналіз голосу є ще одним перспективним напрямком біометричної автентифікації. Python пропонує кілька бібліотек, які дозволяють розробникам працювати з аудіоданими та створювати системи розпізнавання голосу.

Librosa - це відкрита бібліотека Python, призначена для аналізу музики та аудіо. Вона надає широкий спектр функцій та інструментів для завантаження, маніпулювання, аналізу та відображення аудіосигналів (див. рисунок 2.4). Хоча її основний фокус спрямований на музичний аналіз, Librosa також знаходить

застосування в інших областях, включаючи біометричну автентифікацію, де аналіз голосових даних відіграє важливу роль. Хоча Librosa не призначена спеціально для біометричної автентифікації, її можливості роблять її цінним інструментом для аналізу голосових даних, які можуть бути використані для ідентифікації особистості.

Librosa може бути використана для вилучення широкого спектру голосових ознак, таких як MFCC (Mel-Frequency Cepstral Coefficients), спектральні ознаки, ритмічні ознаки тощо. Ці ознаки можуть бути використані для створення унікального голосового профілю користувача, який потім можна порівняти з іншими зразками для ідентифікації.

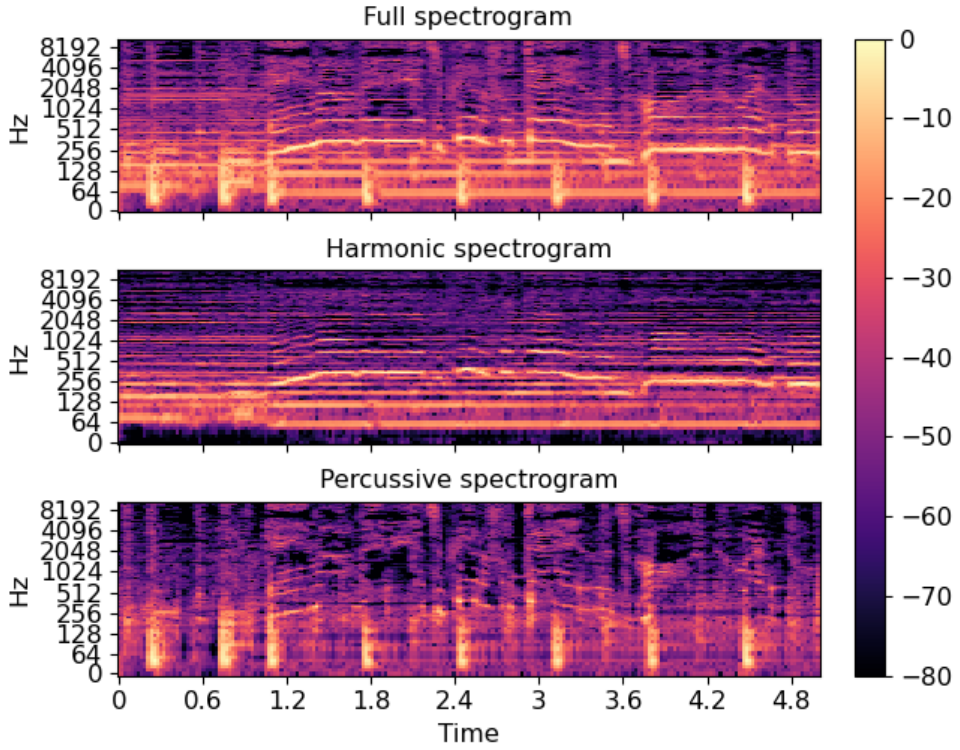

Рисунок 2.4 - Інтерфейс спектрограм у Librosa

Також, Librosa інтегрується з іншими бібліотеками машинного навчання, такими як scikit-learn, що дозволяє використовувати вилучені ознаки для навчання моделей розпізнавання голосу. Ці моделі можуть бути використані для ідентифікації користувачів за їхнім голосом, наприклад, для доступу до банківських рахунків або розблокування смартфонів.

Ця чудова бібліотека навіть може бути використана для аналізу голосових

даних з метою виявлення емоційного стану людини (наприклад, радості, гніву, страху) або навіть деяких захворювань (наприклад, хвороби Паркінсона).

2.3.4 SpeechRecognition

SpeechRecognition – це потужна та універсальна бібліотека Python, що спрощує процес розпізнавання мови. Вона надає простий та зручний інтерфейс для роботи з різними рушіями розпізнавання мови, включаючи як онлайн-сервіси (Google Web Speech API, Microsoft Bing Speech API, IBM Speech to Text), так і офлайн-двигуни (CMU Sphinx). Завдяки своїй гнучкості та простоті використання, SpeechRecognition є ідеальним інструментом для розробки різноманітних застосунків, пов'язаних з голосовим управлінням, транскрипцією аудіо та, звичайно ж, біометричною автентифікацією.

SpeechRecognition може бути використана для створення систем біометричної автентифікації на основі розпізнавання голосу. Це може включати такі сценарії використання як ідентифікацію та верифікацію за голосом і безперервна автентифікація. Користувач може вимовити певну фразу або пароль, а система розпізнавання мови порівняє його голос зі збереженим зразком для підтвердження особистості. Система може попросити користувача вимовити випадкову фразу або відповісти на запитання, щоб переконатися, що він є тим, за кого себе видає і вона буде постійно моніторити голос користувача під час використання пристрою або програми та виявляти будь-які зміни, які можуть свідчити про несанкціонований доступ.

SpeechRecognition є потужним та зручним інструментом для розробників, які хочуть інтегрувати функціонал розпізнавання мови у свої проекти. Незважаючи на деякі обмеження, бібліотека пропонує широкий спектр можливостей та дозволяє створювати різноманітні застосунки, включаючи системи біометричної автентифікації на основі голосу.

2.3.5 PyAudioAnalysis

PyAudioAnalysis - це відкрита бібліотека Python, призначена для широкого спектру завдань аналізу аудіосигналів.

Хоча її основний фокус спрямований на вилучення ознак, класифікацію та сегментацію аудіо, її потужний функціонал та гнучкість роблять її привабливим інструментом для дослідників та розробників, які працюють у сфері біометричної автентифікації.

