МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна інженерія»

Група: 2БКС-27

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання

БКС.27.06.000.КРБ

БОРЩА ОЛЕГА ОЛЕГОВИЧА

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**
Освітня програма: «**Комп'ютерна інженерія»**
Група: **2БКС-27**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційній роботі бакалавра на тему:_____

«Дослідження біометричних систем комп'ютерної ідентифікації особистості»

Проектний матеріал складається з пояснювальної записки на ____60__ сторінках та графічного (презентаційного) матеріалу на ___10___ аркушах (слайдах).

Виконавець _____ (Борщ О. О.)
Керівник _____ (Краснієнко Н.В.)

Консультанти:
з охорони праці_____ (Чорновол Н.І.)
з дотримання вимог ЄСКД _____ (Петрашова В.І.)
старший консультант _____ (Кривченко Ю.В.)

До захисту допущений
Завідувачка кафедри _____ (Іванова Л.В.)
Завідувач відділення _____ (Скорнякова О.В.)

Захист «24» 06 2023 р. Протокол ДКК № 2
Оцінка ДКК 4 (добре)

Секретар ДКК _____

АНОТАЦІЯ

Метою даної роботи «**Дослідження біометричних систем комп'ютерної ідентифікації особистості**» є дослідження та впровадження сучасних біометричних методів ідентифікації особистості.

Методи дослідження - аналіз технологій біометричної ідентифікації особистості, порівняльний аналіз обладнання для таких систем.

У підсумку обрано одну з біометричних систем для побудови системи контролю доступу до об'єкта із використанням смартфонів та програмного забезпечення Azure Cognitive Services Face API.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення **комп'ютерних систем** Комісія **КТ та ПІ**

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **«Комп'ютерна інженерія»**

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР **Ігор Беркань**

"_____" _____2023 р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

Здобувачеві (здобувачці) освіти **Борщу Олегу Олександровичу**

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи

Дослідження біометричних систем комп'ютерної ідентифікації особистості

затверджена наказом по коледжу від "__17_" _____10_____2022__р. №_235-А2-ОД_____

2. Термін здачі кваліфікаційної роботи _____

3. Вихідні данні до проекту (роботи) _____

Об'єкт аналізу – методи та засоби біометричних систем комп'ютерної ідентифікації особистості. Програмне забезпечення API Face Azure Cognitive Services ся для виявлення, розпізнавання і аналізу людських облич на зображенні (2 D).

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

Вступ. 1. Технологічний розділ. 2. Охорона праці. Висновки. Перелік використаних джерел. Додаток

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)

Презентація (10 слайдів) 1. Назва теми 2.Узагальнена структура методів ідентифікації особистості 3. Система захисту інформації в комп'ютерних системах 4. Комплекс заходів щодо забезпечення інформаційної безпеки 5. Класифікація способів біометричної ідентифікації користувачів комп'ютерних систем 6. Концептуальна модель біометричної системи 7 Загальний алгоритм функціонування систем біометричної ідентифікації 8. Узагальнений алгоритм алгоритм роботи системи біометричної ідентифікаці 9. Технологія рольового розмежування доступу 10. Висновки.

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний	Краснієнко Н.В.		
Охорона праці	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		

7. Дата видачі завдання 01.06.2023

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1	Робота над Вступом	01.06.2023	виконано
	Робота з літературою	02.06.2023	виконано
2	Аналіз біометричних засобів комп'ютерної		
	ідентифікації особистості	03.06.2023	виконано
4	Дослідження методів комп'ютерної		
	Ідентифікації особистості	04.06.2023	виконано
5	Виконання розділу «Охорона праці»	08.06.2023	виконано
6	Виконання графічної частини роботи	13.06.2023	виконано
7	Чистове оформлення пояснювальної		
	записки кваліфікаційної роботи	15.06.2023	виконано
8	Підготовка доповіді та презентації до захисту	17.06.2023	виконано
9	Малий захист		
10		21.06.2023	виконано
		24.06.2023	виконано

Виконавець _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27. 06 000. 00 КРБ	*Дипломний проект*		
А4			*БКС 27. 06 000. 00 КРБ ПЗ*	*Пояснювальна записка*	*1*	

Зм.	Арк.	№ докум.	Підпис	Дата	*БКС 27. 06 000. 00 КРБ ПЗ*		
Розробив		Борщ О.О.			Дослідження біометричних систем комп'ютерної ідентифікації особистості	Літ.	Аркуш 5 / Аркушів 60
Перевірив		Краснієнко Н.				Н Д П	
Н. Контр.		Петрашова В.				*ВСП "ОТФК ОНТУ" гр.2БКС-27*	
Затверд.		Кривченко Ю.					

ЗМІСТ

стор.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Аналіз технічного завдання

Предметом дослідження кваліфікаційної роботи бакалавра згідно технічному завданню є методи і засоби біометричних систем комп'ютерної ідентифікація особистості.

Об'єктом дослідження даної теми щодо впровадження біометричних методів ідентифікації особистості.

Предмет дослідження – біометрична система ідентифікації особистсті.

Методи дослідження - аналіз технологій біометричної ідентифікації особистості, порівняльний аналіз обладнання для таких систем , застосування програмного забезпечення для побудови системи контролю доступу до об'єкта із використанням смартфонів та програмного забезпечення Azure Cognitive Services Face API .

На рисунку 1.1 представлена узагальнена структурна схема ідентифікації.

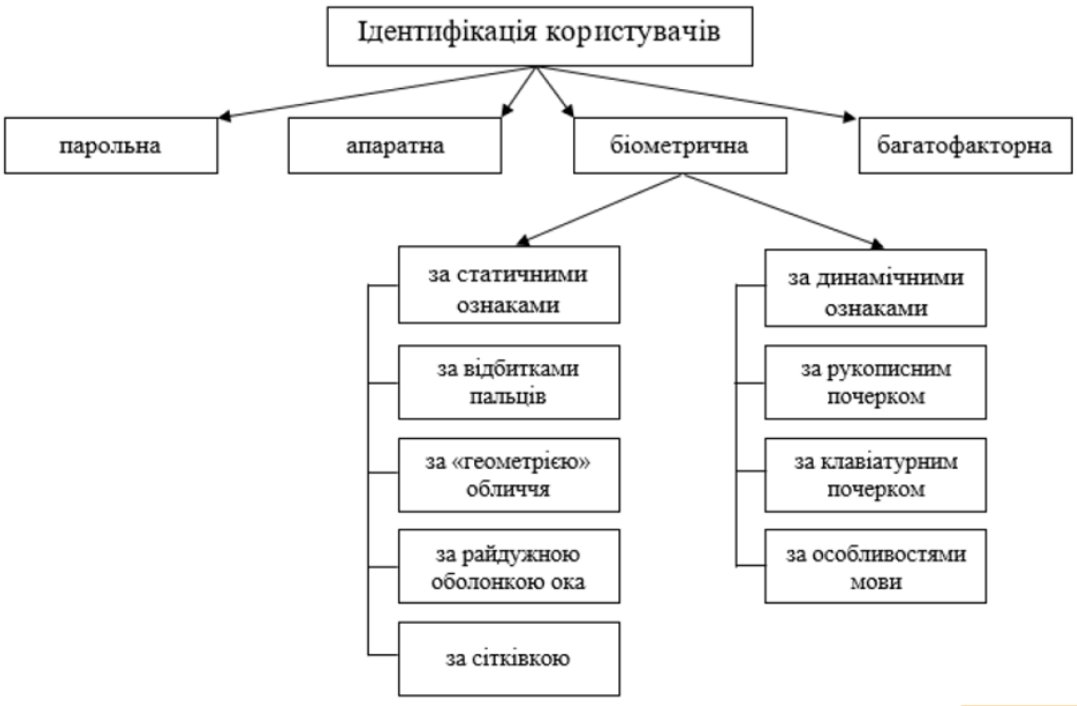


Рисунок 1.1 – Узагальнена структурна схема ідентифікації

1.2 Організація системи захисту в комп'ютерних системах

В комп'ютерних системах власник інформації (фізичне або юридична особа) зобов'язаний вживати заходи щодо забезпечення її захисту та здійснювати обмеження доступу до неї.

Така реалізація можлива з використанням побудови системи захисту. Основна мета такої реалізації – надання доступу до інформації тільки авторизованим користувачам відповідно до їхніх прав. На рисунку 1.2 представлена система захисту інформації в комп'ютерних системах

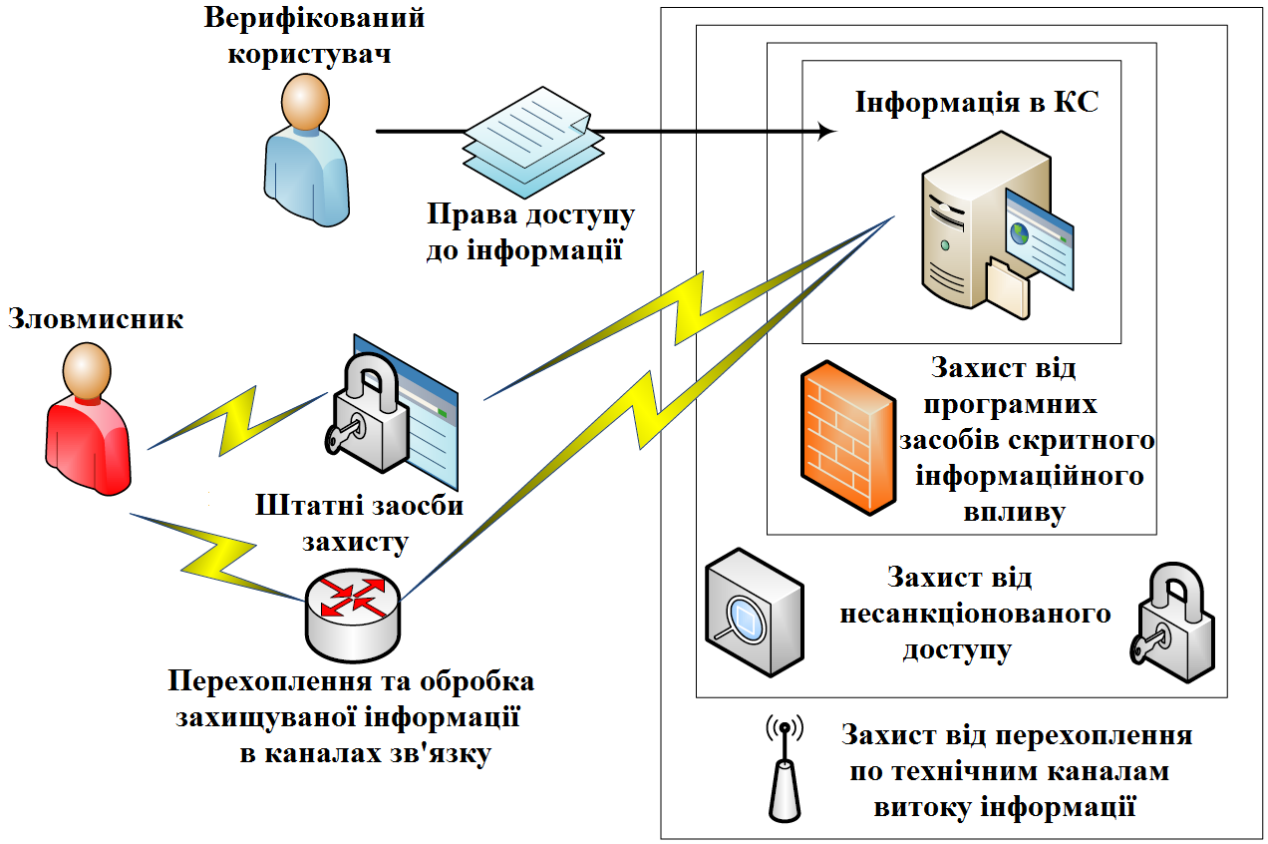


Рисунок 1.2 – Система захисту інформації в комп'ютерних системах

Згідно приведеної схеми, можна стверджувати, що система захисту інформації демонструє, що для захисту інформації потрібно виконання виконання цілого комплексу різних заходів., що спрямовані на:

- запобігання можливості її витоку,
- навмисного викривлення або знищення

- запобігання можливості ненавмисного потрапляння до осіб, не наділених правом доступу до неї.

Можна виділити цільові функціїзахисту інформації, що спрямовані на забезпечення її безпеки:

– забезпечення конфіденційності інформації;

– ідентифікація й аутентифікація користувачів;

– керування доступом до інформаційних ресурсів;

– підтвердження достовірності інформації.

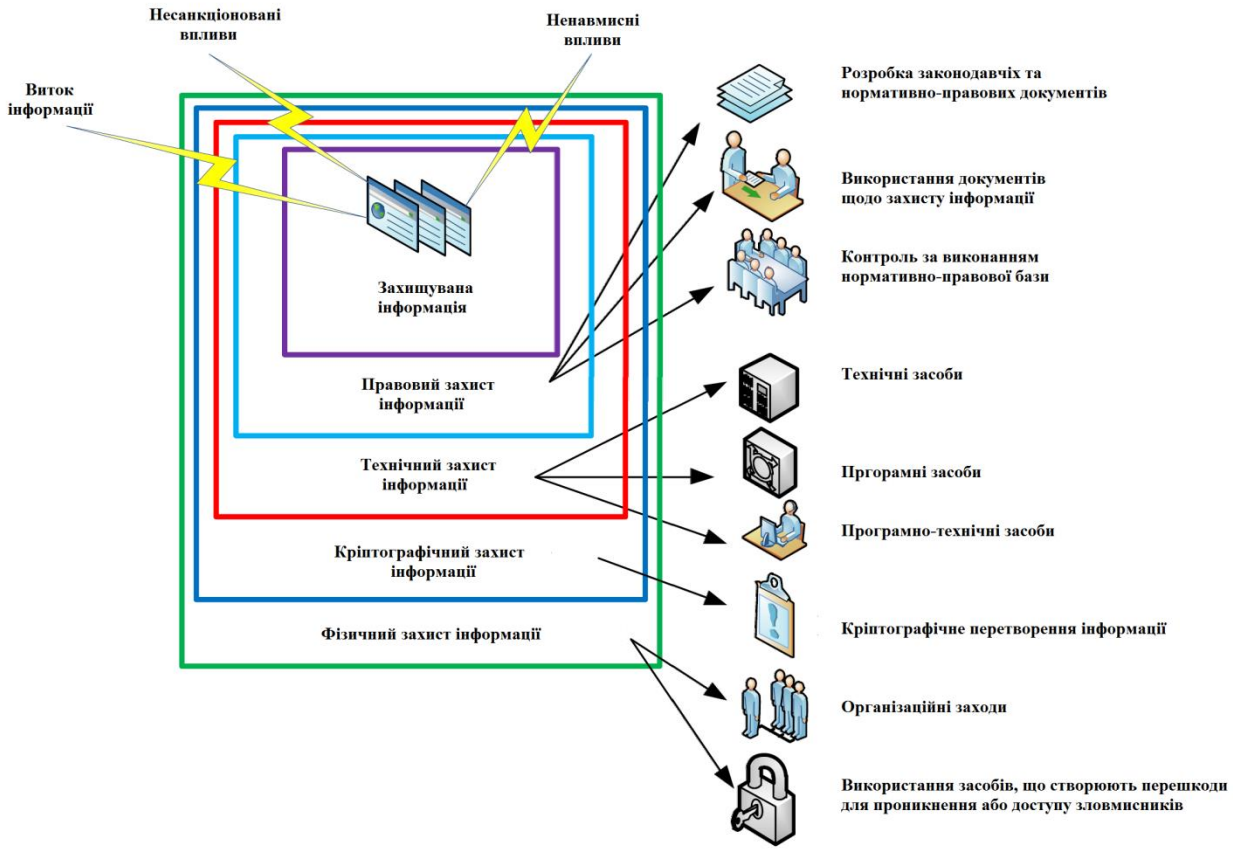


Рисунок 1.3– Комплекс заходів щодо забезпечення інформаційної безпеки

У підсумку на рисунку 1.3 представлено комплекс заходів щодо забезпечення інформаційної безпеки.

