Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

Підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії

Виконала: ст. 2-го курсу, групи УБ-20м
спеціальності 125– Кібербезпека
Освітня програма – Управління інформаційною безпекою
(шифр і назва напряму підготовки, спеціальності)

Безмощук О. В.
(прізвище та ініціали)

Керівник: к.т.н., проф. каф МБІС
Азарова А. О.
(прізвище та ініціали)
«____» _____ 2021 р.

Опонент: к.т.н., доц., доцент каф. ОТ
Савицька Л. А.
(прізвище та ініціали)
«____» _____ 2021 р.

Допущено до захисту
Голова секції УБ кафедри МБІС
д.т.н., проф. Яремчук Ю.Є.
«____» _____ 2021 р.

Вінниця ВНТУ - 2021 рік

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

АНОТАЦІЯ

Під час виконання роботи було здійснено аналіз теоретичних засад біометричної ідентифікації користувачів у системах безпеки. Досліджено переваги та недоліки даного виду ідентифікації, проаналізовано методи реалізації біометричного розпізнавання та особливості їх використання, при цьому значна увага приділялася методу дактилоскопії та розпізнаванню за образом обличчя.

У магістерській дипломній роботі вдосконалено метод дактилоскопії з використанням оператора Собеля, що уможливило підвищення достовірності ідентифікації користувачів.

На основі запропонованого автором удосконаленого методу розпізнавання відбитків пальця було розроблено відповідний програмний засіб, що уможливив комплексну ідентифікацію осіб за їх біометричними даними – відбитками пальців. Програмна реалізація даного додатку здійснювалася мовою програмування C# у середовищі Visual Studio.

Ключові слова: біометрична ідентифікація, дактилоскопія, відбиток пальця, розпізнавання, сегментація, оператор Собеля.

SUMMARY

During the master's thesis the analysis of theoretical bases of biometric identification of users in security systems was carried out. The advantages and disadvantages of this type of identification are studied, the methods of biometric recognition implementation and features of their use are analyzed, and considerable attention was paid to the method of dactyloscopy and facial image recognition.

In the master's thesis the method of dactyloscopy with the use of the Sobel operator was improved, which made it possible to increase the reliability of user identification.

On the basis of the improved method of fingerprint recognition proposed by the author, an appropriate software tool was developed, which enabled the complex identification of individuals by their biometric data - fingerprints. The software implementation of this application was carried out in the C # programming language in Visual Studio.

Key words: biometric identification, dactyloscopy, fingerprint, recognition, segmentation, Sobel operator.

ЗМІСТ

ВСТУП

Актуальність. Біометрична ідентифікація – це автоматизований метод, що уможливлює ідентифікацію особи шляхом перевірки унікальних фізіологічних особливостей людини. Такі фізіологічні особливості, як папілярний узор пальця, геометрія долоні або малюнок райдужної оболонки ока є постійними фізичними характеристиками людини. Даний тип вимірів (перевірки) практично незмінний, як і самі фізіологічні характеристики.

У багатьох випадках процес ідентифікації особи за відбитками пальця привертає до себе увагу як важлива біометрична технологія. Застосування відбитка пальця для ідентифікації особи в системі є найбільш зручним зі всіх біометричних методів, оскільки ймовірність помилки є суттєво меншою порівняно з іншими біометричними методами.

Сьогодні технологія ідентифікації особистості методом дактилоскопії активно використовується у різноманітних галузях, зокрема, у системі управління доступом, інформаційній безпеці, різних соціальних проектах, де потрібна ідентифікація людей і т. п.

Розпізнавання відбитків пальців – один із потужних біометричних методів. Він ґрунтується на визначенні структури ліній на подушечках пальців рук, інакше – папілярних візерунках. Після зчитування сканером, унікальний малюнок трансформується на цифровий біометричний шаблон, за допомогою якого система визначає, хто перед нею знаходиться.

Питання ідентифікації користувачів досліджується в роботах багатьох провідних науковців, таких, як Домарьов В. В., Захаров В. П., Карпінець В. В., Рудешко В. І., Сафронов В. В., Хорошко В. А., Яремчук Ю. Є. та ін. [1 – 7]. Із розвитком сучасних інформаційних технологій доступ до системи з використанням біометричного методу дактилоскопії для ідентифікації користувачів стає все більш поширеним. Разом із тим, деякі методи дактилоскопії мають недоліки, що полягають у їх складності в реалізації та великій математичній базі, неможливості підключення до деяких баз даних та,

зокрема, недостатній точності. Такі проблеми методу зумовлюють актуальність застосування оператора Собеля при реалізації біометричної ідентифікації методу дактилоскопії з метою підвищення достовірності ідентифікації користувачів.

Мета і задачі дослідження. Метою роботи є розроблення та реалізація програмного засобу для підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії.

Задачами дослідження є:

– проаналізувати недоліки та переваги існуючих методів і засобів біометричної автентифікації та особливості їх застосування;

– дослідити специфіку використання та реалізації процедури ідентифікації користувачів методом дактилоскопії;

– удосконалити метод розпізнавання відбитку пальця за методом Собеля;

– розробити алгоритм роботи програмного додатку для ідентифікації користувачів на основі удосконаленого методу розпізнавання відбитків пальців;

– обґрунтувати вибір мови та середовища програмування для додатку;

– спроектувати та розробити інтерфейс користувача додатку;

– розробити програмний засіб для підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії;

– обґрунтувати економічну доцільність програмного додатку.

Об’єкт дослідження – процес ідентифікації користувачів за методом дактилоскопії.

Предмет дослідження – розроблення удосконаленого методу розпізнавання відбитку пальця з використанням оператора Собеля.

Наукова новизна дослідження полягає в удосконаленні методу розпізнавання відбитку пальця, що, на відміну від існуючих підходів, дозволяє підвищити точність розпізнавання відбитків пальців, використовуючи метод дактилоскопії на основі оператора Собеля.

Практична цінність дослідження полягає у створенні програмного засобу, що уможливлює більш точну автентифікацію користувачів на основі удосконаленого методу дактилоскопії.

Апробація результатів дослідження відбулася на Науково-технічній конференції підрозділів Вінницького національного технічного університету (м. Вінниця, 2020р., 2021р.) [8 – 9] та Всеукраїнській науково-практичній Інтернет-конференції студентів, аспірантів та молодих науковців «МОЛОДЬ В НАУЦІ: ДОСЛІДЖЕННЯ, ПРОБЛЕМИ, ПЕРСПЕКТИВИ (МН-2022) [10 – 11]

Результати роботи представлені у 1 турі Всеукраїнського конкурсу студентських наукових робіт зі спеціальності "Кібербезпека" у 2021-2022рр.

Публікації. Було опубліковано 4 тез доповідей.

1 АНАЛІЗ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ ТА ТОКЕНІВ

1.1 Сутність та класифікація біометричних засобів у системах захисту інформації

Типові системи автентифікації за сучасних умов не завжди задовольняють вимогам політики інформаційної безпеки підприємства чи компанії, які до них висувають. Саме тому все більшої популярності набирає біометрична автентифікація користувача, що дозволяє автентифікувати користувача за допомогою зчитування його фізіологічних даних [8].

Методи автентифікації, що базуються на паролях, мають вагомий недолік: багаторазовий пароль можна скомпрометувати різними способами. USB-токени та смарт-карти можна втратити, скопіювати. У біометричних методах автентифікації таких проблем майже не існує.

Як біометричні параметри можуть використовуватися такі: форма кисті руки; відбиток пальця; розмір та форма особи; візерунок сітківки ока та райдужної оболонки; особливості голосу.

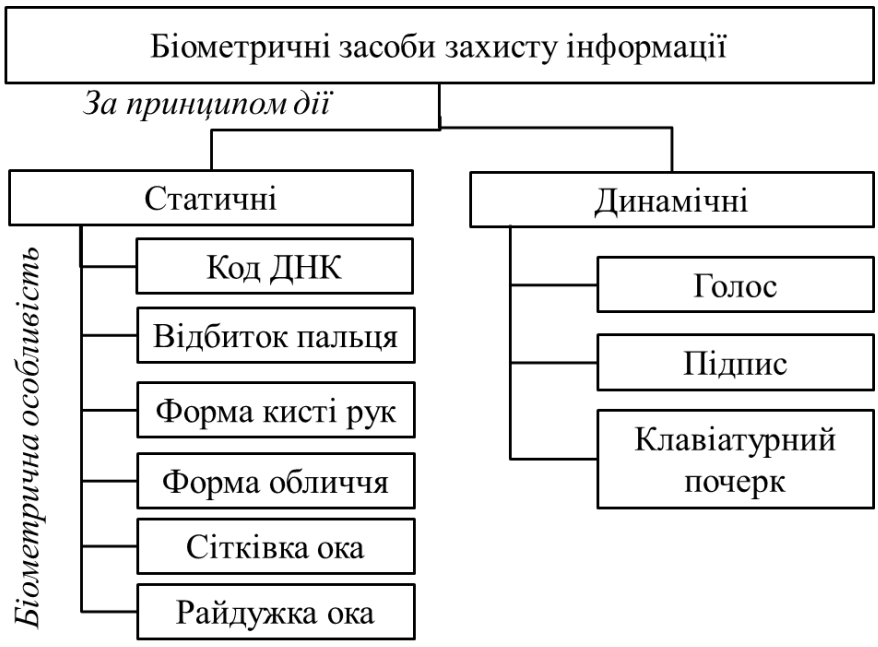


Рисунок 1.1 – Класифікація біометричних засобів захисту інформації (за [8 – 9])

До основних переваг таких методів можна віднести: великий рівень достовірності автентифікації за біометричними параметрами у зв'язку з їх унікальністю, невіддільність біометричних параметрів від користувача, складність фальсифікації біометричних ознак.

Розглянемо схему роботи біометричної системи автентифікації [10].

Під час реєстрації в системі користувач повинен зафіксувати в системі один або кілька разів біометричну ознаку, за якою відбувається подальша автентифікація. Ці ознаки у системі реєструються як контрольний зразок користувача. Цей зразок обробляється системою отримання ЕІП (еталонний ідентифікатор користувача).

ЕІП – числова послідовність, з якої не можна відновити початковий зразок. При проходженні автентифікації користувачем порівнюється еталонні ЕІП та ЕІП при проходженні автентифікації. Оскільки ці два параметри ніколи не збігатимуться, існує параметр, що відповідає за ступінь збігу.

На основі цього ступеня збігу система вирішує проходження автентифікації [11 – 12].

Помилкова відмова (FRR) – це відмова, коли система не підтверджує законного користувача. Такі відмови бувають 1 на 100.

Помилкове підтвердження (FAR) – підтвердження, коли система підтверджує автентифікацію незаконного користувача. Такі помилки бувають 1 на 10 000.

Біометрична автентифікація: зручність чи безпека. Поняття «автентифікація» характеризує перевірку на справжність. Процес автентифікації може бути виконаний одним із трьох можливих способів:

– заснований на тому, що можу бути відомо користувачеві, наприклад кодова комбінація (пароль);

– заснований на тому, що у користувача наявний: ключ, магнітна карта, брелок;

– те, що належить безпосередньо тільки користувачеві: папілярні візерунки, геометрія обличчя, будова ока.

Саме третій пункт містить у собі біометричну автентифікацію, яка з розвитком технологій стає дедалі актуальнішою.

Основна перевага та недолік біометричної автентифікації [13 – 14].

Явна перевага системи – зручність, тому що немає необхідності запам'ятовувати кодову комбінацію (пароль) або послідовність графічного ключа, думати про те, що краще встановити: ПІН-код чи графічний ключ?

Явний недолік – безпека, оскільки існує низка вразливостей і система розпізнавання не є надійною на всі 100%. У той самий час біометричні параметри (відбиток пальця чи малюнок райдужної оболонки) не можна змінити, на відміну пароля чи ПІН-коду. Це істотний недолік, оскільки, якщо один раз дані потраплять до зловмисника ми піддаємо себе серйозним ризикам.

Враховуючи, наскільки зараз поширена біометрична технологія розпізнавання в сучасних смартфонах, є кілька рекомендацій, які дозволяють певною мірою підвищити рівень захисту.

Більшість відбитків, які залишаються на поверхні – це відбитки великого пальця та вказівного, тому для автентифікації на смартфоні найкраще використовувати інші пальці; незважаючи на наявність біометричної перевірки, застосування надійного пароля або ПІН-коду – обов'язкова умова для повноцінної безпеки.

Біометричні системи автентифікації як спосіб реалізації контролю.

Сьогодні біометричні системи захисту застосовуються все частіше завдяки розробкам нових математичних алгоритмів автентифікації. Коло завдань, яке вирішується за допомогою нових технологій, досить широке [15]:

– охорона правопорядку та криміналістика;

– пропускна система (СКУД) та обмеження доступу в громадські та комерційні будівлі, приватні житла (розумний будинок);

– передача та отримання конфіденційної інформації особистого та комерційного характеру;

– здійснення торгових, фінансових та банківських електронних операцій;

– вхід на електронне віддалене та/або локальне робоче місце;

– блокування роботи сучасних гаджетів та захист електронних даних (ключ криптації);

– ведення та доступ до урядових ресурсів;

Умовно, біометричні алгоритми автентифікації можна умовно поділити на два основні типи:

Статичні – дактилоскопія, райдужна оболонка очей; вимірювання форми кисті, лінії долонь, розміщення кровоносних судин, вимірювання форми обличчя в 2D та 3D алгоритмах;

Динамічні – почерк та ритм набору тексту; хода, голос тощо.