Бібліотека дозволяє вилучати широкий спектр акустичних ознак, таких як MFCC, спектрограми, хромограми, спектральний контраст та багато інших. Ці ознаки можуть бути використані для характеристики звукових сигналів та їх подальшої класифікації та для створення унікального голосового профілю користувача, який потім можна порівняти з іншими зразками для ідентифікації.

Вбудовані класифікатори можуть бути використані для класифікації голосових зразків за різними параметрами (наприклад, стать, вік, емоційний стан) або для верифікації особистості користувача шляхом порівняння його голосу зі збереженим зразком.

Бібліотека надає готові до використання класифікатори, такі як k-NN, SVM, Random Forests та Gradient Boosting, які можуть бути використані для класифікації аудіо сегментів за різними категоріями (наприклад, музика, мова, шум).

Містить алгоритми для сегментації аудіопотоків на однорідні сегменти, що може бути корисним для ідентифікації мовних сегментів, виявлення музичних фрагментів або видалення шумів та створює різноманітні візуалізації аудіоданих, такі як спектрограми, хромограми та інші, що допомагає візуально аналізувати та інтерпретувати дані.

Також може бути використана для розробки алгоритмів виявлення живого мовлення (Liveness Detection), які дозволяють відрізнити справжній голос людини від запису або імітації. Це важливий аспект безпеки біометричних систем, оскільки допомагає запобігти атакам за допомогою підроблених голосових зразків.

PyAudioAnalysis є цінним інструментом для аналізу аудіо, який можна використовувати для розробки ефективних систем біометричної автентифікації на основі голосу. Завдяки своїм широким можливостям та гнучкості, вона дозволяє дослідникам та розробникам експериментувати з різними підходами та створювати інноваційні рішення.

2.4 Висновки до другого розділу

Біометрична автентифікація є потужним інструментом підвищення безпеки не тільки для мобільних пристроїв та додатків, а й для ПК та ноутбуків. Вона пропонує зручний, безпечний та надійний спосіб підтвердження особистості користувача. Однак, для досягнення максимальної безпеки необхідно використовувати біометричну автентифікацію в комплексі з іншими методами захисту, такими як багатофакторна автентифікація, безпечне зберігання даних, налаштування блокування пристрою, відстеження та управління пристроями, а також використання додаткових засобів захисту. В зв’язку з чим, розглянуто методи та інструменти біометричної автентифікації.

3 РЕАЛІЗАЦІЯ МЕТОДУ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

3.1 Налаштування БА завдяки розпізнавання обличчя у Windows Hello

Налаштування Windows Hello з використанням розпізнавання обличчя для біометричної автентифікації є простим та інтуїтивно зрозумілим процесом, який дозволяє користувачам швидко та безпечно входити до своїх пристроїв з Windows 10 або Windows 11.

Створивши обліковий запис Microsoft та авторизувавшись у свої системі, налаштуємо автентифікацію за допомогою Windows Hello (див. рисунок 3.1).