В таблиці1.1 розглянуто перелік ідентифікації різноманітних категорій осіб, що реєструються та мають доступ до конфіденціальної інформації.

Нижче наведено види і способи ідентифікацій користувачів КС. Їх можна реалізувати:

– з використанням унікальних фізичних предметів (чипів, смарт-карт тощо);

– на основі інформації, яка повинна зберігатися в секреті (пароль);

– за допомогою унікальних фізіологічних або поведінкових характеристик людини.

Таблиця 1.1 − Класифікація осіб для доступа до конфіденціальної інформації

Категорія	Опис
Користувач	Зареєстрований суб'єкт системи, який має певні права доступу до технічних, програмних та інформаційних ресурсів для виконання своїх функціональних задач. Може мати рівні права доступу до всього обсягу
Оператор	Зареєстрований, також як і користувач, суб'єкт системи, який має додаткові права щодо керування роботою системи. Може бути зареєстровано декілька
Адміністратор	Зареєстрований суб'єкт системи, який володіє всіма необхідним правами щодо керування системою, модифікації параметрів та режимів її роботи тощо. Може бути зареєстровано декілька адміністраторів
Технічний персонал	Суб'єкт, який не є зареєстрованим користувачем системи, але має доступ до її технічних засобів для виконання
Сторонній	Незареєстрованний суб'єкт системи, для якого виконання покладених на нього функціональних задач не пов'язане з доступом до технічних засобів системи

Ідентифікація за допомогою паролів має просту форму реалізації.

Основною перевагою звичність використання з одного боку, та нодоліком є саме наявність слабкого засобу фідентифікації особистості.

Це по'язано на можливих помилках при запам'ятовувані пароля саме особистістю.

Також наявність програмних засобів щодо зламу паролів та програм, що перехоплюють паролі під час введення в систему.

На рисунку 1.4 приведено класифікацію біометричної аутентификації

особистості. Основними характеристиками біометричних систем є: унікальність, сталість, вимірювальність та прийнятність щодо кожного коистувача.

Застосування біометричної ідентифікації в КС дозволяє підвищити рівень захисту інформації, тому що процес встановлення особи користувача, який має доступ до інформації, буде здійснюватися багаторазово й навіть постійно, а не тільки в початковий період роботи (як при використанні індивідуальних ключів чи паролів).

Через унікальність поведінкових характеристик людини, їх невіддільності від неї й сталості прояву в часі багаторазова аутентифікація користувача суттєво спрощується завдяки динамічним способам ідентифікації (див. рис. 1.4).

Їх використання дозволяє розв'язати відразу дві проблеми в процесі ідентифікації: «цілісність особистості» (незмінність особистості користувача під час роботи з КС) і «неможливість відмови від авторства» (користувач несе повну відповідальність за оброблювану інформацію).

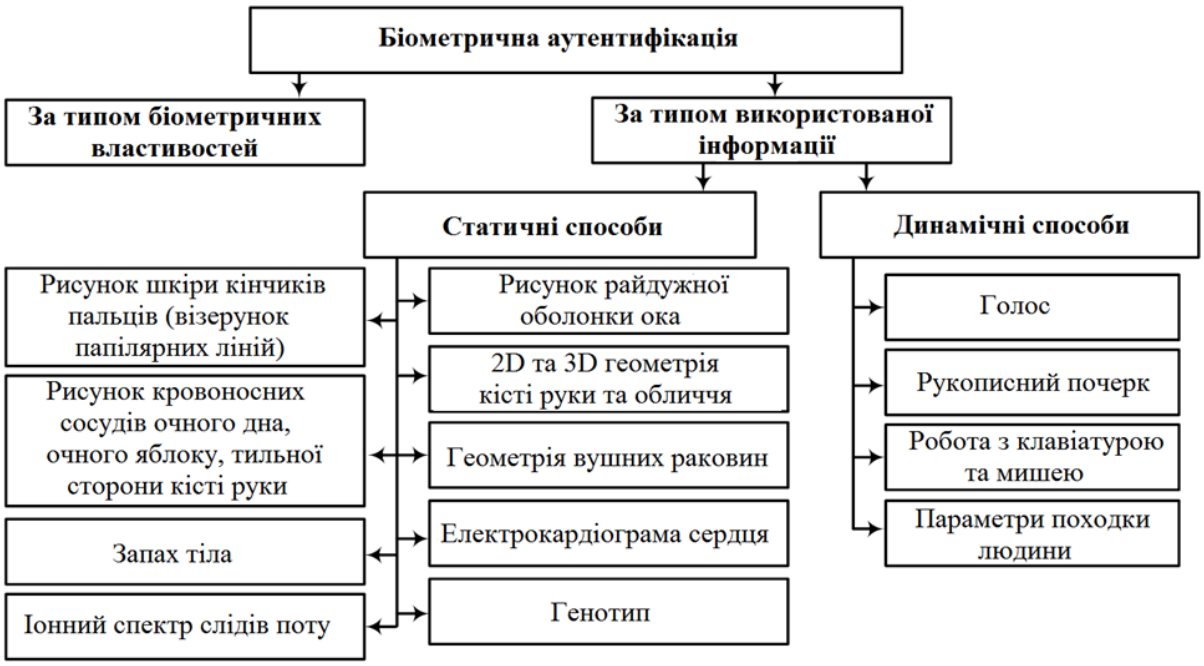


Рисунок 1.4 – Класифікація способів біометричної ідентифікації користувачів комп’ютерних систем

Щодо обмежень застосування біометричних систем, то вони пов'язані з можливими похибками під час введення інформації у зв'яку з власним станом людина, або зовнішніх показників освітленості, підвищенної вологості тощо.

1.3 Основні вимоги до систем ідентифікації користувачів комп'ютерних систем

В таблиці 1.2 преведено аналіз вимог до ідентифікації користувача.

Вимоги щодо імовірності помилкової відмови (помилки першого роду – FRR– False Rejection Rate) пред'являються, в основному, до біометричних систем ідентифікації користувача, тому що в інших випадках ідентифікації помилкові відмови через особливості алгоритмічних і технічних рішень практично відсутні.

Таблиця 1.2 – Аналіз вимог до ідентифікації користувачів

Властивості	Визначення	Показники та критерії	Вимоги
1	2	3	4
Достовірність ідентифікації	Здатність встановлювати істинність користувача з заданою точністю	Помилка другого роду (FAR) – ймовірність надання доступу неавторизованому користувачеві $p_{FAR} \leq p_{\text{ДОП}}^{II};$ помилка першого роду (FRR) – ймовірність заборони доступу зареєстрованому в системі користувачеві $p_{FRR} \leq p_{\text{ДОП}}^{I}$	ДСТУ ISO/IEC TR 24741:2017 Інформаційні технології. Біометрія. Загальні основи
Неперервність ідентифікації	Здатність забезпечувати аутентифікацію протягом усього сеансу роботи користувача	Коефіцієнт неперервності $K_{\text{НЕПР}} = \frac{T_{\text{АΣ}}}{T_{\text{РАБ}}},$ $T_{A\Sigma}$ – сумарний час роботи системи ідентифікації; $T_{\text{РАБ}}$ – тривалість сеансу	$K_{\text{НЕПР}} = 1$

Продовження таблиці 1.2			
1	2	3	4
Захищеність системи ідентифікації	Неможливість використання аутентифікаторів іншими особами	Ймовірність використання аутентифікатора іншими особами $p_{\text{АУТ}} \leq p_{\text{АУТ ДОП}}$	$p_{\text{АУТ ДОП}} = 10^{-6}$
Оперативність системи ідентифікації	Здатність проведення однократної ідентифікації за час	Час ідентифікаці$\tau_{\text{АУТ}} \leq \tau_{\text{АУТ ДОП}}$	$\tau_{\text{АУТ ДОП}} \leq 60$ с
Ресурсоємність системи ідентифікації	Обсяг ресурсів системи захисту інформації від НСД, що використовує КС	Об'єм використовуваних ресурсів $V_{\text{АУТ}} \leq V_{\text{АУТ ДОП}}$	$V_{\text{АУТ ДОП}} \leq 0.2V_{ЗЗІ\ НСД}$
Зручність використання системи ідентифікації	Здатність забезпечити зручність використання	ступінь зручності використання	відсутність впливу на роботу персоналу

Основними недоліками автентифікації користувача за індивідуальними ключами є можливість втрати ключ (жетон, картку) або його підробка.

З цією метою використовують різні види ключів: механічні та кріптографічні та біометричні ознаки людини.

Що стосується біометричних ключів то потрібно обгрунтувати можливість застосування підроблених елементів, такх як штучне око або штучний неживий палець.

У підсумку можно вважати, що паролі є найменш стійким засобом підтвердження особистості користувача, а широке використання інтелектуальних апаратних засобів вимагає значних фінансових витрат на їх поширення та адміністрування.

Застосування біометричних засобів ідентифікації особистості потребує подальшого розвитку як з теоретичної так і практичної точку зору.

Порівняльна характеристика біометричних систем приведена в таблиці 1.3.

Таблиця 1.3 – Порівняльна характеристика біометричних систем

Порівняльна характеристика біометричних систем	Відбиток пальця	Голос	Райдужна оболонка	Обличчя
Надійність верифікації, %	96.7-98	99.14-99.9	95.4-95.9	95.9
Помилка реєстрації, %	4	2	7	0.1
Ймовірність «допуску чужого», %	2.5	0.75	6	4
Ймовірність «відмови своєму», %	0.1	0.75	0.001	10
Вартість системи	Висока	Низька	Дуже висока	Висока

1.4 Аналіз законодавчів документів доступу до біометричної інформації

Встановлення обмежень доступу до інформації здійснюється в Україні згідно чинного законодавства, де визначені певні умови віднесення інформації до відомостей, що становлять державну, комерційну, службову й іншу таємницю, обов'язки дотримання конфіденційності даної інформації, а також відповідальність, що виникає, у випадку її розголошення.

Рішення про перехід до біометричної ідентифікації особи в Україні передбачені Державною цільовою програмою по організації і реконструкції державного кордону.

Біометрія (Biometrics) це технологія ідентифікації особи, яка використовує фізіологічні параметри суб'єкта (код ДНК, відбитки пальців, райдужну оболонку ока, зображення обличчя, тембр голосу тощо).

Біометричні технології активно використовуються в багатьох областях, які пов'язані зі захистом доступу до конфіденційної інформації, до матеріальних цінностей, при перетині державного кордону і т. ін.

Стандарти в області біометрії розробляються підкомітетом SC 37 "Біометрія"

Технічного комітету ISO/IEC JTC 1 "Інформаційні технології". У роботі підкомітету приймає участь 26 країн, серед яких є і Україна.

Ще 10 країн беруть участь у роботі підкомітету як спостерігачі. Підкомітетом "Біометрія" розроблено 39 стандартів [2].

Чинним на даний момент часу є ДСТУ ISO/IEC TR 24741:2017Інформаційні технології. Біометрія. Загальні основи. (ISO/IEC TR 24741:2007; IDT) затверджений Наказом від № 30.11.2017 № 392 Про прийняття нормативних документів України, гармонізованих з міжнародними та європейськими нормативними документами, скасування національних стандартів України [2].

Вид документа ДСТУ (Державний Стандарт України)

Шифр документа 24741:2017

Початок дії 01.01.2019

На рисунку 1.5 представлено узагальнену схему взаємозв'язку стандартів.