Основними видами сучасних біометричних систем є [16]:

– розпізнавання за відбитками пальців; розпізнавання за райдужною оболонкою ока;

– розпізнавання по геометрії особи; розпізнавання по сітківці ока; розпізнавання по геометрії руки;

– розпізнавання по малюнку вен долоні.

Розглянемо у порівнянні деякі з них.

Таблиця 1.1 – Порівняння біометричних методів ідентифікації (за [17])

Біометричні сканери	Дактилоскопія (розпізнавання відбитків пальців)		Райдужна оболонка		Розпізнавання за обличчям	
Об'єкт методу	Відбиток пальця		Райдужна оболонка ока		2D розпізнавання	
Методика	Унікальність для кожної людини малюнка папілярних візерунків на пальцях		Виділення зображення райдужної оболонки ока за допомогою декількох знімків		3D розпізнавання	
Статистичні характеристики методу (середні)	FAR	FRR	FAR	FRR	FAR	FRR
	0,10%	0,30%	0,10%	0, 065%	0,10%	2,5%
	0,01%	0,40%	0,01%	0,070%	0,01%	05%
	0,0010%	0,60%	0,0010%	0,115%	0,0010%	6%
	0,0001%	0,90%	0,0001%	0,150%	0,0001%	9%
Переваги методу	Низька вартість пристроїв сканування,		Надійність алгоритму, захист об'єкта від		Відсутність необхідності контакту із	

	простота процедури	пошкоджень і підробок	пристроєм сканування. Низька чутливість до зовнішніх факторів Високий рівень надійності
Недоліки методу	Високий ступінь відмови, залежність від зовнішніх впливів (поріз, опік), можливість підробки	Висока ціна, низька доступність готових рішень	Дороговизна обладнання. Зміни міміки погіршують статистичну надійність методу
Основні виробники	SecBayometric Inc., Digital Persona Inc., BioLink, Сонда, СмартЛок	LG Electronics, Panasonic, OKI. Iris Access 2200, BMET500, OKI IrisPass,	Artec Group, Cognitec Systems GmbH, Bioscrypt, Identity Solutions Genex Technologies

Більш детальніший аналіз методів біометричної ідентифікації на сучасному етапі проведемо у наступних підрозділах, зокрема, здійснимо порівняння надійності, зручності, швидкості оброблення даних різними методами.

1.2 Вивчення існуючих методів біометричної ідентифікації

Порівняємо методи біометричної ідентифікації з використанням математичної статистики (FAR та FRR) [18 – 19].

Головними для оцінювання будь-якої біометричної системи є два параметри:

– FAR (False Acceptance Rate) – коефіцієнт помилкового пропуску, тобто відсоток виникнення ситуацій, коли система дозволяє доступ користувачеві, який є незареєстрованим у системі.

– FRR (False Rejection Rate) – коефіцієнт хибної відмови, тобто відмова у доступі справжньому користувачеві системи.

Обидві характеристики отримані розрахунковим шляхом з урахуванням методів математичної статистики. Чим нижчі ці показники, тим точніше розпізнавання об'єкта.

Для найпопулярніших сьогодні методів біометричної ідентифікації середні значення FAR та FRR представлені в таблиці 1.2 та мають такий вигляд:

Таблиця 1.2 – Середні значення FAR та FRR

Метод розпізнавання	FAR	FRR
Відбиток пальця	0,001%	0,6%
Розпізнавання обличчя 2D	0,1%	2,5%
Розпізнавання обличчя 3D	0,0005%	0,001%
Райдужка ока	0,00001%	0,016%
Сітківка ока	0,0001%	0,4%
Малюнок вен	0,0008%	0,01 %

Але для створення ефективної системи контролю доступу FAR та FRR параметри недостатньо досконалі. Наприклад, складно уявити СКУД на основі аналізу ДНК, хоча при цьому методі автентифікації значення цих параметрів наближуються до нуля. Але час ідентифікації зростає, зростає вплив людського чинника, невиправдано зростають витрати на систему. Тому для якісного аналізу біометричної системи контролю доступу необхідно використовувати інші дані, які іноді можна отримати лише експериментально.

Насамперед, такі дані повинні включати можливість фальсифікації біометричних даних для ідентифікації в системі та способи підвищення рівня безпеки.

Крім того, стабільність біометричних факторів: їхня незмінність у часі та незалежність від умов навколишнього середовища. Як логічний наслідок – швидкість автентифікації, можливість швидкого отримання безконтактних біометричних даних для ідентифікації. І, звичайно, нижчі витрати на

впровадження біометричної системи управління доступом на основі розглянутого методу автентифікації та доступності компонентів.

Порівняння біометричних методів стійкості до фальсифікації даних [20 – 21].

Фальсифікація біометричних даних у будь-якому випадку є досить складним процесом, який часто вимагає спеціальної підготовки та технічної підтримки. Але якщо можна змоделювати відбиток пальця в домашніх умовах, то успішна підробка райдужної оболонки ще не відома. Для біометричних систем автентифікації на сітківці створити фальшивку просто неможливо (табл. 1.3).

Таблиця 1.3 – Порівняння біометричних методів стійкості до фальсифікації даних

Метод розпізнавання	Фальсифікація
Відбиток пальця	Можлива
Розпізнавання обличчя 2D	Можлива
Розпізнавання обличчя 3D	Проблемна
Райдужка ока	Безуспішна
Сітківка ока	Неможлива
Малюнок вен	Неможлива

Порівняння біометричних методів наскільки можна суворої автентифікації [22 – 23].

Підвищення рівня безпеки біометричної системи контролю доступу зазвичай досягається за допомогою програмних та апаратних методів. Наприклад, технологія «живий палець» для відбитків пальців, аналіз мимовільного трясіння очей. Щоб підвищити рівень безпеки, біометричний метод може бути одним із компонентів системи багатофакторної автентифікації (табл. 1.4).

Таблиця 1.4 – Порівняння біометричних методів по можливості суворої автентифікації

Метод розпізнавання	Сувора автентифікація (один фактор)
Відбиток пальця	Можлива
Розпізнавання обличчя 2D	Неможлива
Розпізнавання обличчя 3D	Неможлива
Райдужка ока	Можлива
Сітківка ока	Можлива
Малюнок вен	Можлива

Включення додаткових програм безпеки до програмно-апаратного комплексу, зазвичай, досить значно збільшує його вартість. Однак для деяких методів можлива сувора автентифікація на основі стандартних компонентів: використання декількох шаблонів для ідентифікації користувача (наприклад, вен).

Порівняння методів автентифікації щодо незмінності біометричних характеристик [24 – 25].

Постійні біометричні характеристики також є умовними: всі біометричні параметри можуть змінюватися в результаті медичної операції або травми. Але якщо звичайний домашній поріз, який може ускладнити перевірку користувача по відбитку пальця, є нормальною ситуацією, то операція, яка змінює малюнок райдужної оболонки, є рідкістю (табл. 1.5).

Таблиця 1.5 – Порівняння методів автентифікації щодо незмінності біометричних характеристик

Метод розпізнавання	Незмінність характеристики
Відбиток пальця	Низька
Розпізнавання обличчя 2D	Низька
Розпізнавання обличчя 3D	Висока
Райдужка ока	Висока
Сітківка ока	Середня
Малюнок вен	Середня

Порівняння чутливості до зовнішніх факторів [26 – 27].

Вплив параметрів навколишнього середовища на продуктивність систем контролю доступу залежить від алгоритмів та технологій роботи, що застосовуються виробником обладнання, і може значно відрізнятися навіть у межах одного біометричного методу (табл. 1.6).

Таблиця 1.6 – Порівняння за чутливістю до зовнішніх факторів

Метод розпізнавання	Чутливість до зовнішніх факторів
Відбиток пальця	Висока
Розпізнавання обличчя 2D	Висока
Розпізнавання обличчя 3D	Низька
Райдужка ока	Середня
Сітківка ока	Висока
Рисунок вен	Середня

Якщо ми порівняємо інші методи біометричної ідентифікації, найбільш чутливим буде розпізнавання обличчя в 2D: тут, наявність окулярів, капелюха, нової зачіски або бороди, що заросла, може стати критичним.

Системи, що використовують метод автентифікації сітківки, вимагають досить жорсткого положення ока щодо сканера, нерухомості користувача та фокусування самого ока.

Методи ідентифікації користувача, що ґрунтуються на малюнках вен і райдужних оболонках, відносно стабільні в роботі, якщо їх не використовувати в екстремальних умовах роботи (наприклад, безконтактна автентифікація на великій відстані під час «грибного» дощу).

Тривимірна ідентифікація особи є найменш чутливою до впливу зовнішніх факторів. Єдиний параметр, який може вплинути на роботу такого СКУДу – це надмірне освітлення.

Порівняємо біометричні методи за швидкістю автентифікації [28].

Швидкість автентифікації залежить від часу захоплення даних, розміру моделі та кількості ресурсів, виділених на її оброблення, а також від основних програмних алгоритмів, що використовуються для реалізації конкретного біометричного методу (табл. 1.7).

Таблиця 1.7 – Порівняння за швидкістю автентифікації

Метод розпізнавання	Швидкістю автентифікації
Відбиток пальця	Висока
Розпізнавання обличчя 2D	Середня
Розпізнавання обличчя 3D	Низька
Райдужка ока	Висока
Сітківка ока	Низька
Рисунок вен	Висока

Порівняння по можливості безконтактної автентифікації [29].

Безконтактна автентифікація пропонує багато переваг використання біометричних методів у системах фізичної безпеки в установах з високими гігієнічними та санітарними вимогами (медицина, харчова промисловість, науково-дослідні інститути та лабораторії).

Крім того, ідентифікація віддаленого об'єкта прискорює процес перевірки, що є важливим для великих систем контролю доступу з високою швидкістю потоку. Крім того, правоохоронні органи можуть використовувати безконтактну ідентифікацію з метою національної безпеки.

Особливо ефективні методи, які фіксують біометричні характеристики об'єкта на великій відстані та під час руху. З поширенням камер спостереження з високою якістю зображення, реалізація цього принципу стає все простіше (табл. 1.8).

Таблиця 1.8 – Порівняння по можливості безконтактної автентифікації

Метод розпізнавання	Безконтактна автентифікації під час руху
Відбиток пальця	Неможлива
Розпізнавання обличчя 2D	На великій відстані
Розпізнавання обличчя 3D	На середній відстані
Райдужка ока	На великій відстані
Сітківка ока	Неможлива
Рисунок вен	На малій відстані

Порівняння біометричних методів психологічного комфорту користувача [30].

Психологічний комфорт користувачів є досить актуальним показником при виборі системи безпеки. Якщо у випадку двовимірного розпізнавання обличчя або райдужної оболонки – це відбувається непомітно, сканування сітківки є досить неприємним процесом.

Порівняння за вартістю реалізації біометричних методів у СКУД [30].

Ціноутворення систем контролю доступу та обліку, залежно від методів біометричної ідентифікації, що використовуються, надзвичайно різне. Проте різниця може бути відчутною в рамках одного і того ж методу, залежно від призначення системи (функціональності), виробничих технологій, методів, які підвищують захист від несанкціонованого доступу тощо (табл. 1.9).

Таблиця 1.9 – Порівняння вартості реалізації біометричних методів в СКУД

Метод розпізнавання	Вартість
Відбиток пальця	Низька
Розпізнавання обличчя 2D	Середня
Розпізнавання обличчя 3D	Висока
Райдужка ока	Низька
Сітківка ока	Висока
Рисунок вен	Середня

Порівняємо біометричні методи за сукупністю факторів [29 – 30].

Звичайно, вибір методу біометричної автентифікації для системи, контроль доступу залежить головним чином від її вимог. Проте порівняння біометричних методів за сукупністю факторів наочно демонструє їх переваги загалом. Аналізуючи отримані результати, зважаючи на їх ефективність, надійність, швидкість та точність розпізнання, було вирішено більш детальніше вивчити можливість ідентифікації особи за відбитком пальця.

1.3 Сутність дактилоскопічного методу ідентифікації користувачів

Відповідно до проведеного аналізу метод автентифікації особи за відбитками пальців є оптимальним з точки зору точності автентифікації та вартості технічної реалізації системи контролю доступу, яка функціонувала б на основі такого методу. Однак, на саму точність автентифікації можуть впливати зовнішні та внутрішні фактори, зокрема, це стан поверхні шкіри на кінчиках пальців, травми, опіки, різного роду пошкодження, забруднення тощо, а також неможливість забезпечення однакової сили притиснення пальців до поверхні сканерів відбитків, неоднакова орієнтація положення пальців на поверхні сканера тощо [31]. Тому актуальним є удосконалення методів попередньої підготовки відсканованих рисунків відбитків пальців до наступного виявлення глобальних та локальних ознак таких рисунків при незмінності технічних параметрів сканерів відбитків пальців, оскільки вирішення другої задачі є значно дорожчим. Отже, необхідно провести аналіз методів покращення якості зображень рисунків відбитків пальців на попередніх етапах автентифікації особи та обґрунтувати вибір тих методів, які в перспективі дадуть найкращі результати.