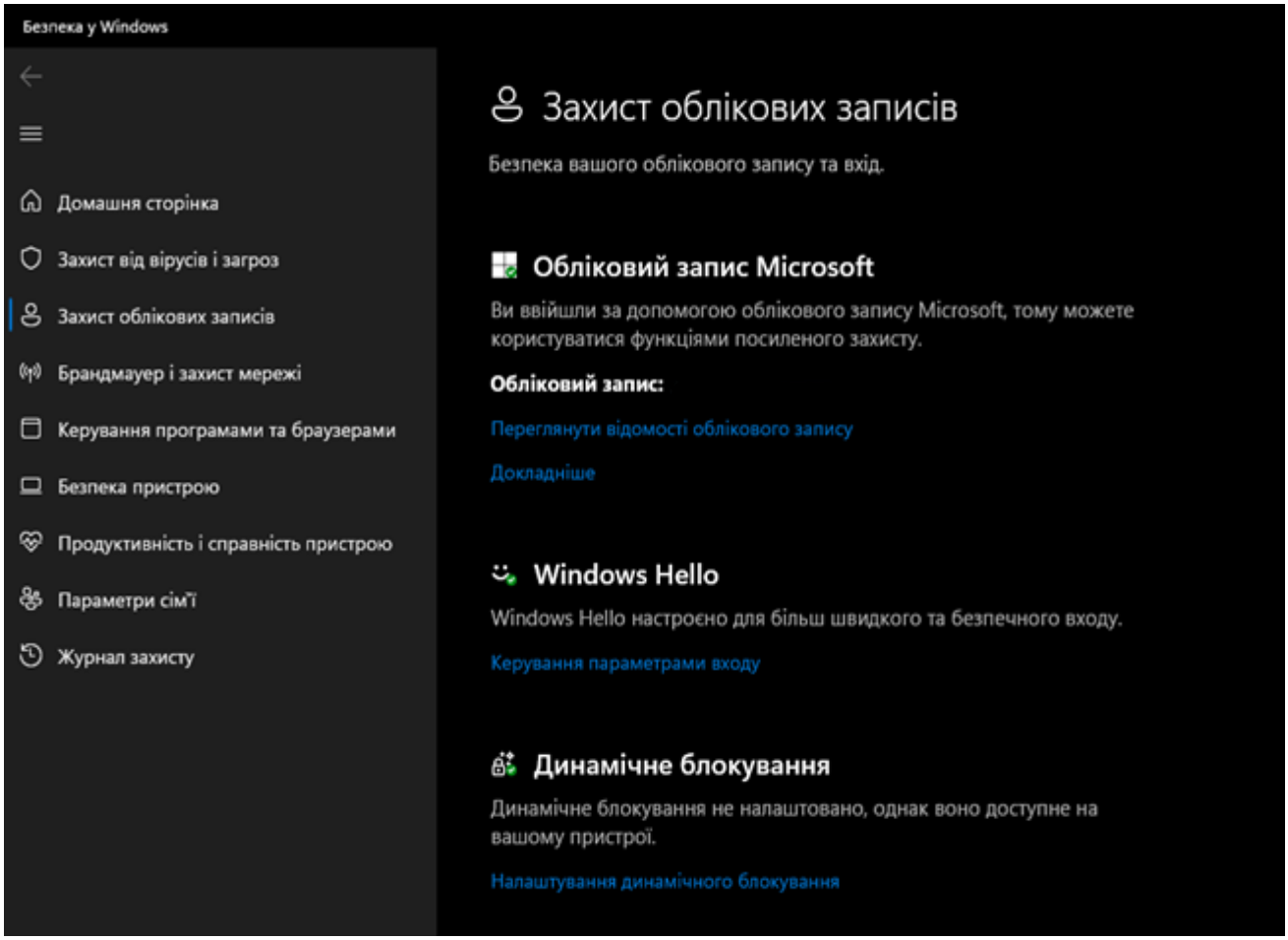

Рисунок 3.1 – Захист облікових записів за допомогою Windows Hello

Перед початком налаштування треба переконатись, що пристрій підтримує Windows Hello з розпізнаванням обличчя.

Рисунок 3.2 - Диспетчер пристроїв

Для цього потрібна спеціальна камера з інфрачервоним сенсором, яка здатна розпізнавати обличчя в різних умовах освітлення.

Більшість сучасних ноутбуків та деякі зовнішні веб-камери мають таку функцію. Якщо опції входу за обличчям недоступні, то на пристрої немає камери з інфрачервоним сенсором.

Перевірити наявність такої камери можна системно. Для цього відкриємо диспетчер пристроїв натиснувши праву клавішу миші на іконку Пуску і вибираємо потрібний пункт (див. рисунок 3.2).

У новому вікні потрібно знайти пункт, який відповідає за робочі камери.

Упевнившись, що камера має інфрачервоний сенсор (наявність приставки “IR” у назві камери), переходимо до наступного кроку (див. рисунок 3.3).

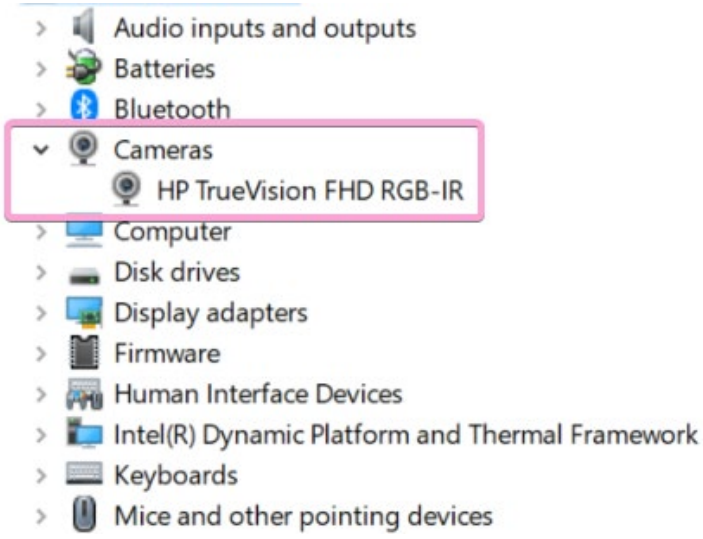

Рисунок 3.3 - Камера з підтримку інфрачервоного сенсора

Треба зазначити, що Windows Hello — спосіб входу не лише до пристроїв, а й програм, онлайн-сервісів і мереж. Це безпечніше, ніж використання суто пароля, тому що Windows Hello підтримує три варіанти входу в обліковий запис системи (див. рисунок 3.4):

– розпізнавання обличчя, щоб настроїти вхід за допомогою інфрачервоної камери комп'ютера або зовнішньої інфрачервоної камери;

– розпізнавання відбитків пальців, щоб налаштувати вхід за допомогою сканера відбитків пальців;

– PIN-код, щоб налаштувати вхід за допомогою PIN-коду.

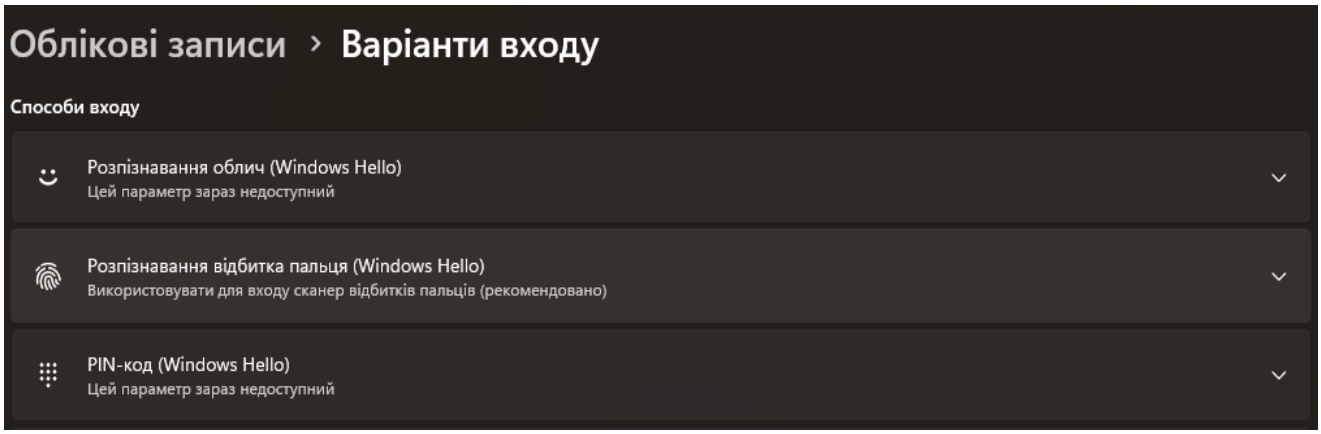

Рисунок 3.4 – Можливі варіанти входу за допомогою Windows Hello

Серед можливих варіантів ходу вибираємо пункт розпізнавання обличчя або

“Windows Hello Face”.