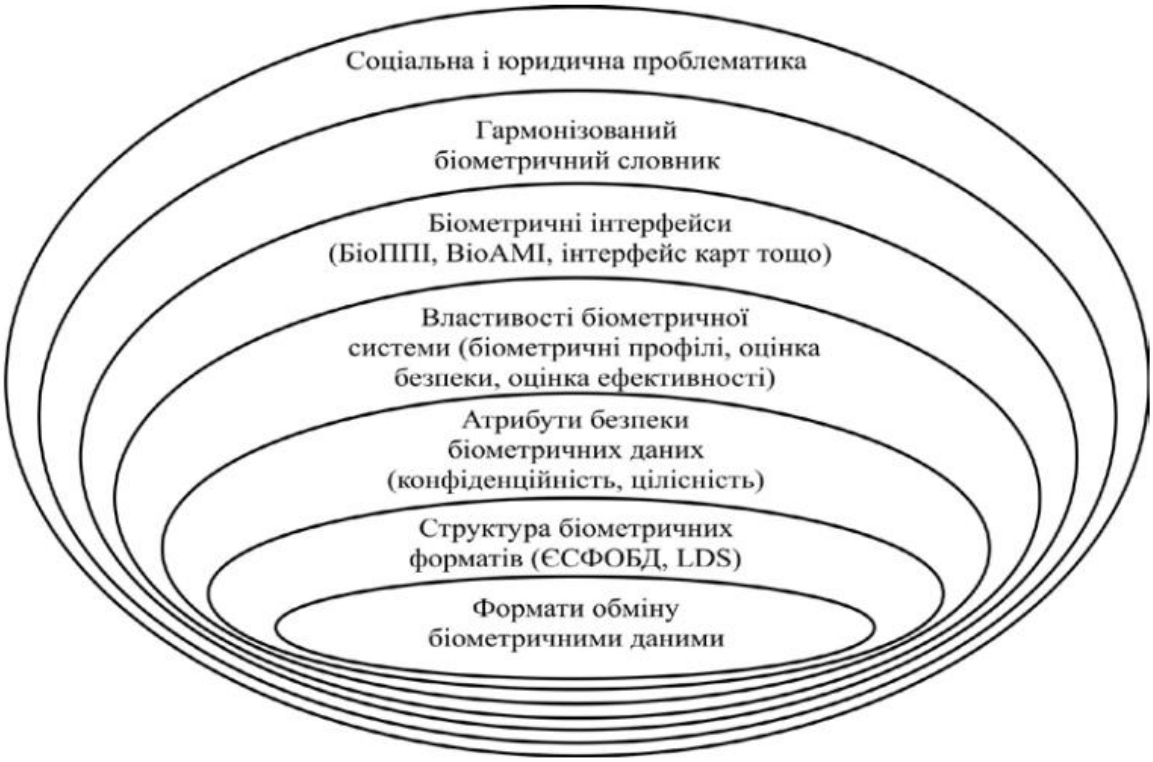


Рисунок 1.5– Схема взємозв'язку стандартів

Такі структури біометричних форматів, які визначені в ISO/IEC 24745:2015 як єдина система форматів обміну біометричними даними (ЄСФОБД), служать обгорткою навколо біометричних даних.

Оскільки біометричні дані є таємними даними й об'єктом атак, то вони підлягають захисту.

А саме в середовищах обміну цими даними мають бути використані криптографічні методи захисту.

Тому напрями розробки біометричних інтерфейсів на даний час є необхідними засобами для покращення інтеграції і використання різноманітних біометричних компонентів, що розроблюються виробниками прикладгих програмних та технічних засобів.

На рисунку 1.6 представлена архітектура базової моделі біометричної системи ідентифікації особистості. Усі біометричні технології характеризуються однаковою базовою моделлю. Спочатку необхідно створити первинний реєстраційний шаблон користувача.

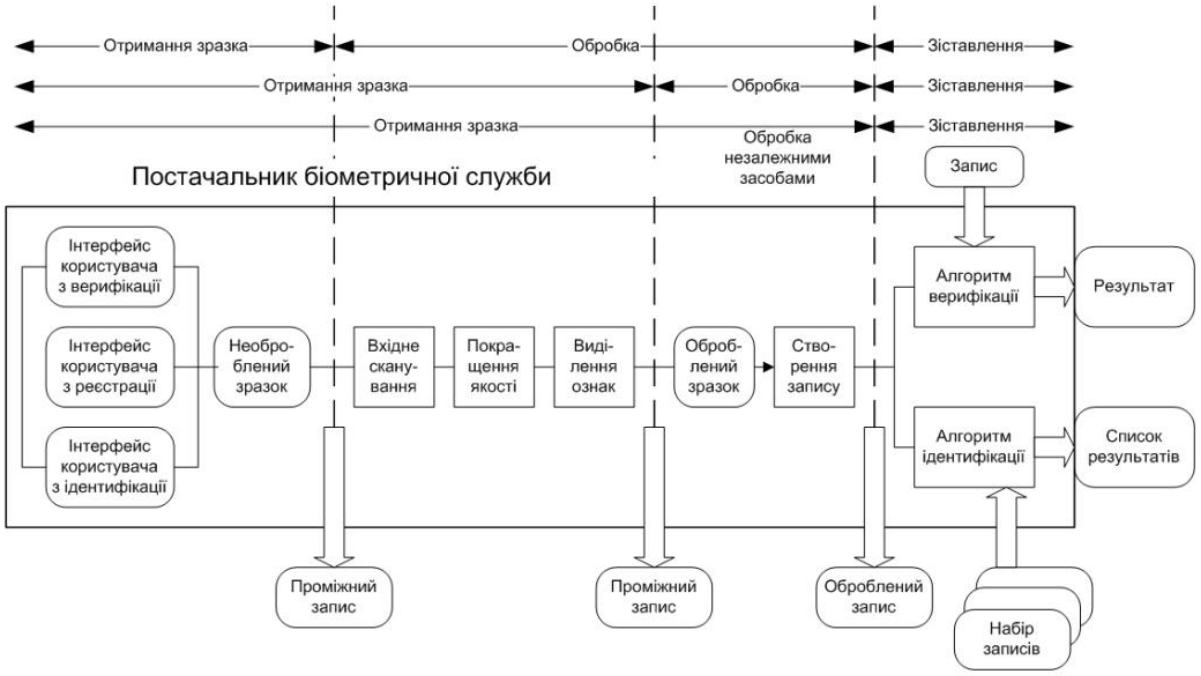


Рисунок 1.6 – Архітектура базової моделі біометричної системи ідентифікації

Ця операція здійснюється шляхом збору кількох зразків за допомогою будь-якого біометричного сенсора.

Далі зі зразків добуваються характерні ознаки й отримані результати об'єднуються згідно певного алгоритму в шаблон.

Процес створення даного первинного шаблона називається реєстрацією (або фіксацією). Алгоритми, які використовуються для створення шаблонів, можуть бути запатентовані за бажанням розробника.

Первинний шаблон зберігається прикладною програмою як контрольний шаблон.

Також можна зберігати цей шаблон за допомогою спеціальних засобів у відповідному модулі архіву біометричного прикладного програмного інтерфейсу. Отже, кожного разу, коли необхідно аутентифікувати користувача, з сенсора отримують "живі" зразки (або зразок), обробляють їх для подання в придатній для використання формі та зіставляють із раніше зареєстрованим контрольним шаблоном.

Таку форму біометричної аутентифікації називають верифікацією, оскільки проводиться перевірка того, чи є користувач тим, ким він себе називає (тобто перевіряється заявлена особистість).

Концептуальна модель демонструє саме інформаційні потоки у біометричній системі. Система містить:

1) підсистему фіксації даних,
2) обробки сигналів,
3) зберігання, зіставлення й ухвалення рішення.

Наведена модель ілюструє декілька процесів:

1) реєстрації,
2) верифікації
3) ідентифікації.

Але у реальній біометричній системі надані в даній концептуальній моделі, можуть бути відсутні або не відповідати безпосередньо фізичним компонентам.

На рисунку 1.7 представлена концептуальна модель біометричної системи.

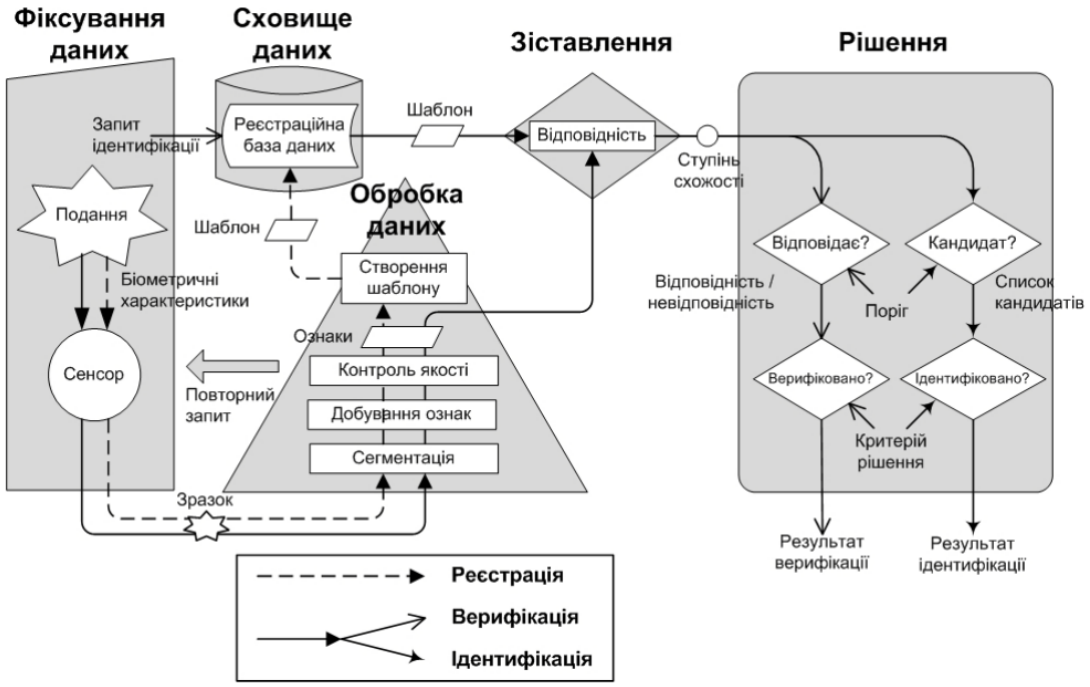


Рисунок 1.7 – Концептуальна модель біометричної системи

Нижче розглянемо саме послідовність процесу обробки інформації у біометричних системах (див. рис. 1.8)

Рисунок 1.8 – Структурна схема послідовності обробки біометричних даних особистості

У випадку реєстрації, підсистема обробки сигналів створює шаблон із добутих біометричних ознак.

Підсистема зберігання даних містить реєстраційну базу, яка служить для зберігання шаблонів, які пов’язані з певною інформацією про суб’єкт реєстрації.

Реєстрація у відповідній базі даних припускає, формат шаблонів може бути зміненим відповідно до формата обміну біометричними даними. Шаблони зберігаються на різних носіях: смарт-карті, персональному комп'ютері або локальному сервері, або в централізованій базі даних.

«На слідуючому єтапі, саме підсистема зіставлення даних порівнює біометричні дані з даними одного або декількох шаблонів та передає інформацію про ступінь схожості до підсистеми ухвалення рішень.

Ступінь схожості визначає ступінь відповідності ознак шаблонам, з якими проводилося порівнювання.

При верифікації один визначений запит суб'єкта реєстрації ініціює один розрахунок ступеня схожості. У випадку ідентифікації декілька або всі шаблони можуть бути порівняні з ознаками, вихідний ступінь схожості буде отриманий для кожного порівняння.

Підсистема ухвалення рішення використовує ступені схожості, створені однією або більше спробами, для надання вихідного рішення щодо запиту верифікації або ідентифікації.

У випадку верифікації, порівняння ознак та шаблону вважається успішним, якщо ступінь схожості перевищує встановлене граничне значення.

Підтвердження реєстрації суб'єкта може бути ухвалене у відповідності з правилами прийняття рішень, які можуть вимагати або допускати кілька спроб верифікації.

У випадку ідентифікації зареєстрований шаблон є потенційним кандидатом для суб'єкта, коли ступінь схожості перевищує встановлене граничне значення. Правила ухвалення рішень можуть дозволити або вимагати декількох спроб перед ухваленням рішення про ідентифікацію» [12].

Узагальнений алгоритм роботи системи біометричної ідентифікації користувачів КС приведено нижче у досліджені.

Звичайно, загальний алгоритм функціонування системи біометричної ідентифікації (СБІ) може бути наданий у вигляді (див.рис. 1.9), а узагальнений алгоритм роботи системи біометричної ідентифікації (див. рис. 1.10). Це ні в коєму разі не має зв'язку з біометричним ідентифікатором, що застосовує система.

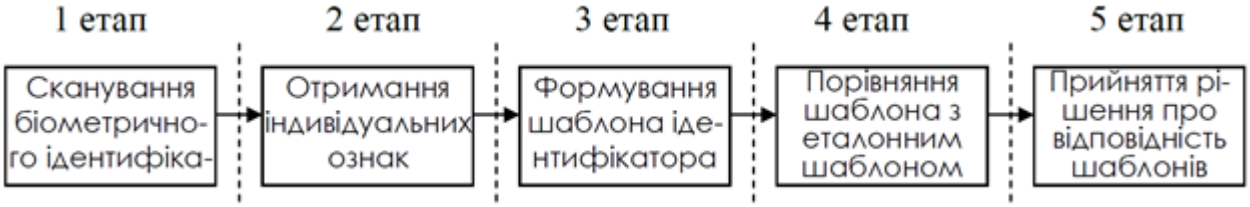


Рисунок 1.9– Узагальнений алгоритм функціонування СБІ

На рисунку 1.9 представлено узагальнений алгоритм роботи системи біометричної ідентифікації.

Цей алгоритм показує, що процес ідентифікації у біометричних системах в цілому поділяється на два види – ідентифікацію та верифікацію.

Обгрунтуємо поняття ідентифікаціїї і веріфікації.

Ідентифікація - це виправлення типу «один-до-багатьох», тобто. можна буде взяти виправлення наданого біометричного ідентифікатора з багатьма шаблонами біометричних ідентифікаторів, які є в базі.

Абсолютно автоматично система виконує пошук та виявляє спочатку декілька найбільш подібних шаблонів.

На другому етапі при використанні математичного апарату обирається найбільш схожий шаблон.

Верифікація – це порівняння типу «один-до-одного».

При веріфікації здійснюється порівняння наданого біометричного вектора з відповідним шаблоном з бази: наприклад, це логін користувача, а потім вже надається відповідний біометричний вектор.

У цьому режимі система працює набагато швидше та в повністю автоматичному режимі.