Поширеною областю застосування методу автентифікації особи за відбитками пальців є дактилоскопія [32], що ґрунтується на припущенні про неповторність та незмінність впродовж життя людини рисунка відпечатків її

пальців. При цьому, попри широке практичне використання, таке припущення не має достатнього наукового обґрунтування, як і загальної теорії, яка однозначно і обґрунтовано підтверджувала це припущення. Однак, практичні дані, які підтверджували факт наявності однакових відбитків пальців у різних осіб, є відсутні або факт однаковості є суперечливим [33]. Тому метод автентифікації за відбитками вважається надійним, наприклад, в області криміналістики.

Для задачі автентифікації особи на рисунку відбитка виділяють типи ознак, які є індивідуальними і придатні для ідентифікації особи. Сьогодні, використовують два основні типи ознак, а саме локальні та глобальні [34].

Перший тип ознак можна побачити неозброєним оком, вони визначаються структурою папілярного рисунка. На цьому рисунку виділяють фрагмент, в якому зосереджені глобальні ознаки [34]. До інформативних ознак належать центр рисунка, дельта, параметри ліній, кількості ліній. Центром рисунка є точка, зосереджена максимально по середині самого рисунка або його фрагмента. Дельтою називають місце поділу або об'єднання складових папілярних ліній. До типів ліній відносять найбільші лінії рисунка, які можуть починатися у вигляді двох паралелей, розходитися і огинати область фрагмента [35].

Для класифікації рисунків використовують певні спільні для окремих груп рисунків параметри. Так, виділяють рисунки типу арки, петлі, дельти або дуги. Деякі приклади типів рисунків наведені на рис. 1.2 [35].

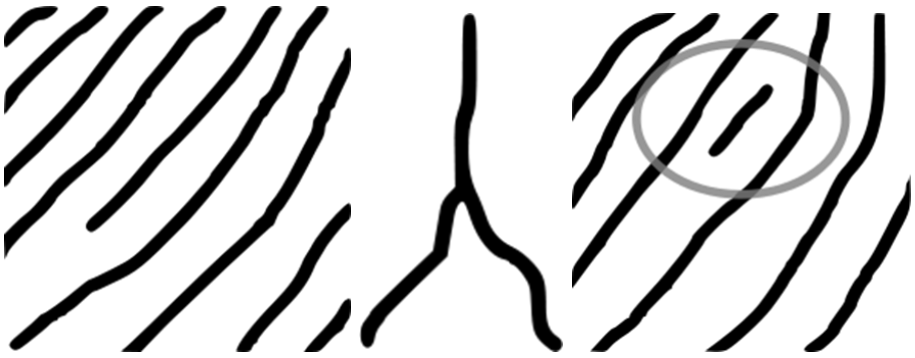
Іншим типом ознак папілярного рисунка є локальні ознаки, які ще називають мінуціями, або особливими точками. Вони є певними унікальними ознаками, індивідуальними для кожного окремого рисунка, що визначають ділянки зміни структури папілярних ліній. Сюди належать ознаки типу закінчення лінії, роздвоєння або розриву лінії, згину, орієнтація ліній, координати точок зміни у структурі ліній тощо. Деякі типи мінуцій наведені на рис. 1.3 [36].

а)

б)

в)

Рисунок 1.2 – Деякі типи папілярних рисунків: а) арка; б) петля; в) завитка



а) б) в)

Рисунок 1.3 – Типи мінуцій: а) закінчення; б) розгалуження; в) острівець

Часто на практиці стаються випадки, коли для різних людей глобальні

ознаки їх рисунків відпечатків пальців є подібними або однаковими [37 – 38]. Однак практично неможливою є ситуація однаковості і локальних ознак. Тому перші ознаки застосовують для поділу дактилоскопічної бази даних відбитків на класи, а автентифікація виконується на основі другого типу ознак в межах класу рисунка за глобальними ознаками [39 – 40].

Більш детальніше про порівняння відбитків пальців для ідентифікації особистості розглянемо в наступному розділі.

1.4 Дослідження недоліків та переваг алгоритмів порівняння відбитків пальців

У сучасній практиці для дактилоскопічної ідентифікації використовують такі алгоритми порівняння відбитків пальців [41 – 42]:

– кореляційне порівняння;

– порівняння за особливими точками;

– порівняння за візерунком;

– зіставлення за шаблоном;

– порівняння на основі графів.

Кореляційне порівняння [43 – 44]. Сутність даного методу можна описати наступним чином: отриманий за допомогою сканера відбиток пальця накладається на кожен стандарт з бази даних порядку черги. Потім, по пікселям зображень здійснюється прорахунок відмінностей між такими відбитками. Процес порівняння відбитка його пальця з існуючими еталонами повинен включати велику кількість ітерацій, оскільки положення пальця при скануванні фактично постійно різне. Тому на кожній ітерації зображення, яке отримане зі сканера, повертається під незначним кутом або трохи зміщується. Таким чином, здійснюється відстежування кореляції між відповідними пікселями, обчислена для різних вирівнювань зображень один щодо одного (наприклад, шляхом різних зміщень та обертань); за відповідним коефіцієнтом приймається рішення про ідентичність відбитків.

Порівняння за особливими точками – з використанням одного або декількох відбитків пальця отриманих зі сканера відбувається формування шаблону (карти), яка являє собою двомірну поверхнею, де виділені кінцеві точки та точки розгалуження.

Такий процес порівняння полягає в тому, що на відсканованому зображенні відбитка також виділяються особливі точки, складається тимчасова карта заданими точками та порівнюється з шаблоном за кількістю точок, що збіглися, приймається рішення по ідентичності відбитків. Результатом такого зіставлення, як правило, є набір ключових точок [45 – 46].

Головною перевагою такого алгоритму порівняння відбитків пальців за особливими точками є швидкість його роботи, оскільки у процесі ідентифікації основна частину виділяється на перебір стандартів у пошуку друку, ідентичного часовому.

Проте, набагато простіше і швидше порівняти кілька десятків окремих точок, ніж зображення. Тим більше, що в цьому випадку використовуються спеціальні алгоритми кореляційного порівняння. Вони враховують положення імовірних точок для обертання або зсуву тимчасової карти. І це дозволяє ще більше прискорити процес ідентифікації.

До переваг можна віднести те, що метод широко відомий і добре досліджений, використовується в додатках AFIS, а також підходить для множинного зіставлення. Завдяки даним перевагам, простій реалізації та швидкій роботі, алгоритми методів даного класу є найбільш поширеними у використанні.

Недоліками алгоритму є високі вимоги до якості зображення папілярного візерунка та розмірів чутливого датчика. Для коректної роботи, розширення зображення зі сканеру повинно бути близько 500 dpi (не менше 300 dpi).

Також слід враховувати, що люди, які не мають зовсім або мають невелику кількість ключових точок (особливий стан шкірного покриву) не можуть користуватися даною системою. Кількість ключових точок може бути обмежуючим фактором безпеки алгоритму.

Порівняння за візерунком [47 – 48]. В даному алгоритмі використовується безпосередньо особливості будови папілярного візерунка, який розташований на поверхні пальців. Отримане зі сканера зображення відбитка пальця, розбивається на безліч дрібних осередків, розмір яких залежить від необхідної точності). Розташування ліній у кожному осередку описується параметрами деякої синусоїдальної хвилі, тобто, задається початковий зсув фази, довжина хвилі та напрямок її поширення.

Спеціальний модуль розглядає папілярні лінії у квадратиках, потім кожну з них визначає рівнянням синусоїдальної хвилі, тобто встановлює початковий зсув фази, довжину хвилі та напрямок її поширення. Такі дані використовуються для ідентифікації: у базі даних еталонів зберігаються параметри всіх відрізків горбків у кожній області. Потім порівнюються параметри хвильових уявлень відповідних осередків еталонного зображення та зображення, отриманого при скануванні.

Головними перевагами розглянутого алгоритму є досить висока швидкість його роботи та низькі вимоги до якості одержуваного зображення. Проте, недоліком методу є його складність в реалізації та велика математична база.

Зіставлення за шаблоном [49 – 50].

В даному алгоритмі порівнюються не тільки окремі точки, але й аналізується загальна характеристика відбитка пальця, яка може включати певний відсоток додаткових даних, товщину ліній, їх кривизну або щільність.

Під час реєстрації алгоритм зіставлення шаблонів визначає наявність додаткових характеристик відбитка пальця. Невеликі ділянки відбитка пальця та відстань між ними витягуються з відбитка з метою максимально збільшити кількість унікальної інформації.

Найбільш значущими є ділянки навколо ключових точок та ділянки з невеликим радіусом вигину, а також основна структура та унікальні комбінації ліній.

Процес підтвердження починається із попереднього оброблення зображення відбитка пальця.

Зареєстроване зображення, зчитане з шаблону, зіставляється із зображенням відбитка, щоб визначити, наскільки шаблон співпадає із зображенням. Поріг, що описує найменше допустиме відхилення використовується при визначенні ступеня відповідності відбитка наявному шаблону.

Перевагами даного методу є сумісність з усіма відомими типами сканерів відбитків пальців, не зважаючи на вихідне розширення файлу, підходить для здійснення роботи з на пристроях з невеликим об’ємом обчислювальної здатності.

До недоліків слід віднести те, що даний метод не може використовувати базу даних AFIS (проте, може використовувати недооброблені зображення) і не пристосований для розпізнавання (для багатьох пошуків у базі даних).

Порівняння на основі графів.

У даному алгоритмі порівняння вихідне зображення відбитка перетворюється на зображення поля орієнтації папілярних ліній, на якому помітні області з однаковою орієнтацією ліній, тому можна провести межі між цими областями. Потім визначаються центри цих областей та формується граф.

1.5 Висновки та постановка задач дослідження

У даному розділі було проаналізовано теоретичні засади біометричних методів ідентифікації особи.

У даній роботі розглянуто поняття біометричної ідентифікації користувачів, її переваги та недоліки та особливості, сфери застосування, існуючі методи ідентифікації особистості із використанням її біометричних даних, детальніше розглянуто метод ідентифікації – дактилоскопію.

Для досягнення поставленої мети було поставлено такі задачі подальшого дослідження:

– удосконалити метод розпізнавання відбитку пальця за методом Собеля;

– розробити алгоритм роботи програмного додатку для ідентифікації

користувачів на основі удосконаленого методу розпізнавання відбитків пальців;

– обґрунтувати вибір мови та середовища програмування для додатку;

– спроектувати та розробити інтерфейс користувача додатку;

– розробити програмний засіб для підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії;

– обґрунтувати економічну доцільність програмного додатку.

Отже, виконання поставлених завдань дозволяє досягти основної мети роботи, а саме розробити та реалізувати програмний засіб для підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії.

2 РОЗРОБЛЕННЯ СИСТЕМИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІЗ ВИКОРИСТАННЯМ МЕТОДУ ДАКТИЛОСКОПІЇ

2.1 Удосконалення методу розпізнавання відбитку пальця

У першому розділі даної роботи було наведено та проаналізовано існуючі актуальні методи розпізнавання відбитків пальців, визначено їх особливості, переваги та недоліки. В ході аналізу було вирішено, що найбільш доцільним для застосування у даній роботі є метод порівняння по особливих точках. Проте, оскільки серед недоліків даного методу є високі вимоги до якості зображень, то для їх усунення (і в якості удосконалення даного методу) застосуємо оператор обробки зображень, за допомогою якого відбуватиметься покращення якості отриманого відбитку пальця.

Однією з головних цілей комп'ютерного зору для оброблення зображень є інтерпретація вмісту на зображенні. Для цього необхідно якісно відокремити фон від об'єктів. Сегментація поділяє зображення на складові чи об'єкти. Вона відокремлює об'єкт від фону, щоб можна було легко обробляти зображення та ідентифікувати його вміст.

Сегментація зображення – це процес розділення цифрового зображення на множину областей або наборів пікселів. Фактично, це поділ на різні об'єкти, які мають однакову текстуру або колір. Результатом сегментації є набір областей, що покривають всі зображення, і набір контурів, витягнутих із зображення. Всі пікселі з однієї області подібні до деяких характеристик, таких як колір, текстура або інтенсивність. Суміжні області відрізняються один від одного тими самими характеристиками. Різні підходи знаходження границь між областями базуються на неоднорідності рівнів інтенсивності яскравості. Таким чином, вибір методу сегментації зображення залежить від проблеми, яку необхідно вирішити [51].

Методи, засновані на областях, базуються на безперервності. Дані алгоритми ділять все зображення на підобласті залежно від деяких правил.

Наприклад, всі пікселі цієї групи повинні мати певне значення сірого кольору. Ці алгоритми покладаються на загальні шаблони інтенсивності значень кластерів сусідніх пікселів.

Порогова сегментація є найпростішим видом сегментації. На основі її області можуть бути класифіковані за базовим діапазоном значення, які залежать від інтенсивності пікселів зображення. Порогова обробка перетворює вхідне зображення на бінарне [52].

Методи сегментації, що ґрунтуються на виявленні областей, знаходять безпосередньо різкі зміни значень інтенсивності. Такі методи називаються граничними методами. Виявлення меж – фундаментальна проблема при аналізі зображень. Техніки виділення границь, зазвичай, використовують для знаходження неоднорідностей на напівтоновому зображенні. Виявлення розривів на напівтонному зображенні – найважливіший підхід виділення границь.