Рисунок 3.4 – Вікно привітання для початку налаштування

У новому вікні необхідно подивитися у центр об’єктиву камери, щоб вона змогла зафіксувати риси обличчя і занести деталі в персональну базу даних для подальшої верифікації обличчя користувача, який бажає розблокувати пристрій (див. рисунок 3.5).

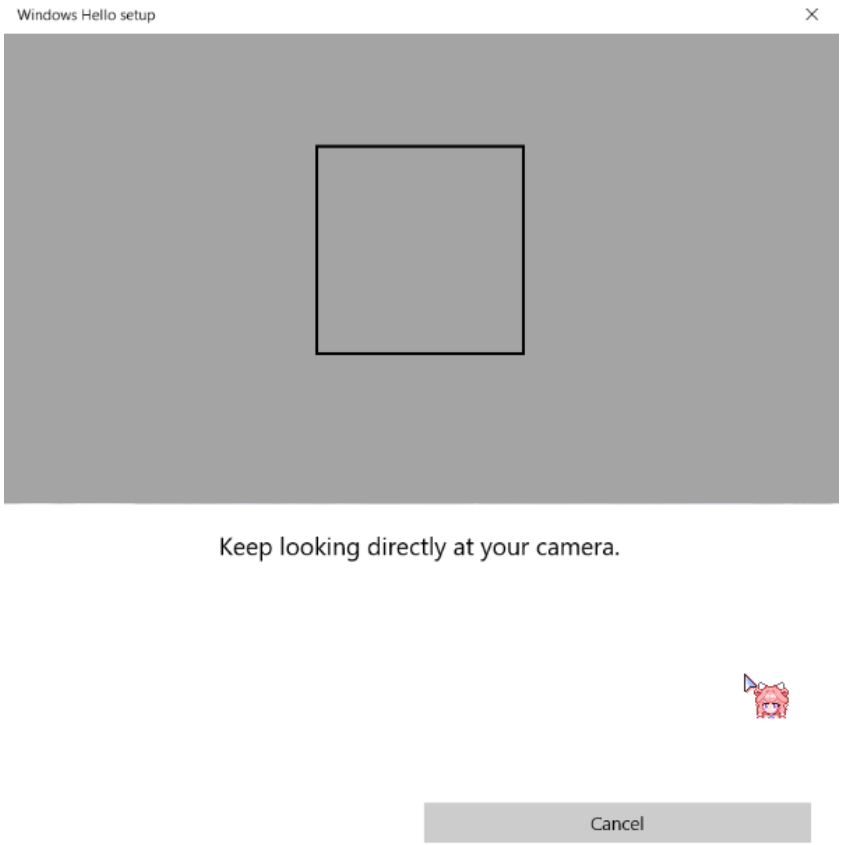

Рисунок 3.5 - Налаштування біометрії

Також можна покращити розпізнавання власника пристрою, натиснувши на відповідну опцію “Покращити розпізнавання”. Завдяки цьому можна додатково налаштувати розпізнавання обличчя з окулярами чи іншими аксесуарами, які змінюють вашу зовнішність (див. рисунок 3.6).

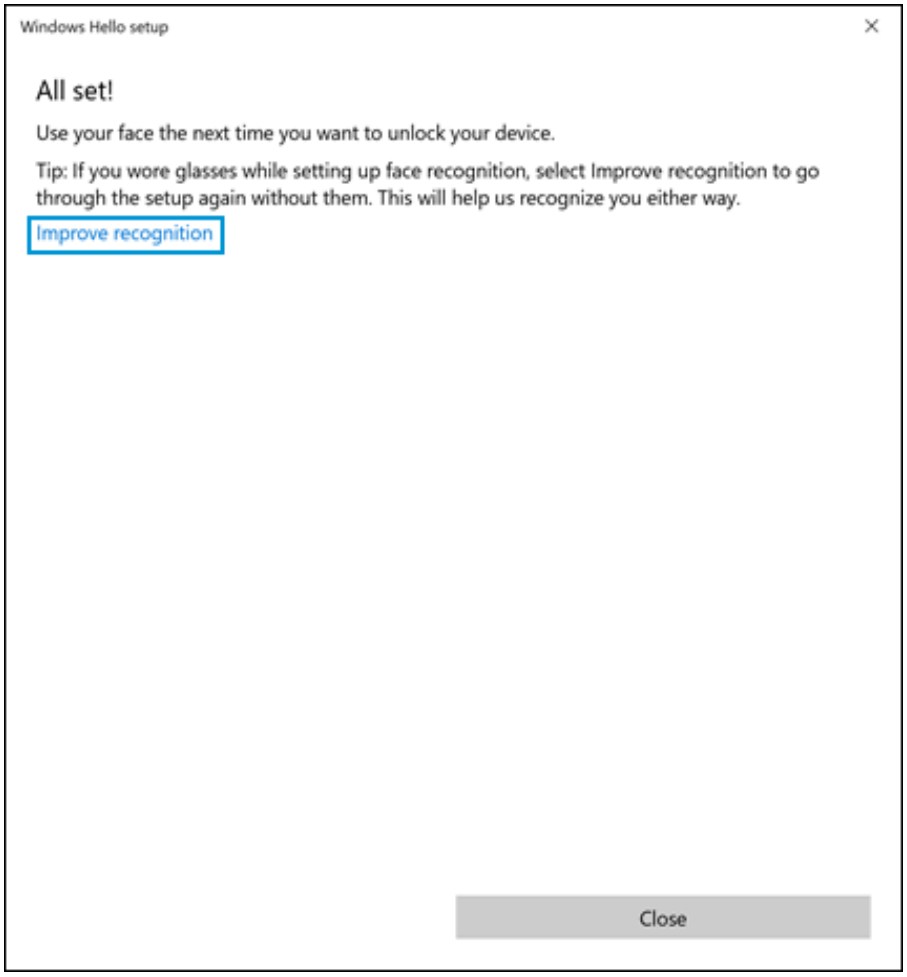

Рисунок 3.6 – Поліпшення розпізнавання

Останнім кроком буде налаштування PIN-коду для забезпечення додаткового захисту у екстрених випадках. Наприклад, якщо камера вийде зі строю, ми зможемо авторизуватись завдяки цьому PIN-коду.