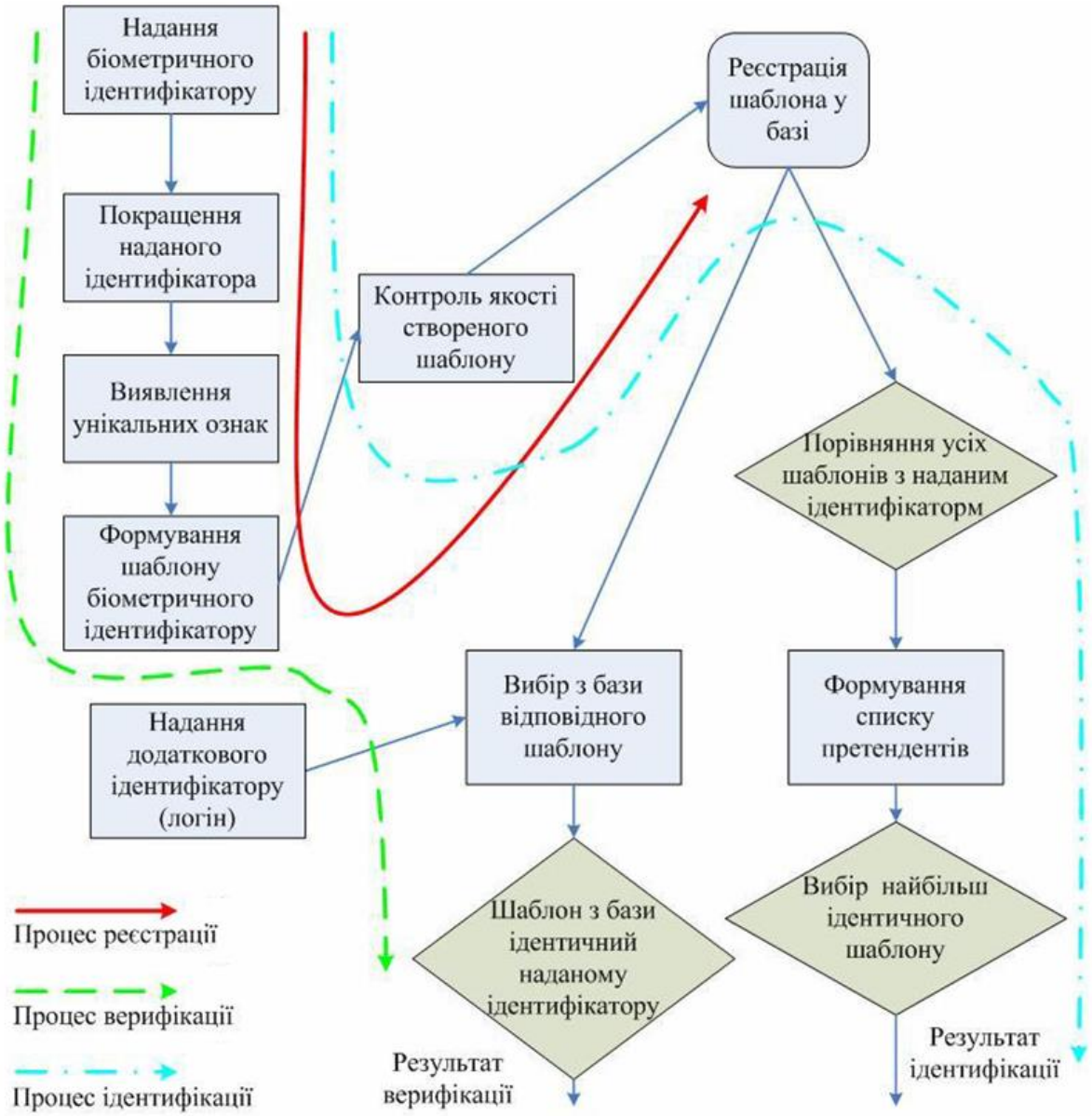


Рисунок 1.10 – Узагальнений алгоритм роботи системи біометричного ідентифікатора (СБІ)

Виділяють два класи біометричної ідентифікації по типу характерних ознак особистості:

– фізіологічні (статичні) – засновані на фізіологічній (статичній) характеристиці людини, тобто унікальних властивостях, які властиві їй від народження і є невід'ємними від неї;

– поведінкові (динамічні) – засновані на поведінковій (динамічній) характеристиці людини, особливостях, характерних для підсвідомих рухів у

процесі відтворення будь-якої дії.

До статичних методів біометричної ідентифікації відносять.

1. За відбитком пальця.

Це найпошереніша система ідентифікації особистості, що використовуєтьса в Україні.

Зображення відбитка пальця, що отримується за допомогою сканера, перетворюється у цифровий код, який порівнюється з шаблоном або еталоном.

Перевагами є висока достовірність, низька вартість пристроїв та проста процедура сканування відбитку.

Недоліками є похибки папілярного візерунку відбитків пальця впродовж життя людини.

2. За формою долоні.

В основі способу полягає геометрія кисті руки особистості.

3. За розташуванням вен на тильній стороні долоні.

В основі цієї технології лежить термографія кровоносних судин зовнішнього боку долоні руки з її неповторністю і сталістю впродовж життя,

Перевагами є відсутність необхідності контакту зі скануючим пристроєм, висока достовірність – статистичні показники методу можна порівняти з показаннями райдужної оболонки.

Недоліками є можливе засвічення сканера сонячними променями і променями галогенних ламп.

4. За райдужною оболонкою ока.

Сканування райдужної оболонки ока виробляється портативною камерою із спеціалізованим програмним забезпеченням.

Перевагами є статистична надійність алгоритму.

Недоліками є ціна та обмежена кількість готових рішень.

5. За малюнком кровоносних судин очного дна.

Система ідентифікації за сітківкою ока має низьку пропускну здатність і досить дорога в використанні, проте ступінь її надійності перевищує інші в рази.

Перевагами є високий рівень статистичної надійності.

Недоліками є складна система з високим часом обробки; висока вартість; відсутність широкого ринку попиту і, як наслідок, недостатня інтенсивність розвитку методу.

6. За формою обличчя: 2-D розпізнавання та 3-D розпізнавання.

Метод 2-D розпізнавання обличчя це процесс, який оснований на процесі виділення контурів очей, брів, носа, губ і т.ін.

В основі методу покладено обчислення що базуються на розрахунку відстані між ними.

В наслідку будуєть образ, що перетворюється в цифрову форму для процесу порівняння.

Перевагами методу є відміна дорого обладнання та можливість розпізнавання на відстані від камери.

Недоліками є низька статистична достовірність; залежність якості розпізнання від рівня освітлення; відсутність таких аксесуарів, як окуляри, зачіска, борода або маска, наявність фронтального фото обличчя без гримас.

Системи розпізнавання по 3D зображенню обличчя це особлива система. Вона застосовується у випадках, коли розпізнавання вимагає відсутності фізичного контакту та поставити систему контролю по райдужній оболонці неможливо.

Перевагами є висока достовірність розпізнавання; стійкість розпізнавання до відхилення ракурсу обличчя від фронтального; стійкість розпізнавання до неоднорідності освітлення; відсутність необхідності контактувати з пристроєм; низька чутливість до зовнішніх факторів.

Недоліками є чутливість до рівня освітлення; висока вартість обладнання;

3D розпізнавання вимагає проведення більше обчислювальних ресурсів ніж 2D.

7. За термограмою обличчя.

В основі цього методу покладено неповторність розподілу на обличчі кровоносних судин, що виділяють тепло.

Для проведення процесу сканування необхідна термочутлива камера інфрачервоного діапазону.

Перевагами є відсутність необхідності контакту зі скануючим пристроєм та висока достовірність.

Цей метод оснований на використанні статистичних показників. Результати використання такого методу порівнюються з аналізом показань райдужної оболонки.

Особливостью такої системи є можливість функціонування при відсутності освітлення та незалежно від оточуючої температури.

Недолікиами є дороге обладнання та обмежені з точки зору вивчення біометричні методи.

8. Інтерес виникає також жо нових біометричних технологій, що пов'язані із застосування іних фізіологічних характеристик стосовно людини, таких як дактилоскопія ДНК, дослідження відбитків долоні, сигнали, що виробляються серцем, мозком або легенями, що вимірюються датчиками «біодинамічного підпису».

В талиці 1.3 приведено класифікація динамічних методів, що ґрунтуються на особливостях поведінки людини - підсвідомих рухах в процесі виконання якої-небудь дії.

Таблиця 1.3 – Реалізація динамічних біометричних характеристик

Біометрична характеристика	Реєструючий пристрій	Зразок	Досліджувані риси
Голос	Мікрофон, телефон	Запис голосу	Частота, модуляція і тривалість голосового образу
Підпис	Планшет для підпису, перо для введення даних	Зображення підпису і значення відповідних динамічних вимірів	Швидкість, порядок ліній, тиск і зовнішній вигляд підпису
Динаміка натискання клавіш	Клавіатура	Ритм машинопису	Час затримки (проміжок часу, протягом якого користувач утримує конкретну клавішу), час «польоту» (проміжок часу, який потрібний користувачеві для переходу з однієї клавіші на іншу)
Динаміка роботи з маніпулятором «миша»	Маніпулятор «миша»	Образ характерної траєкторії	Характерні точки траєкторії та інші параметри траєкторії

Також проводиться аутентифікація за особливостями голосу.

Вона використовується із застосуванням телефонної мережі або із застосуванням звукових карт персонального комп'ютеру та мовного шаблону, з яким порівнюватиметься голосовий ключ, що вводиться в систему.

Недоліком є відзначаення за паролем, який потребує необходість зберігання в таємниці.

Ймовірність помилки для голосових систем складає від 1% до 2%.

Переваги: звичний для людини спосіб ідентифікації; низька вартість (найнижча серед усіх біометричних методів); не потребує контакту зі сканером.

Недоліками є можливість перехоплення фрази диктофоном та залежність якості розпізнавання залежить від інтонації, швидкості проголошення,

психологічного стану, хвороб горла у особистості.

Ідентифікація за динамікою рукописного підпису.

Ця проблема вирішується у двох напрямках: ідентифікація живого підпису або статичного-мертвого підпису.

Особливостью ідентифікації живого підпису є аналізпараметрів коливання пера при відтворенні підпису у тривимірному просторі декартової системи координат $(\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z})$. При цьому дані про динаміку відтворення підпису отримують у вигляді двох функцій часу коливань пера в площині графічного планшету $\boldsymbol{X(t)}, \boldsymbol{Y(t)}$ і ще одну функцію – варіації тиску пера на графічний планшет $\boldsymbol{Z(t)}$.

Перевагами такого методу є невисока вартість; відносна звичність для людини.

Недоліками є необхідність первинного навчання користувача системи із нестабільним почерком та додатковий час реєстрації користувача.

Ідентифікація за клавіатурним почерком (КП).

На рисунку 1.11 приведено ігнфографіку подання моделі часового ряду з використанням часового параметру F^t для двох суб'єктів, які набирають довільний текст

Під час роботи користувача з клавіатурою формується часова послідовність (ряд) подій, що супроводжують натискання клавіш. Таким чином, Отримані часову послідовність подій в процесі набору довільного тексту має вигляд:

$$K_{ts} = [\{t_1, k_1\}, \{t_2, k_2\}, \ldots \{t_n, k_n\}]. \quad (1.1)$$

Інфографіка (див. Рис. 1.11) демонструє вісь X , де відкладаються значення t_i послідовних унікальних ідентифікаторів часового ряду, та вісь Y –значення часу між натисканням двох сусідніх клавіш (flight time, F^t) або час утримання окремої клавіші (hold time, H^t). Інфографіка на рис. 1.11 демлнструє, що кожен користувач має унікальну сукупність часових рядів натискань клавіш, що може бути використано для побудови профілів клавіатурного з наборів F^t і H^t.

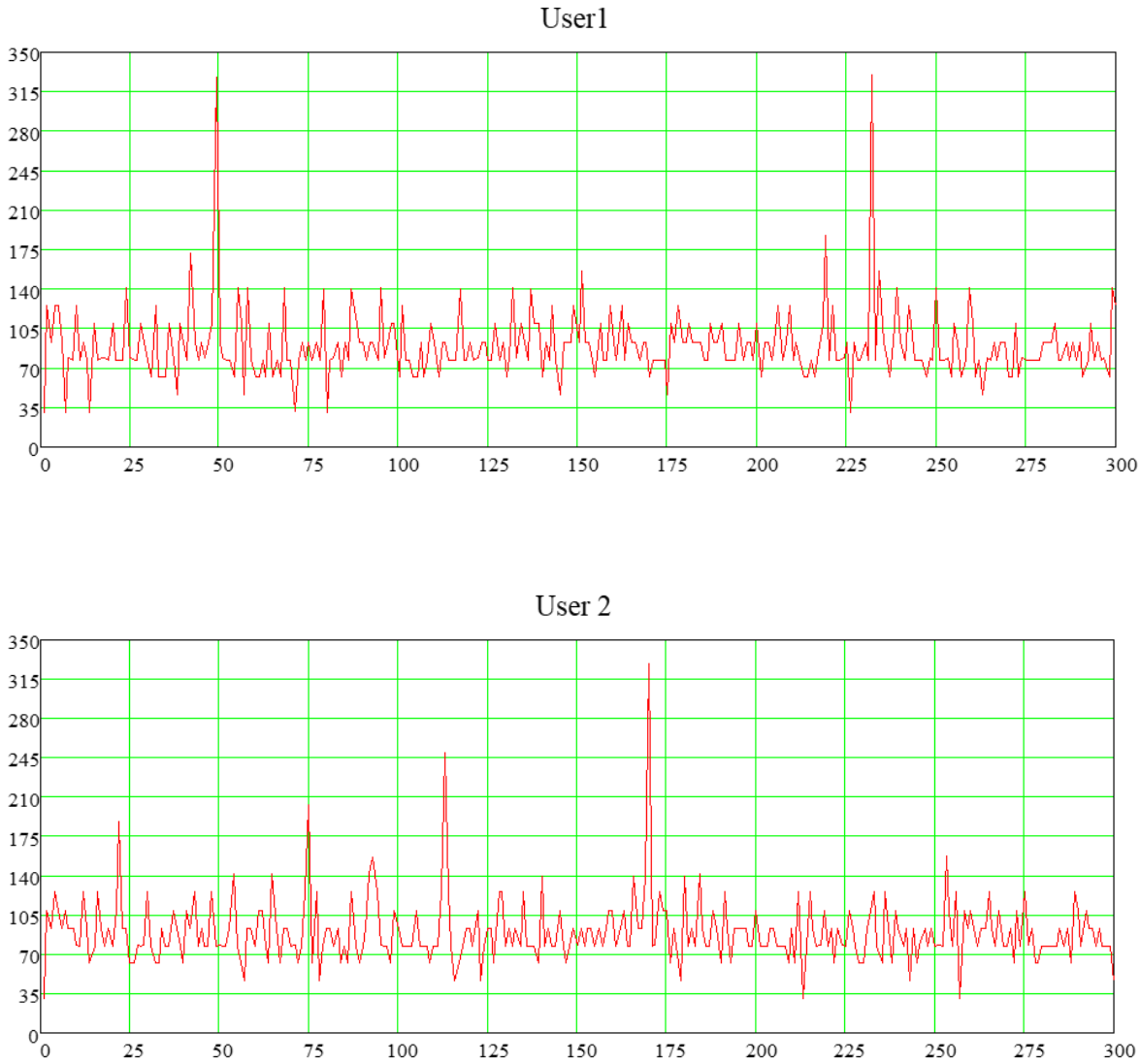


Рисунок 1.11 – Порівняльна інфографіка моделі часового ряду F^t для двох суб'єктів, що набирають довільний текст

Перевагами методу є дешевизна та простота реалізації й впровадження

Недоліками є вплив на коректність роботи алгоритму ідентифікації психофізичний стан користувача.