Межі об'єктів на зображенні значною мірою зменшують кількість даних, які необхідно обробити, і водночас зберігають важливу інформацію про об'єкти на зображенні, їх форму, розмір, кількість. Головною особливістю техніки виявлення границь є можливість отримати точну лінію з гарною орієнтацією. У літературі описано безліч алгоритмів, які дозволяють виявляти межі об'єктів, але немає опису, як оцінювати результати обробки. Результати оцінюються суто індивідуально та залежать від сфери їх застосування [53 – 54].

Виявлення меж – фундаментальний інструмент для сегментації зображення. Такі алгоритми перетворюють вхідне зображення на зображення з контурами об'єктів, переважно в сірих тонах. В обробці зображень, особливо в системах комп'ютерного зору, виділення контуру розглядають важливі зміни рівня яскравості на зображенні, фізичні та геометричні параметри об'єкта на сцені. Це фундаментальний процес, який описує в загальних рисах об'єкти, отримуючи тим самим деякі знання про зображення. Виявлення границь є найпопулярнішим підходом виявлення значних неоднорідностей.

Границя є місцевою зміною яскравості зображення. Вона, зазвичай, проходить по краю між двома областями. За допомогою меж можна отримати

базові знання про зображення. Функції їх отримання використовуються передовими алгоритмами комп'ютерного зору в таких галузях, як медична обробка зображень, біометрія тощо.

Виявлення границь – активна сфера досліджень, оскільки вона полегшує високорівневий аналіз зображень. На напівтонових зображеннях існує три види розривів: точка, лінія та границя. Для виявлення всіх трьох видів неоднорідностей можна використовувати просторові маски [55 – 56].

У технічній літературі наведено та описано велику кількість алгоритмів виділення контурів та кордонів. До них відносяться: оператор Робертса, Собеля, Превітта, Кірша, Робінсона, алгоритм Кані та LoG-алгоритм [57].

Проаналізувавши особливості кожного з операторів та враховуючи їх переваги, в даній роботі доцільно використати фільтр (оператор) Собеля [58].

Оператор Собеля здійснює вимірювання двовимірного просторового градієнта на зображенні та виявляє області з великим значенням цього параметра [59].

Ці області відповідають краям. Як правило, він використовується для оцінки модуля градієнта у кожній точці чорно-білого зображення.

Градієнт функції двох змінних для кожної точки зображення (якою є функція яскравості) – двомірний вектор, компонентами якого є похідні яскравості зображення по горизонталі та вертикалі. В кожній точці зображення градієнтний вектор орієнтований у напрямку найбільшого збільшення яскравості, його довжина відповідає величині зміни яскравості. Це означає, що результатом оператора Собеля у точці області постійної яскравості буде нульовий вектор, а в точці, що лежить на межі областей різної яскравості – вектор, перетинає кордон у напрямі збільшення яскравості.

Ідея методу Собеля полягає у накладенні на кожну точку зображення двох масок обертання. Ці маски є двома ортогональними матрицями, розмірністю 3×3 (рис. 2.1).

-1	0	+1
-2	0	+2
-1	0	+1

+1	+2	+1
0	0	0
-1	-2	-1

+1	0	-1
+2	0	-2
+1	0	-1

-1	-2	-1
0	0	0
+1	+2	+1

Рисунок 2.1 – Маски Собеля (вертикальна, горизонтальна) (за [60])

Для вирішення питання інваріантності щодо повороту використовуються так звані діагональні маски, призначені виявлення розривів у діагональних напрямах (рис. 2.2).

0	+1	+2
-1	0	+1
-2	-1	-0

2	+1	0
+1	0	-1
0	-1	-2

Рисунок 2.2 – Маски Собеля (діагональні) (за [60])

Ці маски виявляють межі, розташовані вертикально та горизонтально на зображенні. При роздільному накладанні цих масок зображення можна отримати оцінку градієнта в кожному з напрямів G_x, G_y [61].

Кінцеве значення градієнта знаходиться формулі:

$$G = \sqrt{G_x^2 + G_y^2}.$$

Отже, використовуючи для розпізнавання відбитку пальця метод порівняння за особливими точками у поєднанні з оператором Собеля, алгоритм роботи додатку *з* оброблення відбитка здійснюватиметься за такими кроками:

Крок 1. Завантаження даних.

Крок 2. Перевірка відповідності отриманих даних заданим умовам. Якщо дані коректні – перехід до кроку 3. Якщо дані не задовольняють умовам – повернення до кроку 1 (повторне завантаження).

Крок 3. Нормалізація зображення.

Крок 4. Побудова операційної та частотної матриць.

Крок 5. Бінаризація зображення.

Крок 6. Візуалізація результатів оброблення.

Структурну схему даного алгоритму роботи представлено на рис. 2.3.

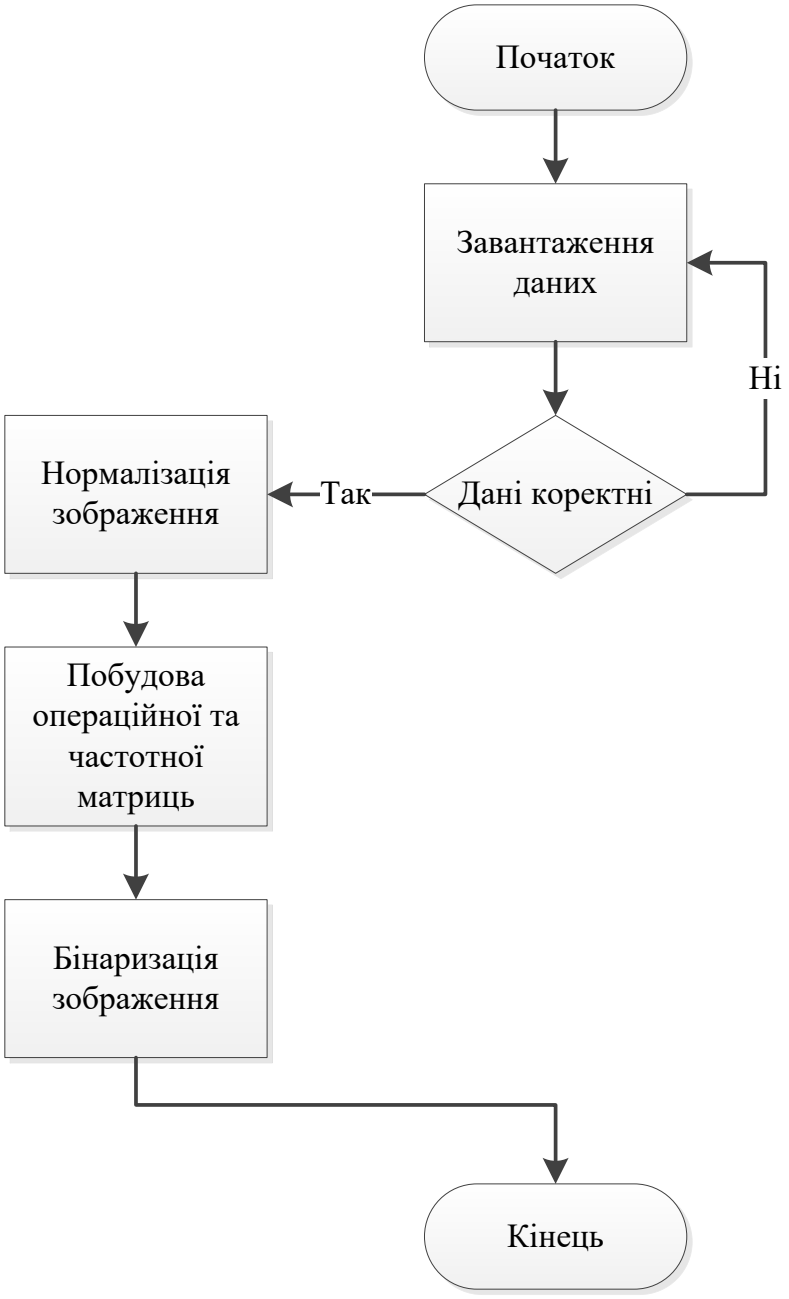


Рисунок 2.3 – Алгоритм опрацювання рисунків відбитків пальців

Таким чином, на основі запропонованого автором алгоритму роботи системи ідентифікації користувачів із використанням методу дактилоскопії, в наступному розділі буде здійснено програмну реалізація та представлення результатів її роботи.

2.2 Розроблення алгоритму роботи системи для ідентифікації користувача

У ході подальшої роботи розробимо систему контролю захищеного доступу, що ґрунтується на застосуванні біометричної ідентифікації, а саме, на розпізнаванні користувачів за відбитками пальців.

Автором запропоновано організувати таку систему контролю доступу, що складається з таких етапів (рис. 2.4):

– етап автентифікації;

– етап оброблення відбитків пальців;

– етап представлення результатів.

Рисунок 2.4 – Загальна структура системи контролю доступу на основі біометричної ідентифікації

Структуру інформаційної бази системи автентифікації на основі відбитку пальця можна представити у вигляді схеми, зображеної на рис. 2.5. Варто відзначити, що дані логіну та зразки відбитків пальців авторизованих користувачів зберігатимуться в окремій базі даних (рис. 2.5).

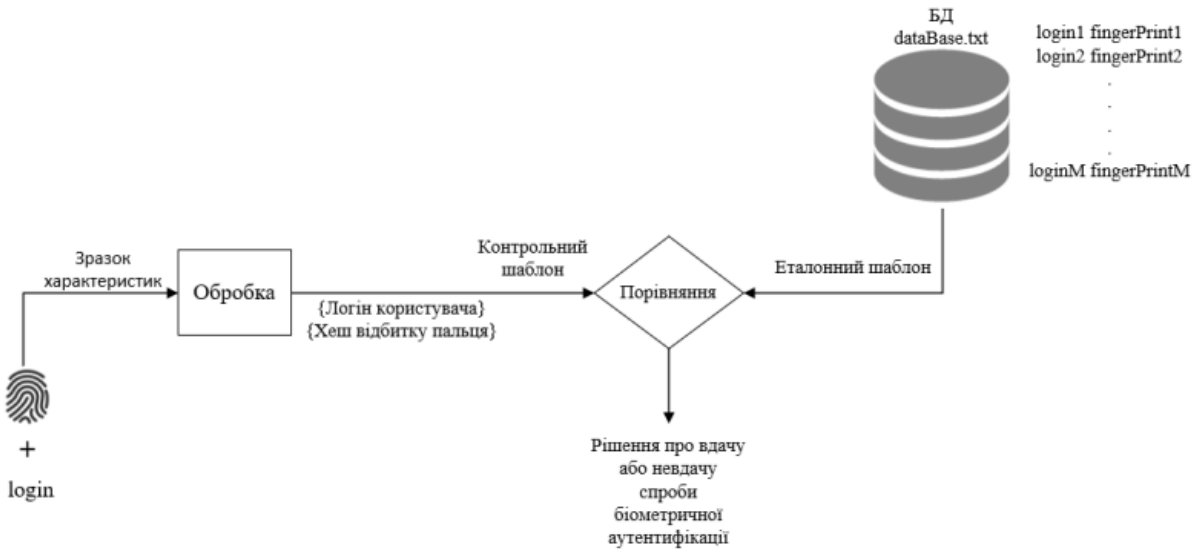


Рисунок 2.5 – Інформаційна структура системи

Ще однією складовою розроблюваної системи контролю доступу на основі біометричної ідентифікації є її функціональна структура, тобто набір певних операцій та зв’язків, які циклічно повторюються, та направлені на кінцевий результат роботи системи. Така структура представлена на рис. 2.6.

Рисунок 2.6 – Функціональна структура системи контролю доступу

Представимо удосконалений алгоритм роботи системи на рис. 2.7.