На цьому налаштування Windows Hello завершено.

3.2 Принцип дії розпізнавання обличчя

Для розпізнавання обличь використовуються алгоритми машинного навчання, такі як HOG (Histogram of Oriented Gradients, гістограма спрямованих

градієнтів) та лінійному алгоритмі машинного навчання SVM (Support Vector Machines, метод опорних векторів):

1. Основна ідея HOG полягає в наступних кроках:

Крок 1. Поділити зображення на маленькі з'єднані клітинки.

Крок 2. Обчислити гістограму для кожної клітинки.

Крок 3. Об'єднати всі гістограми разом, щоб сформувати одну унікальну для кожного обличчя гістограму.

2. SVM є алгоритмом класифікації, що визначає гіперплощину, яка робить поділ між класами. Функцію прийняття рішень SVM можна виразити як:

$$f(x) = sign\left(\sum_{i=1}^{N} a_i y_i K(x_i, x) + b\right), \quad (1.1)$$

де N — розмір навчальних даних, K — функція ядра, яка вимірює подібність між x_i (опорний вектор) і x (значення ознак), α_i — множник Лагранжа, y_i представляє клас належності кожного даного (±1) , а b — числова константа [7].

Лінійний SVM: функція ядра виражається як внутрішній добуток опорного вектора та значень ознак:

$$K(x_i, x) = x_i^T \cdot x. \quad (1.2)$$

Фактично, HoG застосовується для обчислення дескрипторів, що використовуються для навчання лінійної SVM, яка виявляє обличчя [8].

За допомогою навченої моделі отримуються орієнтири або ключові точки на знайденому обличчі.

Однією з відомих функцій вже раніше згаданої бібліотеки Dlib є модель для виявлення обличчя, сама яка і включає ключові точки на обличчі (див. рисунок 3.7), що робить її популярною для реалізації різноманітних додатків у сфері комп'ютерного зору та розпізнавання обличчя.

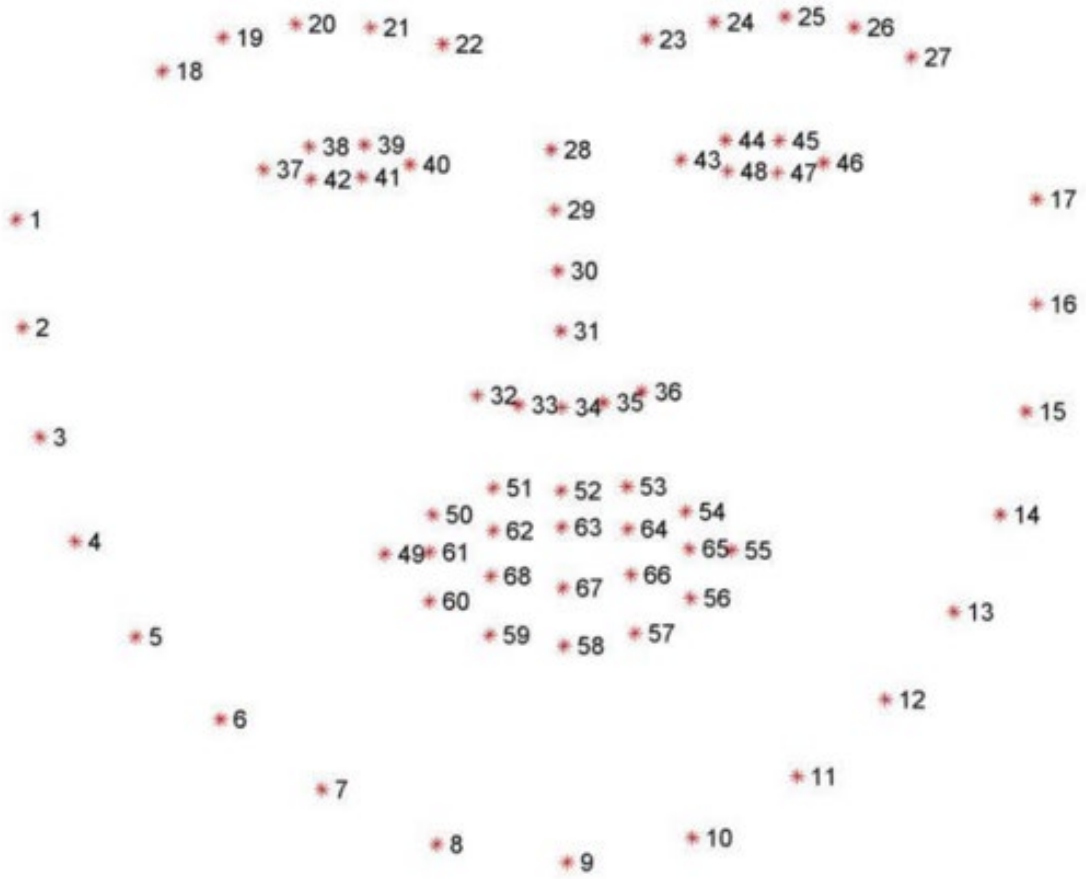

Рисунок 3.7 - Візуалізація ознак обличчя

Алгоритм розпізнавання обличчя за допомогою Dlib наведено на рисунку 3.8.

Бібліотека Dlib є більш точною, ніж бібліотека OpenCV, якщо використовувати її для виявлення обличчя на зображеннях. Ця точність пояснюється тим, що Dlib має більше моделей розпізнавання обличчя [9]. Орієнтирами обличчя є індексовані списки, які зображені на рисунку 3.7.

Принцип дії Windows Hello при розпізнавання обличчя той самий. Біометрична автентифікація дозволяє ідентифікувати та провести верифікацію людини на основі набору специфічних та унікальних рис, властивих їй від

народження, які завжди присутні на людині, унікальні та вкрай незмінні у часі, і даному випадку мова іде про обличчя [10].