Впровадження систем біометричної ідентифікації особистості регламентується підкомітетом SC 37 "Біометрія" Технічного комітету ISO/IEC JTC 1 "Інформаційні технології".

Наразі розроблено і введено в дію 39 стандартів в області біометрії та відповідних технологій.

У підсумку можна сказати, що існюча різноманітність біометричних

технологій, як апаратних так і програмних засобів мають свої вразливості у процесі ідентифікації особистості.

Достовірність ідентифікації реальної особистості в умовах відхилення його біометричних параметрів від норми в різних функціональних станах може бути підвищена шляхом врахування мултімодалного характеру взаємодії користувача з автоматизованими засобами захисту інформації. «Мультимодальні біометричні системи використовують декілька сенсорів або біометричні пристрої для подолання обмежень унімодальних біометричних систем».

1.5 Апаратна біометрична ідентифікація

Розглянемо приклади технічних засобів, що використовують біометрічну ідентифікацію. Перш за все, за осову таких приладів взято технологію ідентификації особистості за відбитками пальців або долоні людини.

Такий спосіб ідентифікації особистості не є захищеним, тому что існують можливості, що копіюють оригінал, а саме: перенесення відбітків на плівку, або використання якісної фотографії. Крім того, такі прилади можуть мати високу вартість, а вони необхідні бути придбані до кожного комп'ютеру, що входить у комп’ютерну систему.

На рисунку 1.12 представлено пальцевий дактилоскопічний сканер

Рисунок 1.12 – Пальцевий дактилоскопічний сканер SUPREMA ID RealScan-G10

Технічні характеристики пальцевого дактилоскопічного сканера SUPREMA ID RealScan-G10 приведено у таблиці 1.4.

Таблиця 1.4 – Технічні характеристики біометричного сканеру відбітків

пальців SUPREMA ID RealScan-G10

Типи відбитків	• Одинарні прокатки • Одинарні відтиски • Відбиток чотирьох пальців • Відбиток двох великих пальців
Частота кадрів	20 кадров за секунду
Швидкість захоплення	4 + 4 + 2 за 15 секунд
Роздільна здатність	500 dpi, 256 відтінків сірого
Розмір робочої панелі (Ш х Д)	89 х 80 мм
Зона чутливості (Ш х Д)	81,28 х 76,2 мм
Розмір зображення (Ш х Д)	•Відбиток чотирьох пальців: 1600 х 1500 px •Одинарні відтиски / прокатки: 800 х 750 px
Стандарти якості зображення	FBI IAFIS Додаток F
Інтерфейс	USB 2.0 High-speed (Data & Power)
Ступінь захисту	IP54
Динаміки	Вбудовані
Світлодіодний індикатор	Так
Робоча температура	-10 ° C ~ 50 ° C
Вологість при експлуатації	10 ~ 90%, без конденсації
Розміри (Ш х Д х В)	152 х 152 х 127 мм
Вага	1,8 кг
Сертифікація	CE, FCC, KC, UL, ROHS, USB-IF, WHQL
Операційна система	Windows: Windows XP, Vista, 7, 8, 8.1, 10 32/64bit

Рисунок 1.13 – Долонний дактилоскопічний сканер

1.6 Розробка нових видів біометричних систем

Процеси розробки нових біометричних систем постійно оновлюються новими розробками.

На стадії розробки з'являються нові біометричні технологічні рішення, пов'язані з іншими фізико-математичними особливостями.

Такі напрямки дослідження є аналіз ДНК, малюнки судин, сигнали серця або мозку людини.

Наразі йдуть розробки щодо створення біометричних системи, що ідентифікують особу в районі райдужної оболочки.

Сучасним методом ідентифікації, який має величезні переваги, став метод ідентифікації особистості за особливостями голосу: з одного боку - це розширення використання телефонної пам'яті, з іншого боку - наявність якісних звукових карт у системному блоці персонального комп'ютера.

Такі методики мають деякі недоліки, а саме: звичайні засоби акустичного прослуховування дозволяють досить прискорено вести несанкціоноване копіювання парольної фрази. Потенційний захист від прослуховування підвищує

можливості комбінування з іншими методами біометричної автентифікації.

Похибка для голосових систем складається не більше 1-2.

Щоб ідентифікувати абонента за голосом, обов'язково мати шаблон, за допомогою якого можна порівнювати ключ голосу, який вводитиметься до системи.

Порівнання ключа і шаблону може здійснюватися у цілому або поза характеристик мовного сигналу.

Можна використовувати такий напрямки, як цифровий мовний сигнал, що пройшов обробку і адаптований до поставленого завдання.

Це мається на увазі: амплітуда і потужність (гучність), часові, частотні (тембр), енергетичні, фазові характеристики.

Для виконання таких напрямеів обробки звукового сигналу використовується нижче приведений фізико-математичний аппарат:

- функція короткочасної енергії з використанням вікон Хеммінга;
- автокореляційна функція (дозволяє визначити енергію і періодичні властивості сигналу);
- число переходів сигналу через нуль (оскільки високі частоти приводять до великого числа переходів через нуль, а низькі – до малого, то існує жорсткий зв'язок між числом нульових переходів і розподілом енергії по частотах);
- спектр сигналу;
- коефіцієнти лінійного передбачення;
- кепстральні коефіцієнти;
- кепстральні коефіцієнти, що обчислені на основі лінійного передбачення. Метод, що пов'язаний з дослідженням застосування користувачем маеіпулятора – миша, який називається «користувач-миша» також показують високу надійність розпізнавання.

Що стосується динамічних характеристик, то тут можна назвати –аналіз подпису. При аналізу приймають до відома антропологічні дані особистості, а саме: довжина ліктьового суглоба і розміри зап’ястя), що впливають на характеристику радіусу кривизни траєкторії.

Фізіологічні дані людини:структура м’язів ліктьового і плечового суглобів, впливають швидкість і прискорення руху курсору, тобто динаміку руху. Позитивним у цьому напрямку досліджень можна вважати той факт, шо комп’ютерна система дає змогу розглянути цей процес в динаміці і скористатися додатковою інформацією про динаміку руху курсору.

Аналіз таких характеристик також проводиться з використанням фізико-математичних методів:

1) статистичний аналіз: обчислюється середнє кожного з ключових значень, його середньоквадратичне відхилення і здійснюється перевірка належності ключових значень зразка, що пред'являється, довірчим інтервалам, отриманим з аналізу еталонних зразків;
2) застосування байєсівських мереж;
3) застосування прихованих моделей Маркова.
4) Для аналізу почерку миши використовується декілька напрямків, це:
5) повний, аналіз;
6) сегментація почерку миши;
7) система єдиного входу (SSO, Single Sign-On) - а саме: Клієнтський; Серверний; Комбінований; Веб-єдиний запит (Web SSO).

1.7 Програмна реалізація засобів біометричної ідентифікації

1.7.1 Обгрунтування вибору Azure Cognitive Services Face API

Кожен з наведених вище методів має недоліки, але як видно головний недолік біометричної індертифікації є її дороговизна адже необхідне додаткове устаткування. Вирішенням даної проблеми є ідентифікація за допомогою смартфонів.

В результаті аналізу переваг та недоліків щодо методів ідентифікації та алгоритму захисту інформації в комп’ютерних мережах на основі біометричних даних було обрано метод ідентифікації за геометрією обличчя.

Підводячи підсумки можна сказати, що у систем, які вимагають особливих

вимог до безпеки, використовуються мультимодальні методи біометричної ідентифікації.

Використання біометричних засобів спрощує процедуру ідентифікації особи, а також підвищує надійність систем безпеки.

Для підтвердження особи при використанні мобільного телефону, планшета або ноутбука найбільш актуальною є біометрія за геометрією обличчя.

У зв'язку з інтенсивним зростанням потреби в обчислювальних і телекомунікаційних системах, розвитком комп'ютерної техніки і збільшенням числа користувачів, все більша увага приділяється питанням контролю доступу до їх ресурсів.

Подібний контроль здійснюється через задані адміністратором обмеження доступу, тобто, можливості виконати певні дії користувачів по відношенню до ресурсів системи.

У результаті проведеного аналізу технологій розмежування доступу було виявлено низку характерних особливостей, переваг і недоліків існуючих напрямів управління доступом.

Визначено, що одними з найбільш перспективних напрямів є використання технології рольового розмежування доступу (англ. Role Based Access Control RBAC). (див. рис.1. 14)

Для реалізації технологіїрозпізнавання обличчя за допомогою смартфону використовується технологія розпізнавання обличчя Face API.

API Face Azure Cognitive Services надає алгоритми, які використовуються для виявлення, розпізнавання і аналізу людських облич на зображенні (2 D). API інтерфейс Face виявляє людські обличчя на зображенні і повертає координати API ідентифікації використовується для ідентифікації виявленого особи по базі даних людей.

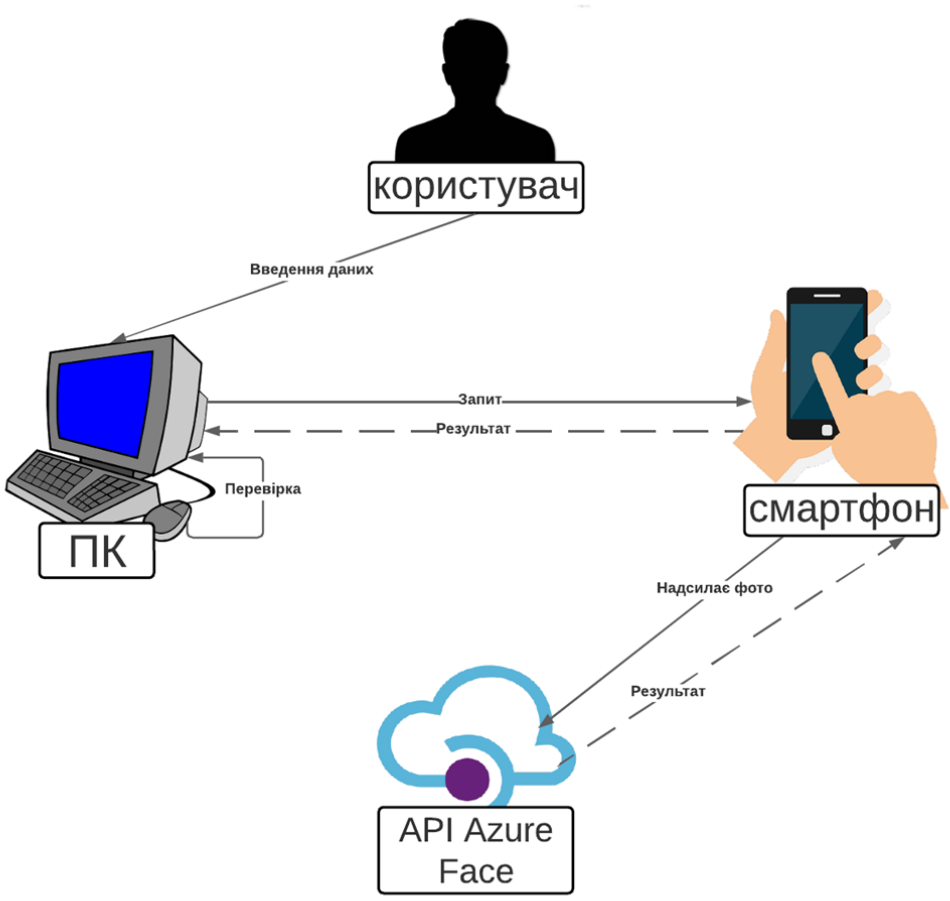


Рисунок 1.14 – Технологія рольового розмежування доступу

Впровадження функції розпізнавання облич у програми для зручної та надійної взаємодії з користувачами дає можливість мати доступ до таких функцій, як;

1) визначення осіб, при якому на зображенні виявляються особи та їх атрибути (наприклад, маска, окуляри, положення особи),
2) ідентифікація особи за збігом із даними в приватному репозиторії або посвідчення з фотографією.

Розпізнавання обличчя потрібне як перший крок у всіх інших сценаріях. Detect API виявляє людські обличчя на зображенні та повертає прямокутні координати їх розташування.

Він також повертає унікальний ідентифікатор, який представляє збережені дані обличчя.

Це використовується в подальших операціях для ідентифікації або перевірки

облич.

Крім того, розпізнавання обличчя може витягти набір пов’язаних з обличчям атрибутів, таких як поза голови, вік, емоції, волосся на обличчі та окуляри.

Ці атрибути є загальними прогнозами, а не фактичними класифікаціями. Деякі атрибути корисні, щоб гарантувати, що ваша програма отримує високоякісні дані про обличчя, коли користувачі додають себе до служби Face. Наприклад, ваша програма може порадити користувачам зняти сонцезахисні окуляри, якщо вони носять сонцезахисні окуляри.

Ідентифікація обличчя може відповідати типу "один-до-багатьох" одного обличчя на зображенні набору облич у безпечному сховищі. Кандидати на збіги повертаються на основі того, наскільки точно дані про їхні обличчя відповідають обличчю запиту. Цей сценарій використовується для надання доступу до будівлі чи аеропорту певній групі людей або перевірки користувача пристрою.

За рекомендаціями корпорації Microsoft нижче приведена концепція розпізнавання обличчя та дані атрибутів обличчя: «розпізнавання обличчя – це процес визначення місцезнаходження людських облич на зображенні та, за бажанням, повернення різних типів даних, пов’язаних із обличчям».

«Ідентифікатор обличчя Face ID – це унікальний рядок ідентифікатора для кожного виявленого обличчя на зображенні. Face ID потребує схвалення обмеженого доступу».

Орієнтири обличчя – це набір точок, які легко знайти на обличчі, наприклад зіниці або кінчик носа.