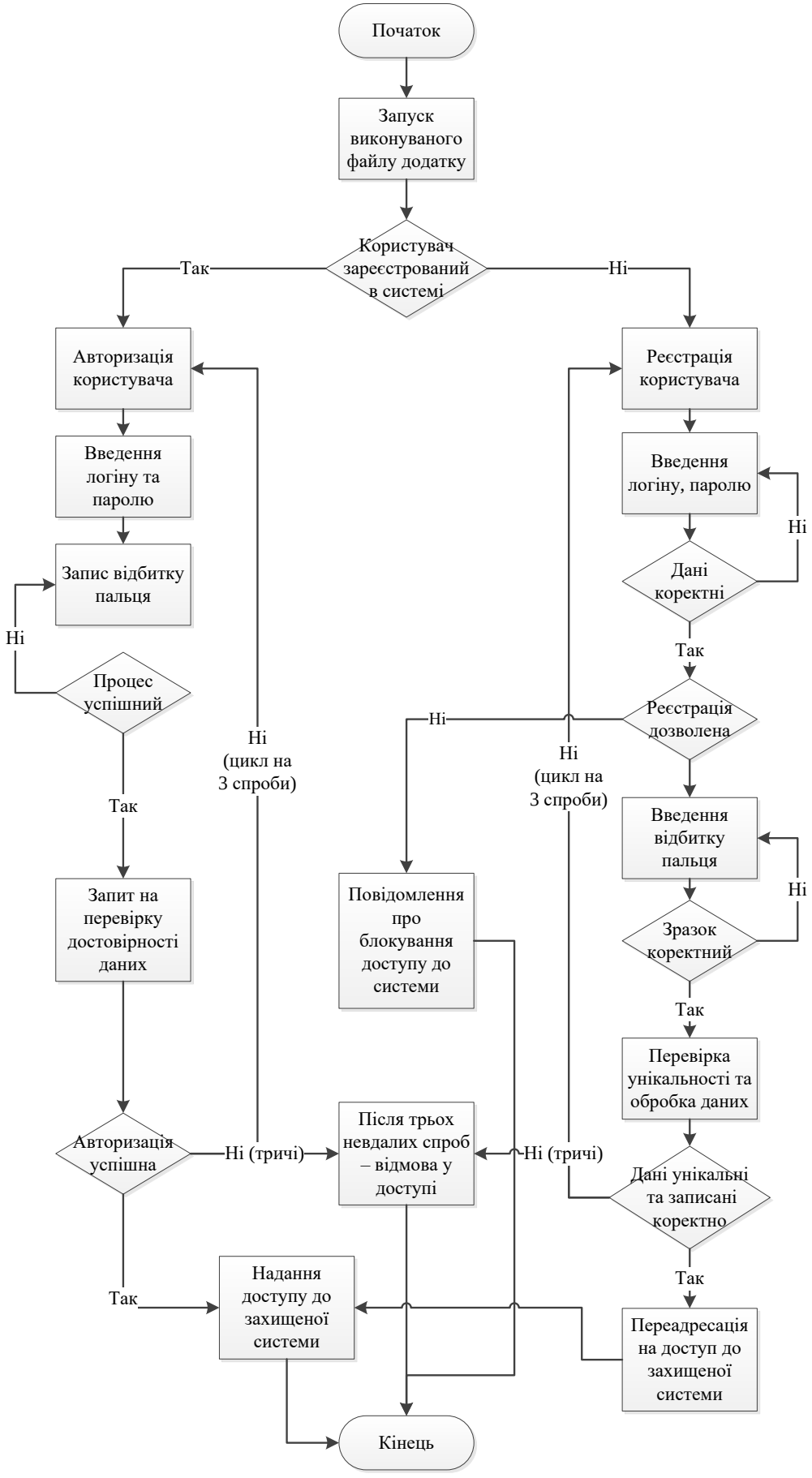


Рисунок 2.7 – Алгоритм роботи додатку

Розглянемо покроково наведений вище алгоритм.

Крок 1. Запуск робочого файлу додатку.

Крок 2. Реєстрація користувача в системі.

Крок 2.1 Користувач натискає кнопку «Реєстрація».

Крок 2.2 У полі для вводу логіну вводить свій логін та пароль. Даний параметр повинен бути унікальним у межах даної системи.

Крок 2.3. У відповідному полі слід додати біометричний ідентифікатор користувача – відбиток пальця.

Крок 2.4. Користувач натискає кнопку «Продовжити».

Крок 2.5. Система перевіряє наявність вказаного логіну у базі даних доступних користувачів. Якщо введений логін рахується у базі даних як дозволений до реєстрації, користувач може переходити до наступного кроку.

У випадку, якщо логін невідомий системі – користувач отримує відмову у доступі до системи (це означає, що особа з такими даними не зареєстрована як користувач з дозвільними правами до програмного забезпечення власника системи).

Крок 2.6. Система перевіряє унікальність введених даних, заносить їх до бази даних.

Крок 2.7. У випадку успішної реєстрації, користувач отримує відповідне повідомлення. У випадку, якщо дані некоректні та не пройшли перевірку в системі, користувачеві повідомляється про невдалу спробу реєстрації.

Крок 3. Авторизація користувача в системі.

Крок 3.1 Користувач натискає кнопку «Увійти».

Крок 3.2 У полі для вводу логіну вводить свій логін та пароль.

Крок 3.3 У відповідному полі слід додати біометричний ідентифікатор користувача – відбиток пальця.

Крок 3.4 Користувач натискає кнопку «Продовжити».

Крок 3.5 Система перевіряє відповідність введених даних, порівнює їх із наявними у базі даних.

Важливо, що логін та відбиток пальця кожного користувача були взаємопов’язані і відповідали одному і тому ж користувачеві.

Крок 3.6. У випадку успішної авторизації – користувач отримує відповідне повідомлення. У випадку, якщо дані некоректні та не пройшли перевірку у системі – користувачеві повідомляється про невдалу спробу реєстрації.

Важливо, що автором передбачено лише можливість трьох спроб авторизації. Після кожної невдалої спроби авторизації, користувач отримає відповідне повідомлення, де зазначається кількість можливих спроб, що залишилися. У випадку трьох невдалих спроби авторизації – додаток самостійно закривається, доступ користувача до авторизації в системі заблокований.

Крок 4. У разі успішного здійснення процесу реєстрації / авторизації користувачеві надається доступ до захищеної системи.

Таким чином, ґрунтуючись на розробленій автором структурі системи контролю доступу та алгоритмі її роботи, в наступному підрозділі буде запропоновано удосконалення для методу розпізнавання за відбитками пальців та реалізовано практично отримані результати роботи.

2.3 Обґрунтування вибору мови та засобу програмування

Ураховуючи особливості поставленої задачі, для програмної реалізації було обрано мову об’єктно-орієнтованого програмування C#. Мова C# є продуктом Microsoft і основним направленням даної мови є продукти для операційної системи сімейства Windows, як для стаціонарних комп’ютерів, так і для мобільних пристроїв [62].

C# – об’єктно-орієнтована мова програмування для платформи .NET. Мова заснована на строгій компонентній архітектурі і реалізує передові механізми забезпечення безпеки коду.

Microsoft .NET – програмна технологія, запропонована фірмою Microsoft як платформа для створення як звичайних програм, так і веб - додатків. Багато в чому є продовженням ідей та принципів, покладених в технологію Java. Одною

з ідей .NET є сумісність служб, написаних різними мовами. Хоча ця можливість рекламується Microsoft як перевага .NET, платформа Java має таку саму можливість [63].

Кожна бібліотека (збірка) в .NET має свідчення про свою версію, що дозволяє усунути можливі конфлікти між різними версіями збірок.

Як і технологія Java, середовище розробки .NET створює байт-код, призначений для виконання віртуальною машиною. Вхідна мова цієї машини в .NET називається CIL (Common Intermediate Language), також відома як MSIL (Microsoft Intermediate Language), або просто IL. Застосування байт-коду дозволяє отримати крос-платформність на рівні скомпільованого проекту (в термінах .NET: збірка), а не на рівні сирцевого тексту, як, наприклад, у C. Перед запуском збірки в середовищі виконання (CLR) байт-код перетворюється вбудованим в середовище JIT-компілятором (just in time, компіляція на льоту) в машинні коди цільового процесора. [64 – 65]

C# було створено спеціально для платформи .NET. У той же час на C# повністю написана і сама платформа .NET. C# розроблялася як мова програмування прикладного рівня для CLR, отже, її функціонал залежить, насамперед, від можливостей самої CLR. CLR надає C#, як і всім іншим .NET-орієнтованим мовам, багато можливостей, яких позбавлені «класичні» мови програмування (C++, Java, Pascal, Delphy та ін.).

C# – це повнофункціональна об’єктно-орієнтована мова, що підтримує всі три «стовпи» об’єктно-орієнтованого програмування: інкапсуляцію, наслідування і наслідування (рис. 2.8).

Інкапсуляція – це механізм програмування, який об’єднує разом код і дані, якими він маніпулює, виключаючи як втручання ззовні, так і неправильне використання даних. У об’єктно-орієнтованій мові дані і код можуть бути об’єднані в абсолютно автономний чорний ящик. Усередині такого ящика знаходяться всі необхідні дані і код. Коли код і дані зв’язуються разом подібним чином, створюється об’єкт. Іншими словами, об’єкт – це елемент, що підтримує інкапсуляцію. Наслідування являє собою процес, в ході якого один

об’єкт набуває властивостей іншого об’єкта. Це дуже важливий процес, оскільки він забезпечує принцип ієрархічної класифікації. Велика частина знань піддається систематизації завдяки ієрархічній класифікації по низхідній.

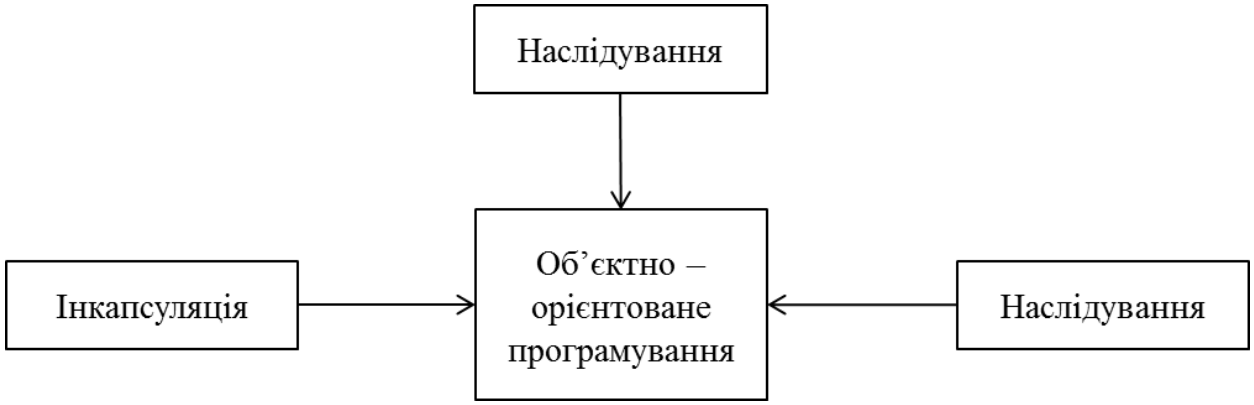


Рисунок 2.8 — Три «стовпи» об’єктно-орієнтованого програмування (за [66])

Якщо не користуватися ієрархіями, то для кожного об’єкта довелося б явно визначати всі його властивості. А якщо скористатися наслідуванням, то досить визначити лише ті властивості, які роблять об’єкт особливим в його класі. Він може так само наслідувати загальні властивості свого батька. Отже, завдяки механізму наслідування один об’єкт стає окремим екземпляром більш загального класу.

Поліморфізм, що з грецької означає «безліч форм», – це властивість, що дозволяє одному інтерфейсу отримувати доступ до загального класу дій. Простим прикладом поліморфізму може служити кермо автомашини, яке виконує одні й ті ж функції своєрідного інтерфейсу незалежно від виду застосовуваного механізму управління автомобілем. У більш загальному сенсі поняття поліморфізму нерідко виражається наступним чином: «один інтерфейс – безліч методів». Це означає, що для групи взаємопов’язаних дій можна розробити загальний інтерфейс.

Поліморфізм допомагає спростити програму, дозволяючи використовувати один і той самий інтерфейс для опису загального класу дій. Обрати конкретну дію (тобто метод) у кожному окремому випадку – це завдання компілятора. Програмісту не потрібно робити це самому.

Мова C# розроблялася «з нуля» й увібрала в себе багато корисних

властивостей таких мов, як C++, Java, Visual Basic, а також Pascal. Delphy та ін. При цьому необхідність зворотної сумісності з попередніми версіями відсутня, що дозволило мові C# уникнути багатьох негативних сторін своїх попередників.

Перевагою цієї мови програмування є те, що вона об’єднує переваги інших поширених мов програмування і має ряд власних особливостей [67]:

– підтримка інкапсуляції, наслідування і поліморфізму;

– підтримка компонентів та чітка типізація змінних;

– використання «збирання сміття» та автоматична ініціалізація змінних;

– використання оброблення виключень та можливість перевантаження операторів.

Мова має строгу статичну типізацію, підтримує вказівники на функції-члени класів, атрибути, події, властивості, винятки, коментарі у форматі XML.

Процес створення програми включає кілька етапів:

– написання програми на мові програмування C#.

– перетворення програми за допомогою компілятора в виконуваний файл (наприклад, myProgram.exe).

– часто комп'ютер виявляє в програмі помилки і повідомляє про це. Тоді необхідно виправити програму і знову спробувати виконати етап 2.

– запуск програми (часто через всілякі логічні помилки програма може виявитися непрацездатною. У цьому випадку необхідно переглянути і виправити її, а потім повторити етапи 1 – 4).

Отже, проаналізувавши всі переваги мови C#, можна зробити висновок, що дана мова найкраще підійде для написання програми для реалізації підвищення достовірності голосової ідентифікації користувача у web-додатку за допомогою поєднання з клавіатурним почерком на основі нейромережі, оскільки ця мова програмування має перелік переваг, яких немає у інших високорівневих мовах програмування, які є попередниками мови C#.

Для створення програмного засобу у магістерській роботі використано

інтегроване середовище розроблення Microsoft Visual Studio 2017 [68]. Microsoft Visual Studio – серія продуктів фірми Майкрософт, які включають інтегроване середовище розроблення програмного забезпечення та низку інших інструментальних засобів.

Ці продукти дозволяють розробляти як консольні програми, так і програми з графічним інтерфейсом, у тому числі з підтримкою технології Windows Forms, а також веб-сайти, веб-застосунки, веб-служби як в рідному, так і в керованому кодах для всіх платформ, що підтримуються Microsoft Windows, Windows Mobile, Windows Phone, Windows CE, .NET Framework, .NET Compact Framework та Microsoft Silverlight. Visual Studio включає один або декілька з наступних компонентів:

– Visual Basic .NET; Visual C++;

– Visual C#;

– Visual Studio Debugger.