Спочатку в персональній базі даних зберігається еталонна модель, заснована на біометричних характеристиках людини - обличчя. Для цього можуть використовуватись один або кілька біометричних зразків.

Збережені дані перетворюються на математичний код; таким чином формується база даних, що є набором кодів до 1000 біт, що фіксують унікальні біометричні характеристики користувачів. При зчитуванні сканер не розпізнає саме зображення, а перетворює його на цифровий код, який потім порівнює із завантаженою раніше еталонною моделлю [11].

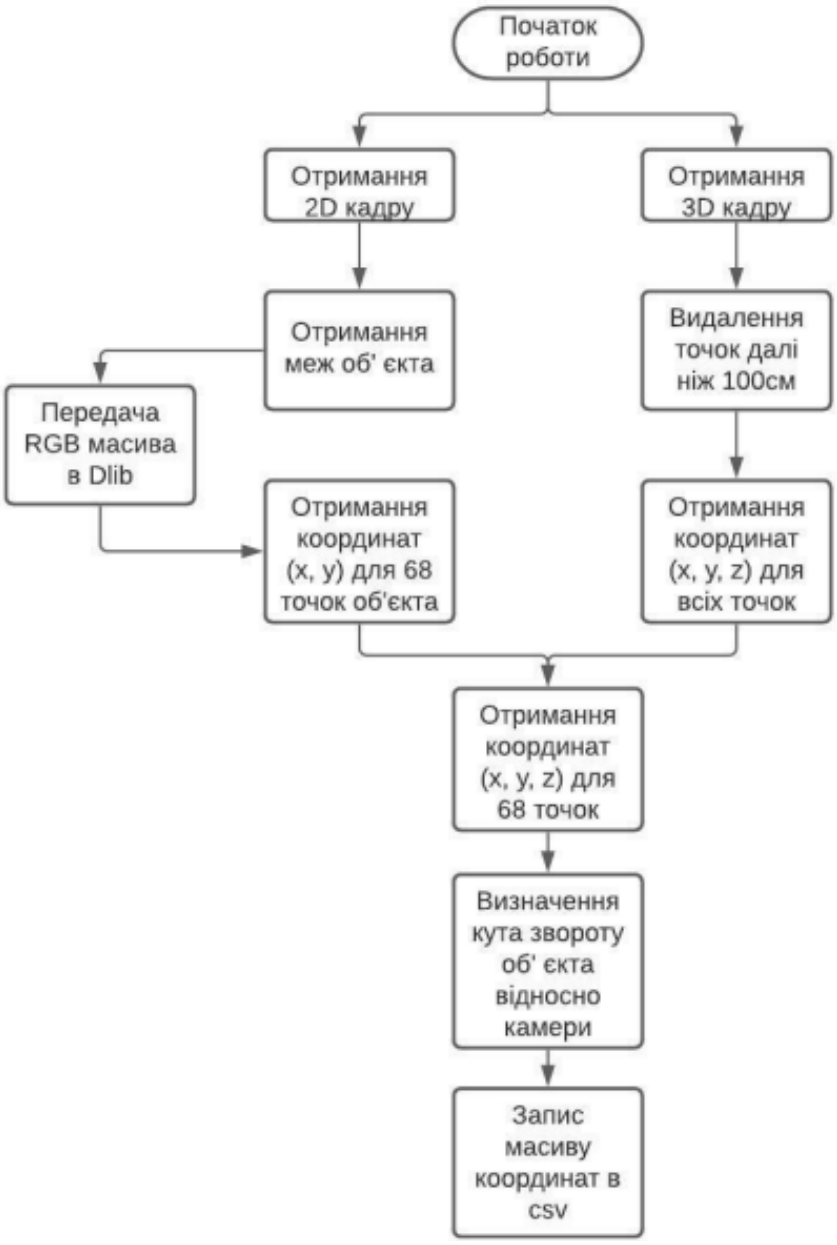

Рисунок 3.8 – Алгоритм визначення очей за допомогою Dlib

Лістинг 3.1 – Детектор обличчя

```
import sys

import dlib

detector = dlib.get_frontal_face_detector()
win = dlib.image_window()

for f in sys.argv[1:]:
    print("Processing file: {}".format(f))
    img = dlib.load_rgb_image(f)
    dets = detector(img, 1)
    print("Number of faces detected: {}".format(len(dets)))
    for i, d in enumerate(dets):
        print("Detection {}: Left: {} Top: {} Right: {}
Bottom:{}".format(i, d.left(), d.top(), d.right(), d.bottom()))

    win.clear_overlay()
    win.set_image(img)
    win.add_overlay(dets)
    dlib.hit_enter_to_continue()


if (len(sys.argv[1:]) > 0):
    img = dlib.load_rgb_image(sys.argv[1])
    dets, scores, idx = detector.run(img, 1, -1)
    for i, d in enumerate(dets):
        print("Detection {}, score: {}, face_type:{}".format(
            d, scores[i], idx[i]))
```

3.3 Висновки до третього розділу

У третьому розділі було проведено налаштування біометричної автентифікації у Windows Hello для захисту облікових записів від несанкціонованого доступу. Та розглянуто принцип дії розпізнавання обличчя на прикладі використовуються алгоритмів машинного навчання, таких як HOG (гістограма спрямованих градієнтів) та лінійному алгоритмі машинного навчання SVM (метод опорних векторів).

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ ТА ОХОРОНА ПРАЦІ

4.1 Долікарська допомога при кровотечах

Кровотеча – це витікання крові з пошкоджених кровоносних судин. Залежно від типу пошкодженої судини кровотечі поділяють на артеріальні, венозні, капілярні та паренхіматозні.

Артеріальна кровотеча виникає при пошкодженні артерій. Кров яскраво-червоного кольору, витікає пульсуючим струменем. Така кровотеча є найбільш небезпечною, оскільки призводить до швидкої втрати великої кількості крові.