За замовчуванням існує 27 попередньо визначених орієнтирів. На наступному малюнку показано всі 27 пунктів (диа. рис.1.15)

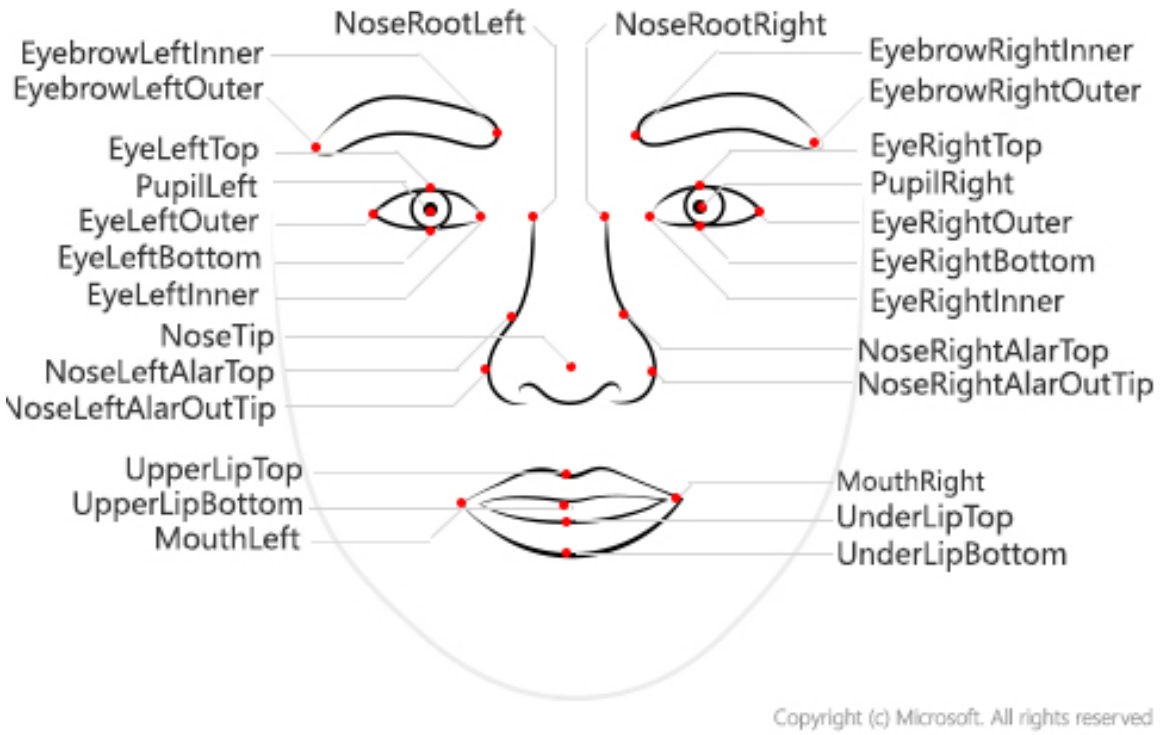


Рисунок 1.15 – Орієнтири обличчя. Розробка корпорації Microsoft

«Координати точок повертаються в одиницях пікселів. Модель Detection_03 наразі має найточніше визначення орієнтирів. Орієнтири очей і зіниць, які він повертає, достатньо точні, щоб можна було відстежувати погляд обличчя.

Модель Detection_03 наразі має найточніше визначення орієнтирів. Орієнтири очей і зіниць, які він повертає, достатньо точні, щоб можна було відстежувати погляд обличчя.

1) Атрибути – це набір функцій, які за бажанням можна виявити за допомогою Face - Detect API. Можна виявити такі атрибути:
2) Аксесуари. Чи є на даному обличчі аксесуари. Цей атрибут повертає можливі аксесуари, зокрема головні убори, окуляри та маску, з оцінкою достовірності від нуля до одиниці для кожного аксесуара.
3) Вік _ Орієнтовний вік у роках певного обличчя.
4) Розмиття. Розмитість обличчя на зображенні. Цей атрибут повертає значення від нуля до одиниці та неформальний рейтинг низький, середній або високий.

5) Емоція. Список емоцій із впевненістю їх визначення для даного обличчя. Показники впевненості нормалізуються, а оцінки всіх емоцій складаються в одиницю. Повернуті емоції - це щастя, смуток, нейтральність, гнів, презирство, огида, здивування та страх.
6) Експозиція. Експозиція обличчя на зображенні. Цей атрибут повертає значення від нуля до одиниці та неофіційну оцінку UnderExposure, goodExposure або OverExposure.
7) Волосся на обличчі. Передбачувана наявність волосся на обличчі та довжина даного обличчя.
8) Стать _ Орієнтовна стать даного обличчя. Можливі значення: чоловічий, жіночий і безстатевий.
9) Окуляри. Чи є на даному обличчі окуляри. Можливі значення: NoGlasses, ReadingGlasses, Sunglasses і Swimming Goggles.
10) Волосся. Тип волосся особи. Цей атрибут показує, чи видно волосся, чи виявлено облисіння та який колір волосся виявлено.
11) Поза голови. Орієнтація обличчя в 3D просторі.

Характеритики вхідних зображень, що дають найточніші результати виявлення:

1) Підтримувані формати вхідних зображень: JPEG, PNG, GIF (перший кадр), BMP.
2) Розмір файлу зображення має бути не більше 6 Мб.
3) Мінімальний розмір обличчя, який можна виявити, становить 36 x 36 пікселів на зображенні, яке не перевищує 1920 x 1080 пікселів. Зображення з розміром понад 1920 x 1080 пікселів мають пропорційно більший мінімальний розмір обличчя. Зменшення розміру обличчя може призвести до того, що деякі обличчя не будуть розпізнані, навіть якщо вони більші за мінімальний розмір, який можна розпізнати.
4) Максимальний розмір обличчя, яке можна виявити, становить 4096 x 4096 пікселів.

5) Обличчя за межами діапазону розмірів від 36 x 36 до 4096 x 4096 пікселів не будуть виявлені.

6) Деякі обличчя можуть не розпізнаватися через технічні проблеми, наприклад:

7) Зображення з екстремальним освітленням, наприклад, сильним контровим освітленням.

8) Перешкоди, які блокують одне або обидва ока.

9) Відмінності в типі волосся або волосся на обличчі.

10) Зміна зовнішнього вигляду обличчя через вік.

11) Екстремальна міміка» [13].

1.7.2 Створення Azure Cognitive Services Face API на порталі Azure

Нижче приведено приклад JavaScript API обличчя Cognitive Services Azure за етапами:

1) створення API обличчя Azure Cognitive Services на порталі Azure,
2) розробка JavaScript для виявлення облич на зображенні,
3) використання ключа Azure Face API Face і EndPoint,
4) отримання кінцевої точки- повертанного значення характеристик обличчя.

Azure Cognitive Services Face API надає розширений алгоритм, який допомагає виявляти або читати людські обличчя на різних цифрових зображеннях, що включає виявлення емоцій і виразів обличчя, як-от щастя, страх тощо та допомагає застосувати функцію ідентифікації особи, яка збігається з особою до 1 мільйона людей.

Передумови роботи в системі Azure.

1) Для роботи в системі необхідно дійсну підписку Azure або дійсний обліковий запис Azure.

2) Необхідно встановити редактор коду, наприклад Visual Studio Code або NotePad.

Перший крок: створення Azure Cognitive Services Face API на порталі Azure. Виконайте наведені нижче дії, щоб створити API обличчя Azure Cognitive Services на порталі Azure.

Увійшовши до порталу Azure у бічному меню зліва необхідно натиснути кнопку: + Створити ресурс Azure Face API. Далі копіювання значення ключа Azure Face API Key1 і збереження його в блокноті. Цей ключ-значення використовується під час розробки JavaScript

Алгоритм створення Azure Cognitive Services Face API

Другий крок: розробка JavaScript і REST API для виявлення облич на зображенні та використання ключа Azure Face API і EndPoint .

Лістінг файлу JavaScript для виявлення обличь на зображенні із використвнням Azure Face API приведено нижче.

```
<!DOCTYPE html>
<html>
   <head>
      <title>Face Detection APP</title>
      <script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.9.0/jquery.min.js"></script>
//Покликання на веб-сайт ресурсу ajax
   </head>
   <body></body>
</html>
//Наступний крок – додавання
<script type="text/javascript">
   function ImageProcessing() {
      var Key = "bd3ad7ff0d0e467ebf24fd3abd69b39a"; // Ключ фото обличчя
      var uri =
         "https://eastus.api.cognitive.microsoft.com/face/v1.0/detect";
```

```
//Додавання ключа зображення Azure.

        // Запит параметрів.
        var params = {
            "detectionModel": "detection_02",
            "returnFaceId": "true"
        }; //Виявлення обличчя на фото

        // Відображення забраження.
        var ImageUrl = document.getElementById("inputImage").value;
        document.querySelector("#sourceImage").src = ImageUrl; // код виведення
на екран

        // Виконайте виклик REST API //Передача даних на сервер Azure для
аналізу  фото
        $.ajax({
            url: uri + "?" + $.param(params),

            //Запит заголовку коду
            beforeSend: function(xhrObj){
                xhrObj.setRequestHeader("Content-Type","application/json");
                xhrObj.setRequestHeader("Ocp-Apim-Subscription-Key", Key);
            },

            type: "POST",

            // Запит body (основна частина обробці зображення).
            data: '{"url": ' + "" + ImageUrl + ""}',
        })
```

```
        .done(function(data) {
            // Показати відформатований JSON на веб-сторінці.
            $("#responsetxt").val(JSON.stringify(data, null, 2));
        })

        .fail(function(jqXHR, textStatus, errorThrown) {
            // Відображення повідомлення про помилку.
            var errorString = (errorThrown === "") ?
                "Error. " : errorThrown + " (" + jqXHR.status + "): ";
            errorString += (jqXHR.responseText === "") ?
                "" : (jQuery.parseJSON(jqXHR.responseText).message) ?
                    jQuery.parseJSON(jqXHR.responseText).message :
                        jQuery.parseJSON(jqXHR.responseText).error.message;
            alert(errorString);
        });
    };
    };
</script>
<h1>Faces Analysis</h1>
Provide the URL to an image, then click
the <strong>Detect</strong> button.<br><br>
Image: <input type="text" name="inputImage" id="inputImage"
    value="https://her33fffff.blob.core.windows.net/new123/nwphoto.png" />
<button onclick="ImageProcessing()">Detect</button><br><br>
<div id="wrapper" style="width:1020px; display:table;">
    <div id="jsonOutput" style="width:600px; display:table-cell;">
        Response:<br><br>
        <textarea id="responsetxt" class="UIInput"
            style="width:590px; height:410px;"></textarea>
    </div>
```

```
    <div id="imageDiv" style="width:410px; display:table-cell;">
      Source image:<br><br>
      <img id="sourceImage" width="400" />
    </div>
  </div>
```

На наступному кроці файл блокнота зберігається як .html. Якщо відкри його, а потім натисніть кнопку «Визначити», програміст отримує очікуваний результат, як показано нижче.

Перед розробкою сценарію необхідно завантажити зображення в сховище blob і переконатися, що воно має публічний доступ, тобто загальнодоступний доступ до сервера або використати будь-який із загальнодоступних серверів для завантаження зображення та використання URL-адреси.

Нижче наведено зображення для завантаження у сховище Azure Blob Storage.

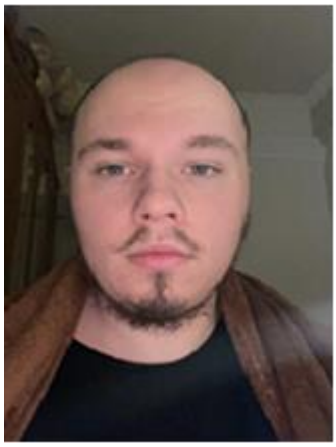


Рисунок 1.15 – Приклад зображення, що завантажується у сховище Azure Blob Storage

Вимоги до характеристик зображення

1) Формат зображення має бути JPG, png, peg, gif (перший кадр) і BMP.
2) Розмір зображення має бути від 1 КБ до 6 МБ .
3) Розмір обличчя має бути від 36×36 пікселів до 1920×1080 пікселів .

Система обробляє та може повернути до 100 обличь на зображенні.

Вимоги до якості обличчя на зображенні - чітке і фронтальне.

Це ключові моменти, які потрібно враховувати при виборі образу. Якщо обличчя на зображенні нечіткі, то можна не отримати очікуваного результату.

Приклад повної URL-адреси мого зображення, що завантажено у Azure Blob Storage має вигляд: https://fffff.blob.core.windows.net/new123/nwphoto.png

Приклад результату роботи програми є повертане значення у вигляді:


```
[
  {
    "faceId": "bdce33af-0cad-487c-9fa5-0bd205322087",
    "faceRectangle": {
      "top": 70,
      "left": 660,
      "width": 66,
      "height": 86
    }
  }
]
```


У розділі розглянуто алгоритм створення прикладу JavaScript API обличчя Cognitive Services Azure, а саме: створення API обличчя Azure Cognitive Services на порталі Azure, розробку JavaScript для виявлення облич на зображенні та використання ключа та кінцевої точки із використанням Azure Face API.

2 ОХОРОНА ПРАЦІ

Вступ

Законодавство України про охорону праці являє собою систему взаємозв'язаних нормативно-правових актів, що регулюють відносини у галузі реалізації державної політики щодо правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці.

Базується законодавство України про охорону праці на конституційному праві всіх громадян України на належні, безпечні і здорові мови праці, гарантовані статтею 43 Конституції України.

Робоче місце користувача послуг біометричних систем може складатися з персонального комп'ютеру та мобільних пристроїв. Тому для нього застосовуються звичайні вимоги користувача персонального комп'ютера.

2.1 Аналіз умов праці й забезпечення безпеки при виконання основних видів робіт на об'єкті дипломного проектування

Однакові по складності зміни в організмі людини можуть бути викликані різними причинами.

Це можуть бути фактори виробничого середовища, надмірне фізичне і розумове навантаження, нервово-емоційна напруга, а також різне сполучення цих причин.

Робота за комп'ютером, як і будь-яка інша, має свої небезпечні виробничі фактори, які враховуються при складанні відповідних правил і норм ОП і ТБ.

2.1.1 Гігієнічні вимоги до виробничого середовища.

На робочому місці програміста необхідно враховувати санітарні нормативи

освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення.

2.1.2 Вимоги до організації робочого місця працівника

Конструкція робочого місця користувача персонального комп'ютера має забезпечувати підтримання оптимальної робочої пози офісного працівника та відповідати сучасним нормам ергономіки, а також забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів.