Visual Studio 2017 являє собою універсальний засіб для фахівців з розробки і проектування, що підтримує більшість платформ розробки, в тому числі Windows і Windows Server, хмарне і веб-середовище, Office і SharePoint і гарантує 100% коректність кінцевого коду.

Зручності написання програм досягаються за допомогою таких чинників [69]:

– при помилці в коді текст буде підкреслено;

– присутній IntelliSense 4 – це помічник, який допомагає програмісту писати код (при його використання кількість помилок сильно зменшується) – його можна відкрити натиснувши Ctrl + Пробіл;

– можливості використання snippets;

– різних додаткових панелей.

Таким чином, обрані мова і середовище програмування дозволяють, завдяки своєму функціоналу, реалізувати поставлені задачі згідно розроблених алгоритмів та функцій роботи системи ідентифікації користувачів із використанням методу дактилоскопії.

2.4 Висновки до розділу

У даному розділі було розроблено систему ідентифікації користувачів із використанням методу дактилоскопії. Автором магістерської роботи запропоновано організувати таку систему контролю доступу, що складається з таких етапів: автентифікації, оброблення відбитків пальців, представлення результатів.

У ході аналізу методів розпізнавання відбитків пальців було вирішено, що найбільш доцільним для застосування у даній роботі є метод порівняння по особливих точках. Проте, оскільки серед недоліків даного методу є високі вимоги до якості зображень, то для їх усунення (і в якості удосконалення даного методу) було доведено доцільність застосування оператору Собеля для оброблення зображень, за допомогою якого стає можливим покращення якості отриманого відбитку пальця.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ ДОДАТКУ КОМПЛЕКСНОЇ АВТЕНТИФІКАЦІЇ ЗА БІОМЕТРИЧНИМИ ДАНИМИ

3.1 Проектування графічного користувацького інтерфейсу

Інтерфейс користувача – це інтерфейсна програма, з якою користувач взаємодіє для використання програмного забезпечення. Користувач може маніпулювати програмним та апаратним забезпеченням і керувати ним за допомогою інтерфейсу користувача. Сьогодні користувацький інтерфейс зустрічається майже у всіх місцях, де є цифрові технології, включаючи комп'ютери, мобільні телефони, автомобілі, музичні плеєри, літаки, кораблі тощо.

Інтерфейс користувача є частиною програмного забезпечення і спроектовано його таким чином, щоб забезпечити розуміння користувачем програмного забезпечення. Інтерфейс користувача забезпечує фундаментальну платформу для взаємодії людини з комп'ютером.

Інтерфейс користувача може бути графічним, текстовим та аудіо-відео, залежно від базової апаратної та програмної комбінації. Інтерфейс користувача може бути апаратним або програмним або їх комбінацією.

Програмне забезпечення стає більш популярним, якщо його інтерфейс користувача:

– привабливий;

– простий у використанні;

– зрозумілий;

– послідовний.

Інтерфейс загалом можна поділити на дві категорії:

– інтерфейс командного рядка;

– графічний інтерфейс користувача.

Детальніше розглянемо графічний інтерфейс користувача.

Графічний інтерфейс користувача надає користувачеві графічні засоби взаємодії із системою. GUI може бути комбінацією як апаратного, і

програмного забезпечення. Використовуючи GUI, користувач інтерпретує програмне забезпечення.

Як правило, GUI більш ресурсомісткий, ніж CLI. За допомогою передових технологій програмісти та дизайнери створюють складні графічні інтерфейси, які працюють із більшою ефективністю, точністю та швидкістю.

GUI програми містить один або кілька з перерахованих елементів GUI.

Вікно програми – у більшості вікон програми використовуються конструкції, що надаються операційними системами, але багато хто використовує власні вікна, створені замовником, для зберігання вмісту програми.

Діалогове вікно – це дочірнє вікно, яке містить повідомлення для користувача та запит на виконання будь-яких дій. Наприклад: програма генерує діалог, щоб отримати від користувача підтвердження видалення файлу.

Text-Box – надає користувачеві область для введення та введення текстових даних.

Кнопки – вони імітують реальні кнопки та використовуються для надсилання вхідних даних до програмного забезпечення.

Прапорець – функції, аналогічні списку. Коли вибрано опцію, поле позначається як зазначене. Можна вибрати кілька параметрів, наведених прапорцями.

Список – виберіть список доступних елементів. Можна вибрати більше одного елемента.

Існує кілька інструментів, за допомогою яких дизайнери можуть створювати весь графічний інтерфейс одним клацанням миші. Деякі інструменти можуть бути вбудовані у програмне середовище (IDE).

Інструменти реалізації GUI надають потужний масив елементів керування GUI. Для налаштування програмного забезпечення дизайнери можуть змінити код відповідно.

Існують різні сегменти інструментів із графічним інтерфейсом залежно від їх використання та платформи.

Далів розділі більш детальніше розглянемо особливості розробки інтерфейсу діалогових вікон для розроблюваного додатку біометричної ідентифікації.

Основним діалоговим вікном для користувача – є вікно авторизації (реєстрації) в системі. В такому вікні важливо обов’язково розмістити кнопки «Вхід», «Реєстрація», «Продовжити», поля для введення логіну та зразку відбитку пальця (рис. 3.1).

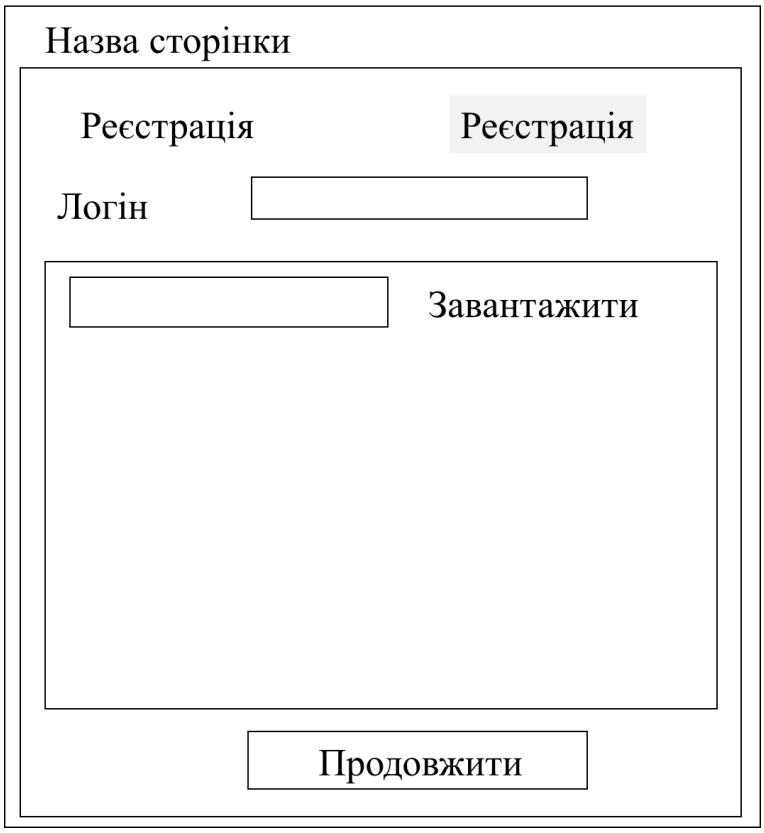


Рисунок 3.1 – Проектування вигляду головного вікна додатку

Таке діалогове вікно повинне бути максимально простим та зрозумілим для користувача. Кнопки реєстрації та авторизації повинні певним чином виокремлюватись при здійснення однієї із операцій (наприклад, виділятись іншим кольором).

Наступне діалогове вікно – це головне вікно додатку авторизованого користувача. У ньому повинні бути розташовані кнопка, яка може відобразити інформацію про систему, кнопка виходу, поле з логіном користувача та основна робоча область.

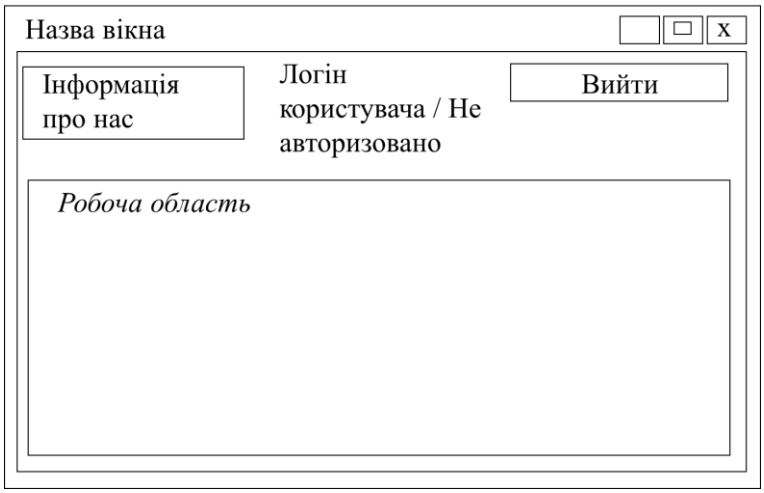


Рисунок 3.2 – Проектування вигляду вікна для роботи в системі

Відповідно, обов’язковим під час розроблення додатку є інтерфейс типових діалогових вікон, які виводять користувачеві основну інформацію від системи (повідомлення про коректність файлів, результати реєстрації, авторизації і т. п.) (рис. 3.3).

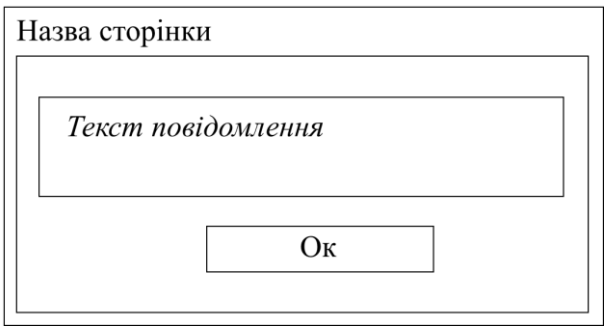


Рисунок 3.3 – Проектування вигляду діалогового вікна

Таким чином, у роботі буде розроблятися графічний інтерфейс користувача за спроектованим зразком. Основною вимогою до розроблення такого інтерфейсу є його зрозумілість та зручність під час експлуатації додатку.

3.2 Програмна реалізація додатку

Під час виконання магістерської дипломної роботи було розроблено алгоритм підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії. Проаналізувавши особливості кожного з операторів та враховуючи їх переваги, в даній роботі доцільно використати фільтр (оператор) Собеля. Наступним кроком виконання роботи є практична програмна реалізація розроблюваного додатку. Враховуючи особливості поставленої задачі, для програмної реалізації було обрано мову об'єктно – орієнтованого програмування C# та середовище Visual Studio.

Розглянемо послідовно окремі фрагменти кодової послідовності програмної реалізації додатку для біометричної ідентифікації користувачів.

Бібліотеки, що використовуються для програмної реалізації додатку:

```
using FaceDetectionAndRecognition.Context;
using FaceDetectionAndRecognition.Models;
using Microsoft.Win32;
using Newtonsoft.Json;
using PatternRecognition.FingerprintRecognition.Core;
using PatternRecognition.FingerprintRecognition.FeatureExtractors;
using PatternRecognition.FingerprintRecognition.Matchers;
using SpeechEyeRecognize;
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Text;
using System.Timers;
using System.Windows;
using System.Windows.Media;
using System.Windows.Media.Imaging;
```

Клас, що спрямований на реалізацію створення та функціональності поля для вводу логіну користувача, є таким:

```
public partial class Login : Window, INotifyPropertyChanged
  {
    public Login()
    {
```

```
            InitializeComponent();
        }
        public string score;
        public string qry;
        public string temp;
        private RecognizeContext _context = new RecognizeContext();
        private string ResourceImage = $"{
Path.GetDirectoryName(AppDomain.CurrentDomain.BaseDirectory)}/ResourceImage";
```

Практична реалізація функціоналу для запиту відбитка пальця під час запуску процесу авторизації / реєстрації користувача.

```
private string RegisterFingerPrint(string personName)
    {
        var extension = Path.GetExtension(pathToFile.Text);
        var newFileName = $"{Guid.NewGuid()}{extension}";
        var resPath = $"{ResourceImage}\\{newFileName}";
        var encoder = new PngBitmapEncoder();
       encoder.Frames.Add(BitmapFrame.Create((BitmapSource)fingerPrintImage.Source));
        using (FileStream stream = new FileStream(resPath, FileMode.Create))
            encoder.Save(stream);
        return newFileName;
    }
```

Практичне розроблення функціоналу кнопки «Реєстрація»:

```
private void Button_Click_1(object sender, RoutedEventArgs e)
    {
        if (type != Type.Registration)
        {
            LoginVoid();
        }
        else
        {
            RegistrationVoid();
        }
    }
```

Розглянемо фрагмент програмного коду для виведення повідомлення щодо невдалої спроби авторизації / реєстрації:

```
private void RegistrationVoid()
    {
        try
        {
            if (!VerifyData())
            {
                MessageBox.Show("Невдала спроба реєстрації");
                return;
            }
            var fileName = RegisterFingerPrint(UserName.Text);

            var user = new User()
            {
                UserName = UserName.Text,
                FingerPrintName = fileName,
            };
            var users = GetUsers();

            if (users == null)
            {
                users = new List<User>() { user };
            }
            else
            {
                users.Add(user);
            }
```