Венозна кровотеча виникає при пошкодженні вен. Кров темно-червоного кольору, витікає рівномірним струменем. Венозна кровотеча менш інтенсивна, ніж артеріальна, але також може бути небезпечною, особливо при пошкодженні великих вен.

Капілярна кровотеча виникає при пошкодженні капілярів. Кров витікає по всій поверхні рани краплями або сочитися. Капілярна кровотеча зазвичай не є небезпечною і зупиняється самостійно.

Паренхіматозна кровотеча виникає при пошкодженні внутрішніх органів (печінки, селезінки, нирок). Кров витікає як із зовнішньої поверхні органу, так і в його порожнину. Паренхіматозна кровотеча є дуже небезпечною і вимагає негайної медичної допомоги.

Долікарська допомога при кровотечах

При наданні долікарської допомоги при кровотечах необхідно дотримуватись наступних принципів:

1. Оцінка ситуації та забезпечення безпеки. Перед наданням допомоги переконайтеся, що місце події безпечне для вас та постраждалого. Якщо є небезпека, вживіть заходів щодо її усунення або перенесіть постраждалого у безпечне місце.

2. Виклик швидкої медичної допомоги. Негайно викличте швидку медичну допомогу, особливо якщо кровотеча сильна, не зупиняється самостійно

або постраждалий має ознаки шоку (блідість, холодний піт, запаморочення, втрата свідомості).

3. Зупинка кровотечі. Залежно від типу кровотечі застосовують різні методи зупинки:

- Прямий тиск на рану. Найпростіший і найефективніший спосіб зупинки капілярної та невеликої венозної кровотечі. Накладіть на рану стерильну пов'язку або чисту тканину і сильно притисніть її рукою. Утримуйте тиск до приїзду швидкої допомоги.
- Підняття пошкодженої кінцівки. Якщо кровотеча виникла на кінцівці, підніміть її вище рівня серця. Це допоможе зменшити приплив крові до рани та полегшити зупинку кровотечі.
- Накладання джгута. Джгут застосовують лише при сильній артеріальній кровотечі, коли інші методи не допомагають. Джгут накладають вище місця поранення, максимально близько до нього. Важливо правильно накласти джгут, щоб не пошкодити нерви та тканини. Під джгут обов'язково підкладіть м'яку тканину. Запишіть час накладання джгута та передайте цю інформацію медикам. Джгут можна тримати не більше 1-1,5 години, після чого його необхідно послабити на кілька хвилин, а потім знову затягнути.
- Тампонада рани. При глибоких ранах, коли неможливо накласти джгут, застосовують тампонаду. Рану щільно заповнюють стерильними марлевими тампонами або бинтами, а потім накладають пов'язку, що давить.

4. Іммобілізація пошкодженої кінцівки. Якщо кровотеча супроводжується переломом або іншим пошкодженням кінцівки, необхідно забезпечити її нерухомість. Це допоможе запобігти додатковому травмуванню та полегшити зупинку кровотечі.

5. Зігрівання постраждалого. При кровотечі постраждалий швидко втрачає тепло. Тому його необхідно зігріти, накривши ковдрою або одягом.

6. Контроль стану постраждалого. Постійно стежте за станом постраждалого, контролюйте його пульс, дихання та свідомість. При погіршенні стану негайно повідомте про це медикам.

Важливо пам'ятати:

- Не панікуйте, дійте швидко та рішуче.
- Не намагайтеся витягувати з рани сторонні предмети, це може посилити кровотечу.
- Не застосовуйте джгут без крайньої необхідності, оскільки це може призвести до серйозних ускладнень.
- Не давайте постраждалому їсти та пити, оскільки це може ускладнити проведення операції, якщо вона буде потрібна.

Своєчасна та правильна долікарська допомога при кровотечах може врятувати життя постраждалому. Тому важливо знати основні принципи надання допомоги та вміти застосовувати їх на практиці.

4.2 Заходи щодо захисту установки від короткого замикання

Захист установки від короткого замикання є критично важливим аспектом забезпечення безпеки та надійності роботи електрообладнання. Коротке замикання, або струм короткого замикання, виникає при безпосередньому контакті фазного провідника з нульовим або між фазними провідниками, що призводить до різкого збільшення струму в електричному колі. Це може спричинити перегрівання проводів, пошкодження ізоляції, виникнення пожежі та інші небезпечні наслідки. Тому важливо вжити комплексних заходів, щоб запобігти цьому явищу та мінімізувати його негативний вплив.

Перш за все, необхідно забезпечити надійну ізоляцію струмоведучих частин електроустановки. Це досягається шляхом використання якісних ізоляційних матеріалів, таких як полівінілхлорид (ПВХ), поліетилен (ПЕ), гума та інші. Ізоляція повинна бути цілісною, без тріщин, пошкоджень та інших дефектів. Також важливо правильно підібрати ізоляцію за номінальною напругою та умовами експлуатації.

Наступним важливим заходом є застосування плавких запобіжників та автоматичних вимикачів. Плавкі запобіжники є найпростішим та найдешевшим засобом захисту від короткого замикання. Вони встановлюються в електричному колі та розраховані на певний номінальний струм. При перевищенні цього струму,

наприклад, при короткому замиканні, плавка вставка запобіжника розплавляється, розмикаючи коло та запобігаючи подальшому протіканню струму. Автоматичні вимикачі є більш сучасним та надійним засобом захисту. Вони також розраховані на певний номінальний струм, але при його перевищенні спрацьовує електромагнітний або тепловий розчіплювач, який відключає живлення. Автоматичні вимикачі мають перевагу перед плавкими запобіжниками в тому, що їх можна багаторазово використовувати після відключення.

Ще одним ефективним засобом захисту від короткого замикання є пристрої захисного відключення (ПЗВ). Вони реагують на витік струму, який може виникнути при пошкодженні ізоляції або дотику людини до струмоведучих частин. ПЗВ постійно контролюють різницю струмів у фазному та нульовому провідниках. Якщо ця різниця перевищує допустиме значення, ПЗВ миттєво відключає живлення, запобігаючи ураженню електричним струмом. ПЗВ є обов'язковими для встановлення у вологих приміщеннях та в місцях з підвищеною небезпекою ураження електричним струмом.