Робочий стіл повинен мати простір для ніг. Робочий стілець має бути підйомно-поворотним, регульованим за висотою, з кутом і нахилу сидіння та спинки регулювання за кожним із параметрів має здійснюватися незалежно, легко і надійно фіксуватися.

Для зниження статичного напруження м'язів верхніх кінцівок слід використовувати стаціонарні або змінні підколінники.

Поверхня сидіння і спинки стільця має бути напівм'якою з нековзним, повітронепроникним покриттям, що легко чиститься і не електризується.

Робочі місця слід розташовувати відносно світових прорізів так, щоб природне світло падало переважно з лівого боку.

Розташування екрану монітору має забезпечувати зручність зорового спостереження у вертикальній площині під кутом +30 градусів до нормальної лінії погляду працівника.

Клавіатуру слід розташовувати на поверхні столу на відстані 100-300мм від краю, звернутого до працюючого.

У конструкції клавіатури має передбачатися опорний пристрій (виготовлений з матеріалу з високим коефіцієнтом тертя, що перешкоджає мимовільному її зсуву).

Під матричні принтери потрібно підкладати вібраційні килимки для гасіння вібрації та шуму. Робоче місце з персональним комп'ютером слід обладнати пюпітром для документів.

2.1.3 Освітлення, шум

Для освітлення приміщення, у якому працює програміст, використовується змішане освітлення, тобто сполучення природного й штучного освітлення. Природне освітлення - здійснюється через вікна в зовнішніх стінах будинку. Штучне освітлення - використовується при недостатньому природному освітленні й здійснюється за допомогою двох систем: загального й місцевого освітлення.

Для загального освітлення приміщення, де перебуває робоче місце програміста, використовуються газорозрядні лампи типу ЛД.

Нормами для даних робіт установлена необхідна освітленість робочого місця ЕН=300 лк (для робіт високої точності, коли найменший розмір об'єкта розрізнення дорівнює 0,3 – 0,5 мм).

Джерелами шуму при роботі з ПК є жорсткий диск, вентилятор блока живлення мережі, вентилятор, розташований на процесорі, швидкісні СБ-КОМ, механічні сканери, пересувні механічні частини принтера.

При роботі матричних голчастих принтерів шум виникає при переміщенні головки принтера і у процесі удару голок головки по паперу.

При роботі вентиляційної системи ПК, яка забезпечує оптимальний температурний режим електронних блоків, створюється аеродинамічний шум. Крім того, діють інші зовнішні джерела шуму, не пов'язані з роботою ПК.

Шум, що створюється працюючими ПК, є широкосмужним, постійним з аперіодичним посиленням при роботі принтерів.

Допустимий еквівалентний рівень шуму для робочого місця оператора складає 65 дБА.

Під час виконання робіт з ПК у виробничих приміщеннях значення характеристик вібрації на робочих місцях мають не перевищувати допустимі відповідно до ДСанПіН 3.3.2.007-98, ДСН 3.3.6-039-99.

2.1.4 Мікроклімат

Для постійних робочих місць, якими є робочі місця операторів ПК, встановлені оптимальні параметри мікроклімату, а за неможливості їх дотримання використовують допустимі параметри

Температура повітря в приміщенні 22...24°С;

відносна вологість 40... 60%;

швидкість руху повітря до 0,1…0,2 м/с.

Для підтримки в приміщеннях нормального, що відповідає гігієнічним вимогам складу повітря, видалення з нього шкідливих газів, пару і пилу використають вентиляцію.

В розроблюваному дипломному проекті рекомендовано застосування припливної вентиляції та застосування кондиціонерів.

2.1.5 Електробезпека

Приміщення, де використовуються імпульсні джерела живлення відповідно до ОНТП24-86 і ПУЕ-87 відноситься до класу приміщень без підвищеної небезпеки поразки персоналу електричним струмом, оскільки відносна вологість повітря не перевищує 75%, температура не більш 35ºС, відсутні хімічно агресивні середовища.

Живлення електроприладів усередині приміщення здійснюється від двухфазної мережі з заземленою нейтралю напругою 220 В і частотою 50 Гц із використанням автоматів токового захисту.

У приміщенні повинна бути застосована схема заземлення.

Ураження людини електричним струмом може відбутися у випадку:

1. дотику до відкритих струмоведучих частин;
2. у результаті дотику до струмопровідних не струмоведучих

елементів устаткування, що опинилися під напругою в результаті порушення ізоляції або з інших причин.

Заземлення повинно бути зроблено за допомогою гнучкого сплетеного мідного проводу діаметром порядку 1,5 мм2.

Для зменшення значень напруг дотику і відповідних їм величин струмів, при нормальному й аварійному режимах роботи устаткування необхідно виконати повторне захисне заземлення нульового проводу.

Відповідно до ГОСТ-12.2.007.0-75 все устаткування (крім ЕОМ - II клас) відноситься до I класу, воно має робочу ізоляцію відповідно до вимог ГОСТ

12.1.009-76.

Підключення устаткування виконане відповідно до вимог ПБЕ та ПУЕ. Додаткових заходів по електробезпечності не потрібно.

2.2 Пожежна безпека

Пожежна безпека входить в комплекс заходів з охорони праці, і включає широкий спектр заходів, а саме:

1) створення умов для безпечної праці, мінімізації ризику виникнення пожеж,

2) своєчасне і повноцінне забезпечення технічними засобами для запобігання займання та усунення самих пожеж та їх наслідків,

3) контроль дотримання протипожежних вимог і норм законодавства,

Приміщення з персональними комп'ютерами рекомендується оснащувати вуглекислотними вогнегасниками з урахуванням граничнодопустимої концентрації вогнегасної речовини.

Для зазначення місцезнаходження первинних засобів пожежогасіння слід установлювати відповідні знаки згідно з чинними державними стандартами

Переносні вогнегасники повинні розміщуватися шляхом:

1. навішування на вертикальні конструкції на висоті не більше 1,5 м від рівня підлоги до нижнього торця вогнегасника і на відстані від дверей, достатній для її повного відчинення;

2. установлення в пожежні шафи пожежних кранів, або у спеціальні тумби;

3. навішування вогнегасників на кронштейни, розміщення їх у тумбах або пожежних шафах повинне забезпечувати можливість прочитання маркувальних написів на корпусі.

Експлуатація та технічне обслуговування вогнегасників повинно здійснюватися відповідно до вимог Правил експлуатації вогнегасників (НАПБ Б.01.008-2004).

Використані вогнегасники, а також вогнегасники із зірваними пломбами

необхідно негайно направляти на перезаряджання або на перевірку.

У розділі охорони праці розглянуто питання охорони праці, які сприяють безпечному використанню персональних комп’ютерів та мобільних пристроїв у біометричних системах.

ВИСНОВКИ

Основною метою впровадження біометричних технологій у системи контролю доступу є покращення ефективності розпізнавання особи шляхом автоматизації процесу верифікації/ідентифікації.

Відносно розповсюджених систем надання доступу, методи яких оперують паролями та картками, біометричні технології пропонують значно більший ступінь захисту.

У кваліфікаційній роботі були розглянуті та вирішені такі задачі:

1) Розглянуто основні типи біометричних систем.

Біометричні системи за базовими параметрами, які застосовуються в процесі розпізнавання людини – це наступні унікальні характеристики людини: риси обличчя, структура ока, особливості відбитків пальців, голос, специфіка підпису, особливості введення тексту з клавіатури та інші.

2) Розглянуто використання та роботу біометричних систем ідентифікації. Виконано аналіз їх переваг та недоліків таких як: швидкість процесу ідентифікації, зручність даної процедури з точки зору користувача, ймовірність виникнення помилок першого та другого роду, коштовність необхідного обладнання.

У досліджені було проведено аналіз кожної з біометричних систем та обрано одну з біометричних систем для побудови системи контролю доступу до об'єкта із використанням смартфонів та програмного забезпечення Azure Cognitive Services Face API.

У розділі охорони праці розглянуто шляхи підвищення безпеки використання комп’ютерного обладнання у системі ідентифікаціїї особистості.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію: Закон України// Відомості Верховної Ради України. - 2001.- № 11.- С. 25-27.
2. Міністерство соціальної політики України НАКАЗ 14.02.2018 № 207 Зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за № 508/31960 Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями [Електронний ресурс]– Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0508-18#Text (Дата звернення 10.06.23)
3. Закон України 2155-VIII «Про електронні довірчі послуги» від 05.10.2017. [Електронний ресурс]–Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2155-19/ed20171005#n9 (дата звернення:10.04.2023).
4. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації вкомп'ютерних системах від несанкціонованого доступу» [Електронний ресурс]–Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=5A88E6FEAB902185A2100ECC92151B59?showHidden=1&art_id=101853&cat_id=89734&ctime=1344501024406 (дата звернення: 10.04.2023).
5. Романов В. Биометрическая идентификация личности: современное состояние и перспективы развития в Украине / В. Романов, И. Галелюка,П. Клочан. //Электронные компоненты и системы. – 2010. – №5. – С. 16–20.
6. ISO/IEC 19785-1:2015 Information technology — Common BiometricExchange
7. Formats Framework — Part 1: Data element specification [Електронний ресурс]. Режим доступу до ресурсу: https://www.iso.org/ru/standard/66179.html.
8. Брюхомицкий Ю. А. Тестирование биометрических систем контроля [Електронний ресурс]– / Ю. А. Брюхомицкий, М. Н. Казарин. – 2006. – Режим доступу до ресурса: https://cyberleninka.ru/article/n/testirovanie-

biometricheskihsistem-kontrolya-dostupa/viewer. (дата звернення:10.04.2023).
9. Гинце А. Новые технологии в СКУД [Електронний ресурс] / А. Гинце //Системы безопасности. – 2005. – Режим доступу до ресурсу: https://www.aktivsb.ru/statii/novye_tekhnologii_v_skud.html. (дата звернення: 10.04.2023).
10. ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация.Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца»
11. ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация.Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальцев».
12. ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными.Часть 5. Данные изображения лица».
13. ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными.
Часть 6. Данные изображения радужной оболочки глаза».
14. Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис.Теорія та практика: монографія./ І.Д. Горбенко, Ю.І. Горбенко – Харків: «Форт», 2010. – 608 с.
15. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія./ І.Д. Горбенко, Ю.І. Горбенко – Харків: «Форт», 2012.
16. .Богуш В.М., Юдін О.К. Інформаційна безпека держави. - К.: «МК-Прес»,2005.- 432с.
17. Конспект лекцій з дисципліни «ОХОРОНА ПРАЦІ В ГАЛУЗІ» О.А. Толок, 2015р. [Електронний ресурс]–Режим доступу до ресурсу: http://www.dstu.dp.ua/Portal/Data/5/10/5-10-kl25.pdf (Дата звернення

10.06.23)

18. Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" : УКАЗ ПРЕЗИДЕНТА УКРАЇНИ від 27 січня 2016 р. [Електронний ресурс]. Режим доступу до ресурсу:: https://zakon.rada.gov.ua/laws/show/96/2016. (дата звернення: 15.05.2023).
19. Конвенція про кіберзлочинність : веб-сайт Верховної Ради України : від 07 вересня 2005р. [Електронний ресурс]. Режим доступу до ресурсу:: https://zakon.rada.gov.ua/laws/show/994_575

(дата звернення: 15.05.2023).

20. Оперативна інформація Держспецзв’язку щодо захисту державних інформаційних ресурсів : від 16 червня 2020 [Електронний ресурс]. Режим доступу до ресурсу:: http://www.dsszzi.gov.ua/ dsszzi/control/uk/publish/article;jsessionid=07515BBA5DC8FCDE53AF420BD 4C 0 5FB8.app1?art_id=321621&cat_id=317163 (дата звернення: 15.05.2023).

ДОДАТОК А

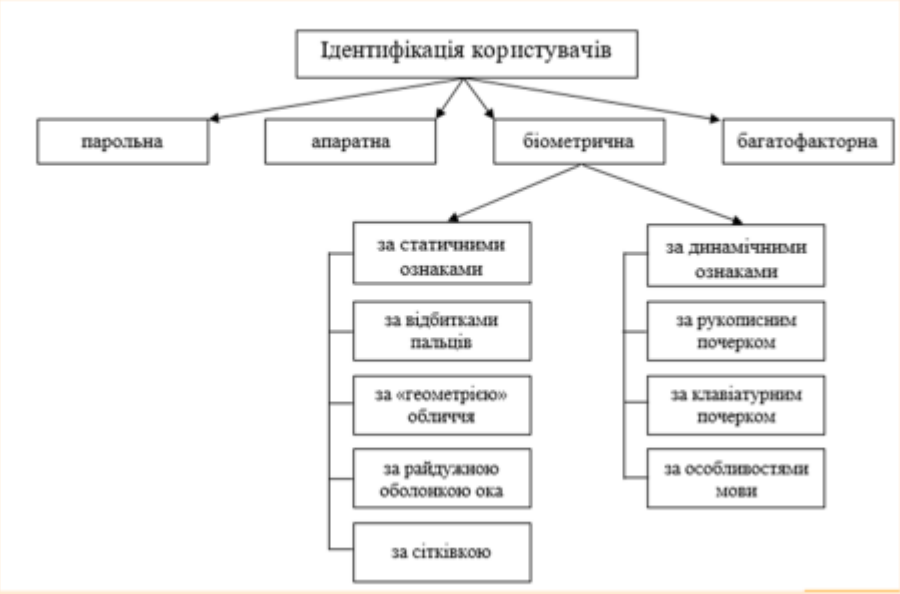
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Дослідження біометричних систем комп'ютерної ідентифікації особистості