Виведення повідомлення про успішну та невдалу спробу реєстрації користувача:

```
MessageBox.Show("Успішно зареєстровано нового користувача");
            w.Close();
        }
        catch (Exception exception)
        {
            Console.WriteLine(exception);
            MessageBox.Show("Невдала спроба реєстрації");
        }
    }
```

Програмна реалізація функціоналу процесу авторизації користувача, звернення до бази даних:

```
private void LoginVoid()
    {
```

```
            if (!VerifyData())
               return;
            var user = GetUsers().FirstOrDefault(x => x.UserName == UserName.Text);
```

Проілюструємо успішну авторизацію користувача таким уривком програмного коду:

```
         if (user == null)
               MessageBox.Show("Кориистувача не було знайдено");
            var score = Convert.ToDecimal(CompareFingerPrint(user));
            if (score > 60)
            {
               var w = Application.Current.Windows[0];
               w.Hide();
```

Якщо авторизація користувача не здійснена:

```
               MessageBox.Show("Спроба входу була вдалою!");
               CommonPage commonpage = new CommonPage();
               commonpage.AuthUserName.Content = user.UserName;
               commonpage.Login.Visibility = Visibility.Hidden;
               commonpage.Exit.Visibility = Visibility.Visible;
               commonpage.ShowDialog();
               captureTimer = null;
               active = false;
               enableAutoNavigate = false;
               w.Close();
            }
            else
            {
               MessageBox.Show("Спроба входу була не вдалою!");
            }
         }
```

Фрагмент оброблення відбитку пальця:

```
      private string CompareFingerPrint(User user)
         {
            Change_ResolutionByPath(Path.Combine(ResourceImage, user.FingerPrintName));
            var tempFile = SaveToTempDir();
            Change_ResolutionByPath(tempFile);
            var fingerprintImg1 = ImageLoader.LoadImage(Path.Combine(ResourceImage,
user.FingerPrintName));
            var fingerprintImg2 = ImageLoader.LoadImage(tempFile);
```

Збереження результатів авторизації:

```
private string SaveToTempDir()
      {
         var path = Path.GetTempFileName();
         var encoder = new PngBitmapEncoder();

encoder.Frames.Add(BitmapFrame.Create((BitmapSource)fingerPrintImage.Source));
         using (FileStream stream = new FileStream(path, FileMode.Create))
            encoder.Save(stream);
         return path;
```

Перевірка повноти введених данх для авторизації / реєстрації:

```
private bool VerifyData()
      {
         if (String.IsNullOrEmpty(UserName.Text))
         {
            MessageBox.Show("Введіть логін");
            return false;
         }
         if (fingerPrintImage.Source == null)
         {
            MessageBox.Show("Необхідно прикріпити зразок відбитка пальця");
            return false;
         }
         return true;
      }
```

Практичне розроблення функціоналу кнопки «Авторизація»:

```
private void Button_Click(object sender, RoutedEventArgs e)
      {
         LoginBtn.Background = new SolidColorBrush(Colors.LightGray);
         RegButton.Background = new SolidColorBrush(Colors.White);

         type = Type.Login;
      }
```

Функціонал кнопки «Завантажити» зразок відбитку пальця:

```
private void Button_Click_3(object sender, RoutedEventArgs e)
      {
         OpenFileDialog dlg = new OpenFileDialog();
         //   dlg.InitialDirectory = "c:\\";
```

```
        //   dlg.Filter = "Image files (*.jpg)|*.jpg|All Files (*.*)|*.*";
        dlg.RestoreDirectory = true;
        if (dlg.ShowDialog() == true)
        {
            string selectedFileName = dlg.FileName;
            pathToFile.Text = selectedFileName;
            BitmapImage bitmap = new BitmapImage();
            bitmap.BeginInit();
            bitmap.UriSource = new Uri(selectedFileName);
            bitmap.EndInit();
            fingerPrintImage.Source = bitmap;
        }
    }
```

Таким чином, із використанням обраних програмних засобів та розробленого і удосконаленого алгоритму, було реалізовано додаток для підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії.

3.3 Реалізація користувацького інтерфейсу

Під час реалізації користувацького інтерфейсу використовувалися спроектовані автором магістерської роботи зразки діалогових вікон.

Розглянемо покроково діалогові вікна програми, що описують роботу з додатком.

Після запуску виконуваного файлу додатку, відкривається головне діалогове вікно програми. У верхній частині даного вікна знаходить два розділи «Вхід» (авторизація користувача) та «Реєстрація» (якщо користувач здійснює роботу із системою вперше).

Обравши вкладку «Реєстрація», далі користувачеві необхідно заповнити відповідне поле логіну, паролю та завантажити зразок відбитку пальця. Доданий зразок буде відображатися у полі нижче.

Після заповнення необхідних полів, користувачеві необхідно натиснути кнопку «Продовжити» для подальшої роботи з додатком. Натиснення даної кнопки автоматично запускає перевірку системою нового користувача.

Якщо логін користувача відомий системі – відбувається подальша перевірка. Якщо логін не зареєстрований у базі даних системи – користувач

отримує відмову доступу до системи.

Далі, у першу чергу перевіряється, чи коректно заповнено всі поля, далі відбувається звернення до бази даних системи, де перевіряється:

– Логін та пароль (який повинен бути унікальним для кожного користувача у межах даної програми);

– відбиток пальця (який, відповідно, також повинен бути унікальним і належати лише одному логіну.

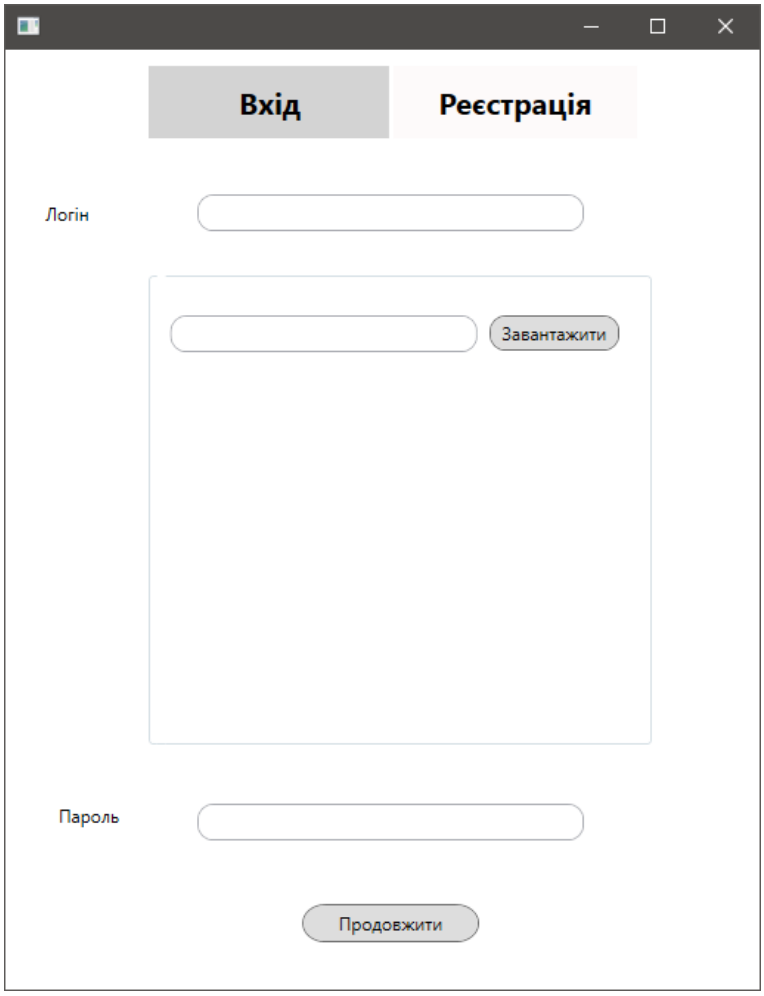


Рисунок 3.4 – Вигляд головного діалогового вікна додатку

Зразок коректно заповненого діалогового вікна розглянемо на рис. 3.5.

Після перевірки системою введених користувачем даних, відкриваються відповідні повідомлення.

У випадку, якщо логін та відбиток пальця введено коректно та є унікальними, користувач отримує повідомлення про успішну реєстрацію (рис. 3.6).

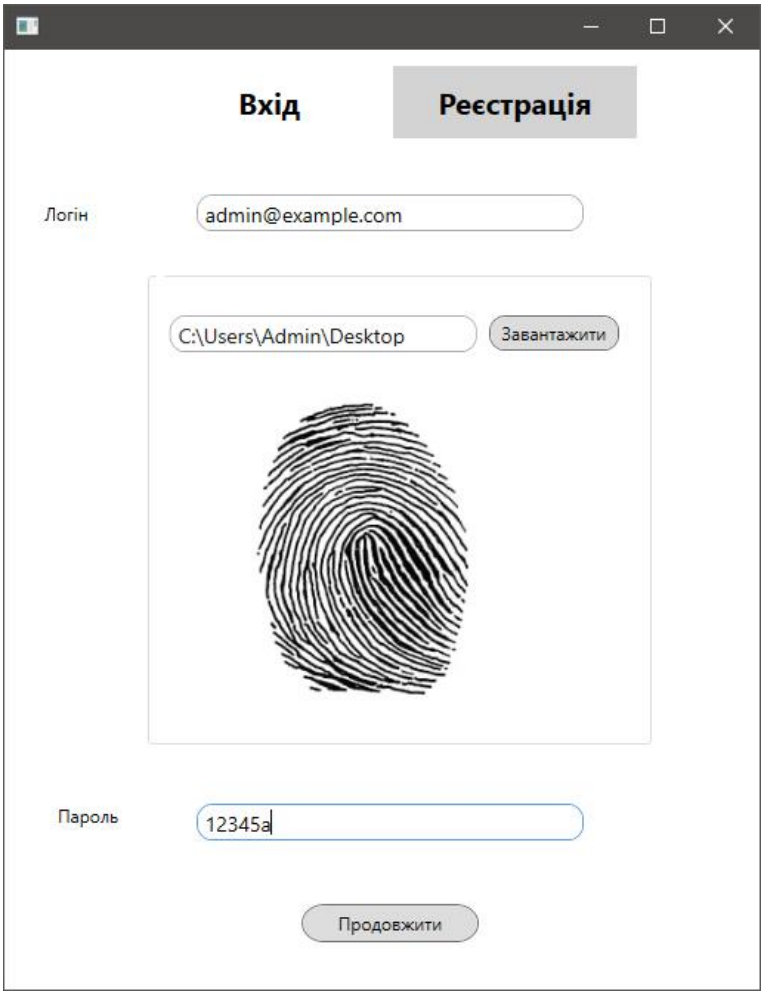


Рисунок 3.5 – Вигляд вікна програми із заповненими полями для реєстрації

У випадку, якщо один із параметрів не відповідає поставленим вимогам, не унікальним, вже належить іншому користувачеві, або ж некоректно задано, то користувач отримує повідомлення про невдалу спробу реєстрації (рис. 3.7).

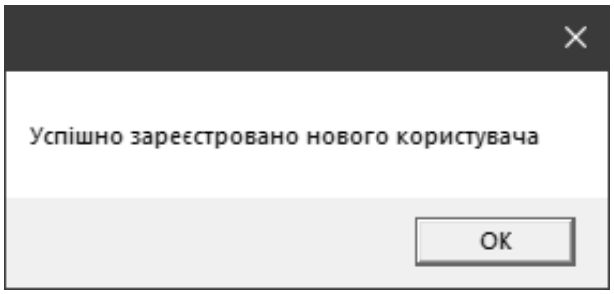


Рисунок 3.6 – Вигляд вікна із повідомленням про успішну реєстрацію

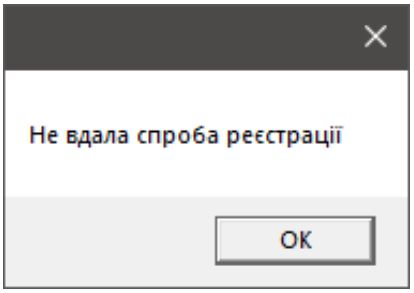


Рисунок 3.7 – Вигляд вікна із повідомленням про невдалу реєстрацію

На рис. 3.8 представлено вигляд діалогового вікна програми після успішної авторизації користувача. У даному вікні у верхній частині розташовано кнопки «Про нас» та «Вийти», а також поле із зазначенням логіну авторизованого користувача.

Рисунок 3.8 – Вигляд вікна авторизованого в системі користувача

У додатковому вікні «Про нас» розміщено загальну інформацію про додаток та його призначення. Дана інформація може бути змінена адміністратором системи.