Важливим заходом захисту від короткого замикання є також заземлення та занулення електроустановок. Заземлення – це навмисне електричне з'єднання корпусу або інших струмоведучих частин електроустановки із землею. Воно забезпечує безпеку при пробої ізоляції, відводячи струм у землю та запобігаючи ураженню електричним струмом. Занулення – це з'єднання корпусу або інших струмоведучих частин електроустановки з нульовим захисним провідником. Воно також забезпечує захист від ураження електричним струмом, але відрізняється від заземлення тим, що нульовий захисний провідник підключений до нейтралі джерела живлення.

Для захисту від перенапруг, які можуть виникнути внаслідок грозових розрядів, комутаційних процесів або інших причин, використовують розрядники, варистори та інші пристрої. Розрядники встановлюються на лініях електропередач та призначені для відведення імпульсних перенапруг у землю. Варистори – це напівпровідникові елементи, які змінюють свій опір залежно від прикладеної напруги. При перенапрузі опір варистора різко зменшується, що дозволяє відвести надлишок енергії у тепло.

Крім технічних засобів захисту, важливо також дотримуватись правил експлуатації електрообладнання та проводити регулярні перевірки його стану. Необхідно своєчасно усувати несправності, замінювати зношені деталі та проводити профілактичне обслуговування. Також важливо не перевищувати допустимі навантаження на електрообладнання та використовувати його за призначенням.

У разі виникнення короткого замикання необхідно негайно відключити живлення та вжити заходів щодо усунення причини. Якщо коротке замикання сталося внаслідок пошкодження ізоляції, необхідно замінити пошкоджений провід або ізоляційний матеріал. Якщо коротке замикання сталося внаслідок перевантаження, необхідно зменшити навантаження або встановити додаткові засоби захисту.

Усі роботи з електрообладнанням повинні проводитись кваліфікованим персоналом з дотриманням правил техніки безпеки. Недотримання цих правил може призвести до серйозних наслідків, включаючи ураження електричним струмом, пожежу та інші небезпечні ситуації.

Захист установки від короткого замикання – це комплексний процес, який вимагає застосування різних технічних засобів та організаційних заходів. Дотримання вищезазначених рекомендацій дозволить забезпечити безпечну та надійну роботу електрообладнання, запобігти виникненню аварійних ситуацій та мінімізувати ризик негативних наслідків.

ВИСНОВКИ

У підсумку, біометричні системи розпізнавання все більше впроваджуються в наше життя, багато в чому полегшуючи його та спрощуючи процеси отримання доступу. Допомагають автоматизувати процеси поведінкового аналізу та виявляти потенційних зловмисників, виявляючись незамінними помічниками на додаток до традиційних методів захисту. Однак, незважаючи на всі вищеописані переваги, варто також згадати про недоліки біометричних систем. Обчислювальне навантаження є однією з ключових проблем у системах біометричної ідентифікації. До того ж, біометрична інформація, як і будь-яка інша, вразлива: банки, лікарні та будь-які інші установи постійно зазнають хакерських атак, і частина інформації потрапляє до рук зловмисників, але одна справа, якщо це – стандартні логін та пароль, а інша – якщо мова йде про біометричні дані. Адже пароль можна змінити, а палець чи райдужку ока – ні. В останньому випадку при компрометації даних зловмисник отримує доступ до всіх активів із біометричною верифікацією. На жаль, необхідно прийняти той факт, що будь-які персональні дані, у тому числі біометричні, не можуть бути повністю захищені від розкрадання. Ряд біометричних характеристик є публічними: обличчя можна сфотографувати, а голос записати на диктофон. Для забезпечення довіри користувачів до біометричної ідентифікації необхідно забезпечити надійність та безпеку використовуваних систем за рахунок: шифрування даних, біометричної ідентифікації в режимі реального часу з перевіркою на живий/неживий або використання мультиспектральних та мультимодальних рішень.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology, 14(1), 4-20.

2. Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.

3. Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (Eds.). (2005). Biometric systems: Technology, design and performance evaluation. Springer Science & Business Media.

4. Jayarathne I, Cohen M, Amarakeerthi S. (2020) Person identification from EEG using various machine learning techniques with inter-hemispheric amplitude ratio. PLoS ONE 15(9): e0238872. https://doi.org/10.1371/journal.pone.0238872.

5. Marasco, E., & Ross, A. (2015). A survey on antispoofing schemes for fingerprint recognition systems. ACM Computing Surveys (CSUR), 47(2), 28.

6. Durna Y, Ari F. Design of a Binocular Pupil and Gaze Point Detection System Utilizing High Definition Images. Applied Sciences. 2017; 7(5):498. https://doi.org/10.3390/app7050498.

7. Y. Boltov, I. Skarga-Bandurova and M. Derkach, "A Comparative Analysis of Deep Learning-Based Object Detectors for Embedded Systems," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 1156-1160, doi: 10.1109/IDAACS58523.2023.10348642.

8. Sedinkin , O., Derkach , M., Skarga-Bandurova , I., & Matiuk , D. (2024). Eye tracking system based on machine learning. COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION, (55), 199-205. https://doi.org/10.36910/6775-2524-0560-2024-55-25

9. Karpinski, M., Korchenko, A., Vikulov, P., Kochan, R., Balyk, A., & Kozak, R. (2017, September). The etalon models of linguistic variables for sniffing-attack detection. In 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications (IDAACS) (Vol. 1,

pp. 258-264). IEEE.

10. Augmented Reality Enhanced Learning Tools Development for Cybersecurity Major Zagorodna N., Skorenkyy Y., Kunanets N., Baran I., Stadnyk M. (2022) CEUR Workshop Proceedings, 3309 , pp. 25-32.

11. Mishko, O. Security of remote IoT system management by integrating firewall configuration into tunneled traffic / O. Mishko, D. Matiuk, M. Derkach // Scientific Journal of TNTU. — Tern.: TNTU, 2024.