Виконав: Борщ О.О., гр.2БКС-27

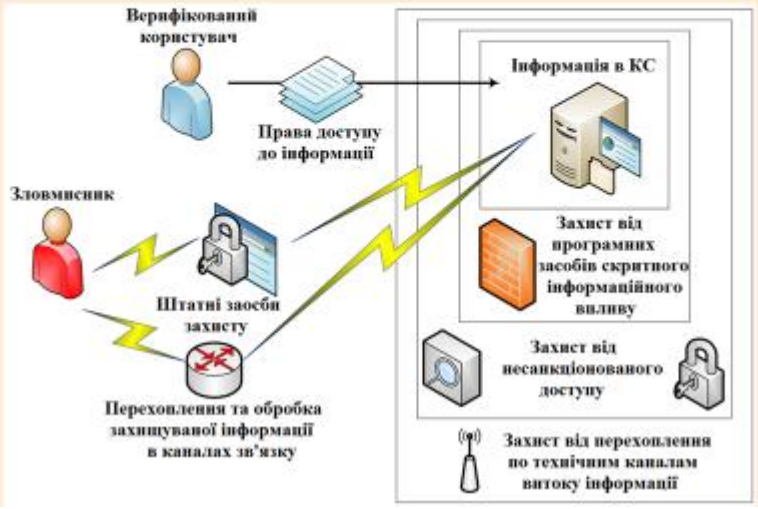
Слайд 1

Узагальнена структура методів ідентифікації особистості



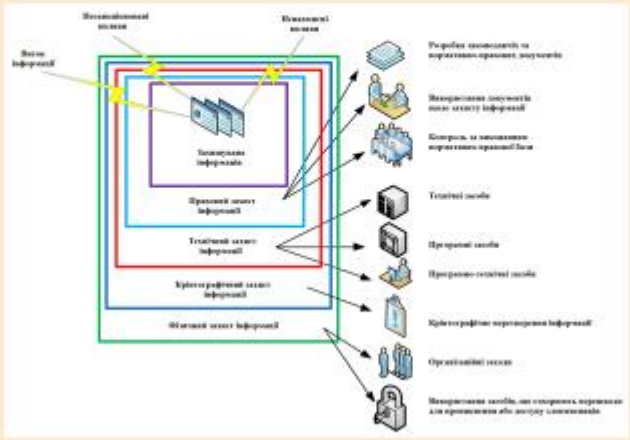
Слайд 2

Система захисту інформації в комп'ютерних системах



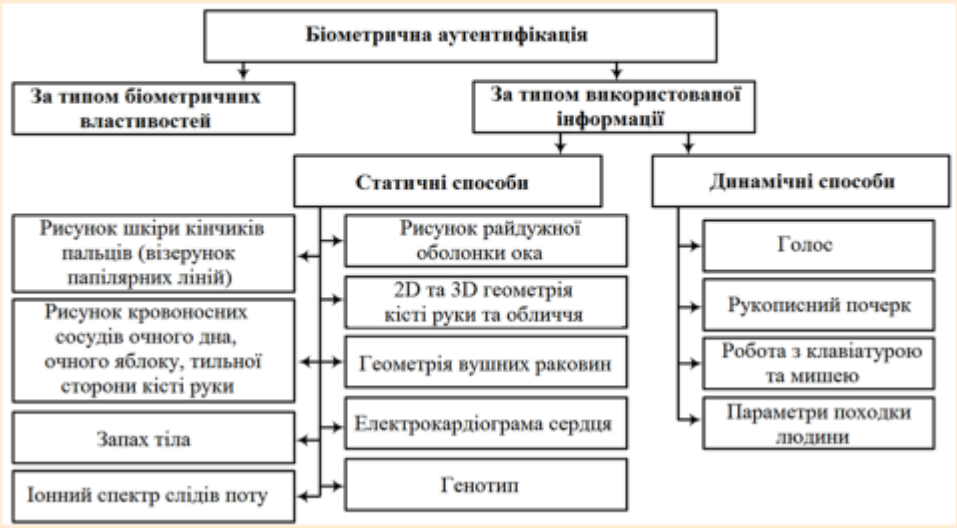
Слайд 3

Комплекс заходів щодо забезпечення інформаційної безпеки



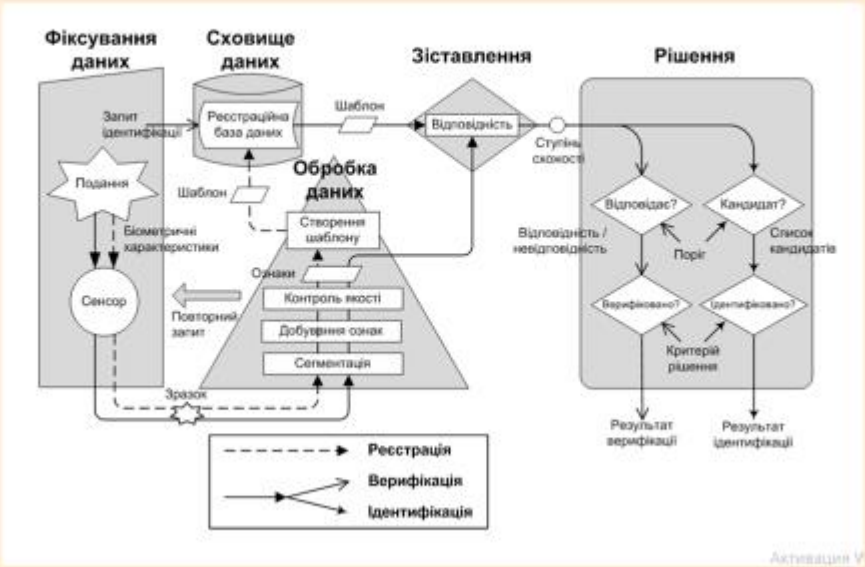
Слайд 4

Класифікація способів біометричної ідентифікації користувачів комп'ютерних систем



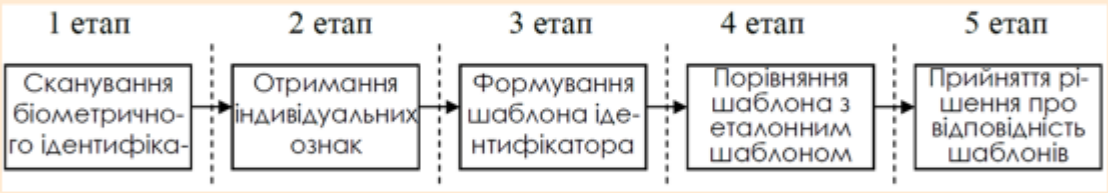
Слайд 5

Концептуальна модель біометричної системи



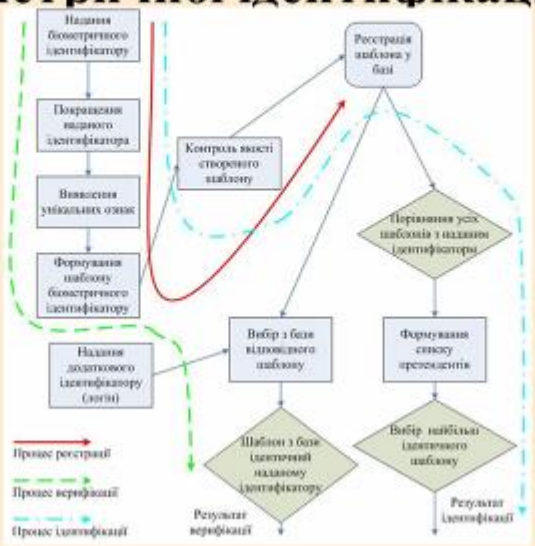
Слайд 6

Загальний алгоритм функціонування систем біометричної ідентифікації



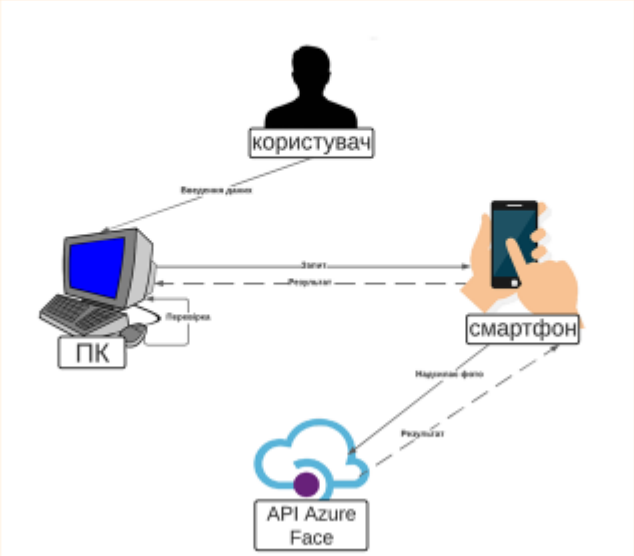
Слайд 7

Узагальнений алгоритм роботи системи біометричної ідентифікації



Слайд 8

Алгоритм розпізнавання Face API



Слайд 9

ВИСНОВКИ

У кваліфікаційній роботі бакалавра досліджено наступне:
1) Розглянуто основні типи біометричних систем.
2) Розглянуто використання та роботу біометричних систем ідентифікації. Виконано аналіз їх переваг та недоліків.

Ознайомившись із основними методами біометричної ідентифікації та їх характеристиками, такими як швидкість процесу ідентифікації, зручність даної процедури з точки зору користувача, ймовірність виникнення помилок першого та другого роду, коштовність необхідного обладнання, було проведено аналіз кожної з біометричних систем та обрано одну з біометричних систем для побудови структури системи контролю доступу до об'єкта із використанням смартфонів та програмного забезпечення Azure Cognitive Services Face API.

У розділі охорони праці розглянуто шляхи підвищення безпеки використання комп'ютерного обладнання у системах ідентифікаціїї особистості.

Слайд 10

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Борщ Олег Олегович
здобувач освіти гр. 2БКС-27, та

Краснієнко Наталія Володимірівна,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи молодшого спеціаліста на тему:

«Дослідження біометричних систем комп'ютерної ідентифікації особистості» ***(автор роботи – Борщ О.О., керівник роботи – Краснієнко Н.В.)***

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Борщ О.О./

Керівник _____ / Краснієнко Н.В./

«___15___» _____06_____ 2023 ____ р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ КОЛЕДЖ ОНАХТ»

ВІДГУК

керівника про кваліфікаційну роботу бакалавра

Борща Олега Олеговича

(прізвище, ім`я та по батькові здобувача/здобувачки освіти)

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

Тема кваліфікаційної роботи

«Дослідження біометричних систем комп'ютерної ідентифікації особистості»

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) обсяг і якість виконання роботи (розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над кваліфікаційною роботою

Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Провів аналіз біометричних технологій, представив модель для СКУД. Виявив навички самостійно опрацьовувати новий матеріал та виконувати пошук необхідної літератури та інших джерел інформації.

в) теоретична підготовка бакалавра

відповідає вимогам, що надаються до бакалавра зі спеціальності 123 «Комп'ютерна інженерія»

г) вміння розв'язувати виробничі та конструкторські питання _____

У кваліфікаційній роботі було проведено аналіз кожної з біометричних систем та обрано одну з біометричних систем для побудови системи контролю доступу до об'єкта із використанням смартфонів та програмного забезпечення Azure Cognitive Services Face API.

Оцінка розрахункової частини _____4(відмінно)_____

Оцінка графічної (презентаційної) частини _____4(добре)_____

Загальна оцінка _____4 (добре)_____

Прізвище, ім'я, по батькові керівника роботи___Краснієнко Наталія Володимирівна

____

Місце роботи і посада керівника роботи _____завідувач лабораторії технічного захисту аналітико-інформаційних технологій ВСП ОТФК ОНТУ, викладач-методист вищої_____ кваліфікаційної категорії_____

«__15__»____06____2023__р. _____ _Краснієнко Н.В.

(підпис) (прізвище та ініціали керівника)

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ КОЛЕДЖ ОНАХТ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
відділення комп'ютерних систем

Борцу Олегу Олеговичу

(прізвище, ім`я та по батькові)

Напрямку підготовки *123 «Комп'ютерна інженерія»*

Керівник кваліфікаційної роботи

Краснієнко Наталія Володимирівна

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи

Дослідження біометричних систем комп'ютерної ідентифікації особистості

Обсяг пояснювальної записки 60 сторінок

Обсяг графічної (презентаційної) частини проекту 10 аркушів (слайдів)

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) заключення про ступінь відповідності виконаної роботи завданню

Робота відповідає технічному завданню до дипломного проекту. Виконана у відповідності з вимогами.

б) характеристика виконання кожного розділу роботи

При виконанні дипломного проекту здобувач освіти продемонстрував уміння використовувати останні досягнення науки та техніки, уміння працювати з літературою. Так, студент грамотно дослідив та проаналізував технологію автентифікації особистості. Запропонував алгоритм ідентифікації особистості із використанням Azure Cognitive Services Face API за створеним ідентифікатором обличчя Face ID

в) оцінка якості виконання графічної (презентаційної) частини роботи і пояснювальної записки

Графічна частина відповідає вимогам, виконана якісно та відображає основні елементи проектування системи. Містить етапи впровадження біометричних систем для комп'ютеної ідентифікації особистості

г) перелік позитивних якостей роботи

Тема дипломного проекту є актуальною, виконана у достатньому обсязі, якісно, відповідно до поставленого завдання. Досліджено та запропоновано аалгоритм біометричної системи для побудови системи контролю доступу до об'єкта із використанням смартфонів та програмного забезпечення Azure Cognitive Services Face API

д) основні недоліки роботи У тексті пояснювальної записки відсутні посилання на використану літературу, для підвищення ефективності дослідження можна було б більш детально розглянути ступінь захисту таких систем

Оцінка розрахункової частини добре

Оцінка графічної (презентаційної) частини добре

Загальна оцінка добре

Прізвище, ім'я та по батькові рецензента Царьов Роман Юрійович

Місце роботи і посада рецензента Державний університет інтелектуальних технологій і зв'язку, старший викладач кафедри комп'ютерної інженерії та інформаційних систем

«16» червня 2023 р. (підпис) Царьов Р. Ю. (прізвище та ініціали рецензента)

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ
КАДРІВ ДУІТЗ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ * 43997335 * ВІДДІЛ КАДРІВ

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015173053

Дата перевірки:
22.05.2023 11:23:04 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
22.05.2023 11:31:06 EEST

ID користувача:
100011688

Назва документа: **2БКС-27_Олег_Борщ**

Кількість сторінок: **58** Кількість слів: **6253** Кількість символів: **49670** Розмір файлу: **2.81 MB** ID файлу: **1014852442**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

35.6%
Схожість

Найбільша схожість: 7.68% з Інтернет-джерелом (https://openarchive.nure.ua/bitstream/document/15305/1/2020_M_IKI...

33.7% Джерела з Інтернету	717	Сторінка 60
11.9% Джерела з Бібліотеки	5	Сторінка 63

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

11.2%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 0%)

11.2% Вилучення з Інтернету	28	Сторінка 64

Немає вилучених бібліотечних джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	20
Підозріле форматування	6 сторінок