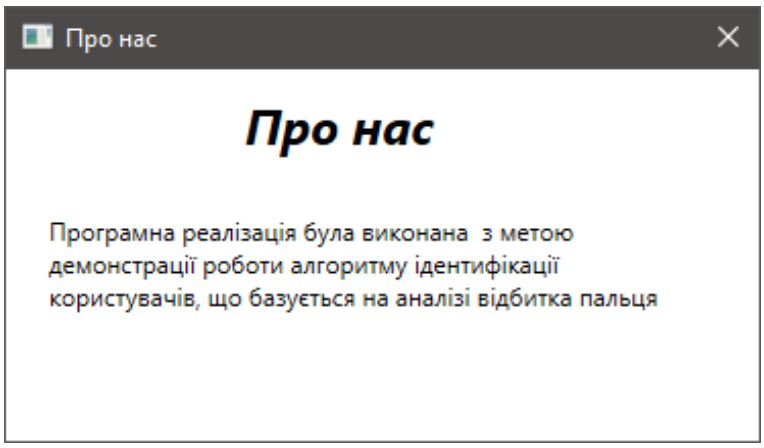


Рисунок 3.9 – Вигляд вікна з інформацією про систему

У випадку, якщо користувач працював у системі, а згодом натиснув кнопку «Вийти», доступ до системи буде заблоковано, у головному вікні буде відображено загальну інформацію, а у полі у верхній частині екрану з’явиться надпис «Не авторизовано».

Рисунок 3.10 – Вигляд вікна не авторизованого в системі користувача

Для здійснення процесу авторизації в системі, після запуску виконуваного файлу додатку, користувачеві слід обрати кнопку «Увійти» у верхній частині вікна та заповнити поля для вводу логіну та зразку відбитку пальця, натиснути кнопку «Продовжити» (рис. 3.11).

У випадку, якщо дані введено коректно та система розпізнає користувача, виводиться повідомлення про успішну авторизацію (рис. 3.12).

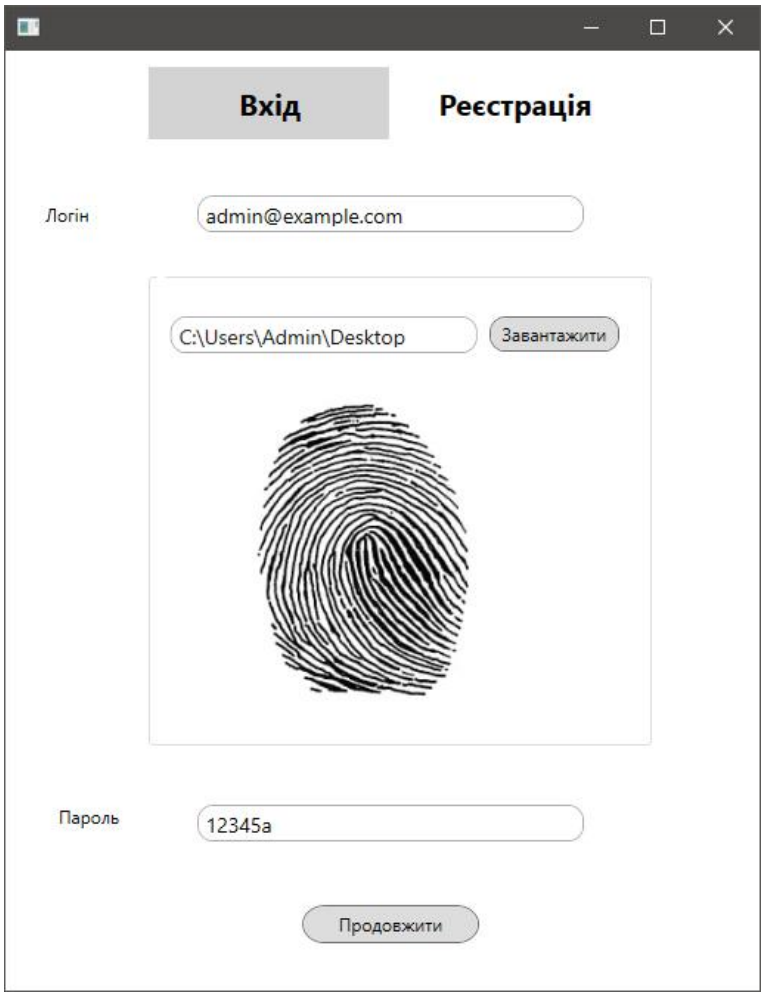


Рисунок 3.11 – Вигляд вікна програми із заповненими полями для авторизації

У випадку, якщо дані введено некоректно, користувачеві повідомляється про невдалу спробу авторизації та кількість спроб входу, що залишилися (не більше трьох).

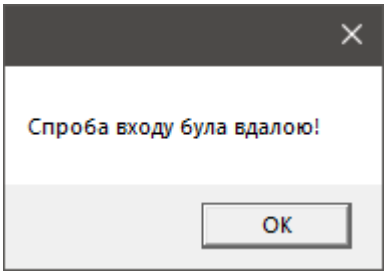


Рисунок 3.12 – Вигляд вікна із повідомленням про успішну авторизацію

Якщо усі спроби входу невдалі, додаток самостійно закривається, а

доступ користувача до системи заблоковано (рис. 3.13 – 3.15).

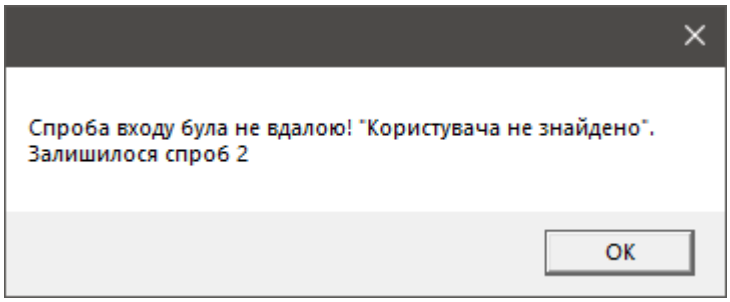


Рисунок 3.13 – Вигляд вікна із повідомленням про невдалу пробу авторизацію, кількість спроб – 2

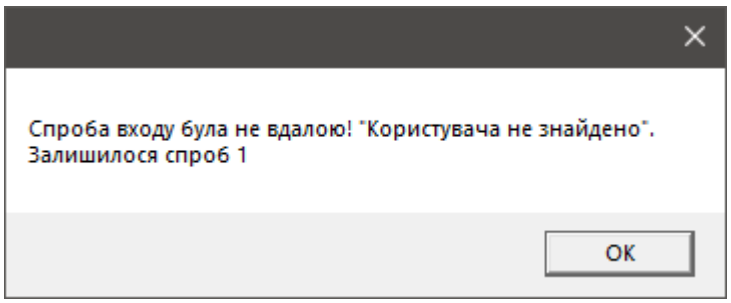


Рисунок 3.14 – Вигляд вікна із повідомленням про невдалу пробу авторизацію, кількість спроб – 1

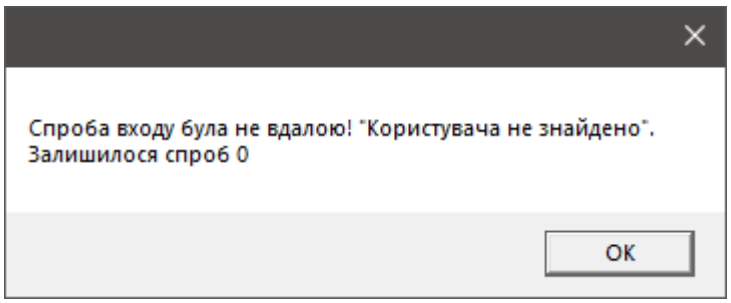


Рисунок 3.15 – Вигляд вікна із повідомленням про невдалу пробу авторизацію, закриття додатку

Повноваження та права доступу до керування системою, реєстрації та видалення нових користувачів належать адміністратору даної системи. Адміністратор здійснює вхід також із використанням унікальних біометричних даних, а також логіну та паролю. Вигляд діалогового вікна додатку для авторизованого адміністратора системи зображено на рисунку 3.16.

Рисунок 3.16 – Вигляд вікна авторизованого адміністратора

У верхній частині діалогового вікна відображається логін авторизованого адміністратора, а також активна кнопка «Адміністрування користувачів», після натискання на яку, надається можливість керувати обліковими записами можливих та існуючих користувачів системи.

У діалоговому вікні (рис. 3.17) адміністратор натискаючи кнопку «Додати користувача» вводить відповідний логін та ім’я користувачів, яким буде дозволений процес реєстрації (а потім, відповідно, авторизації) у системі із використанням їх біометричних даних.

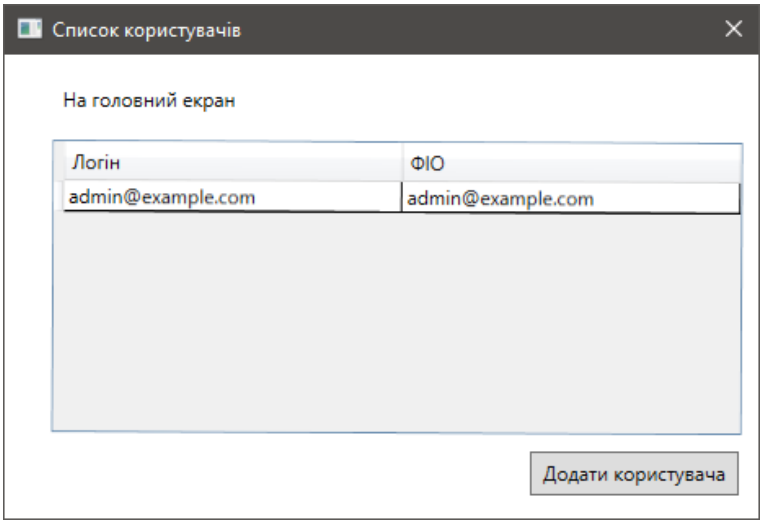


Рисунок 3.17 – Вигляд вікна додавання нового користувача

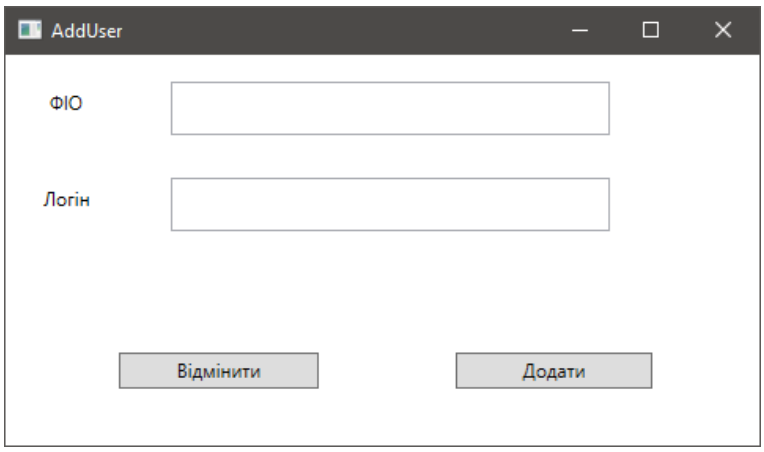


Рисунок 3.18 – Вигляд вікна введення даних нового користувача

Таким чином, було розроблено графічний користувацький інтерфейс додатку для підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії. Під час розроблення інтерфейсу увага приділялася його зручності та зрозумілості для типового користувача.

3.4 Представлення результатів роботи вдосконаленого методу

Згідно із запропонованим алгоритмом, вхідним файлом для опрацюванням програмою, є зображення у форматі bmp (24 біти). Для конвертування даного зображення у чорно-біле можна використати функцію rgb2gray. Далі у підрозділі наведено приклад вхідного і обробленого зображення. Орієнтаційні зображення будуються за градієнтами вихідного зображення.

Рисунок 3.19 – Вигляд відбитка пальця
(початковий та нормалізований рисунок)

Оператор Собеля – це дискретний диференціальний оператор, який обчислює наближене значення градієнта яскравості зображення. Такий оператор засновано на здійсненні згортання зображення із сепарабельним цілочисельним фільтром у вертикальних та горизонтальних напрямках.

Обчислення градієнтного зображення відбувається методом застосування двовимірної операції згортання між зображенням і оператором Собеля (рис. 3.20, 3.21).

Рисунок 3.20 – Зразок полів напрямку для окремого рисунка відбитка пальця

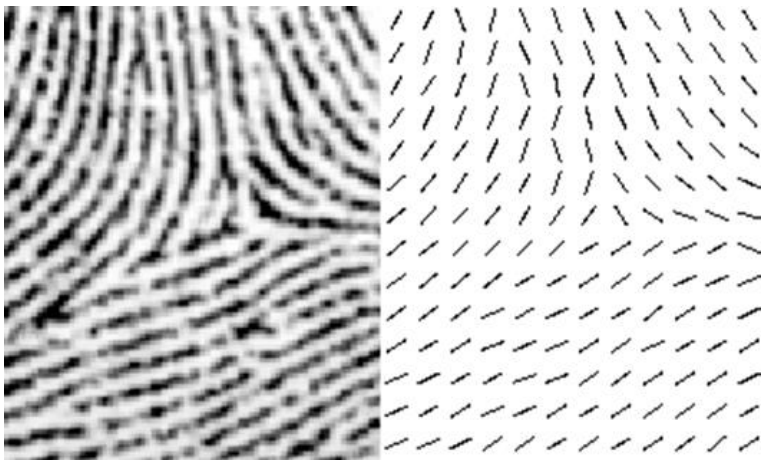


Рисунок 3.21 – Частина полів напрямку для окремого рисунка відбитка пальця

Далі, наступним кроком опрацювання зображень є отримання бінарних зображень, де кожен піксель є пікселем впадини або пікселем гребеня папілярної

лінії. Для оброблення бінарного зображення у нормалізоване зображення застосовують порогове оброблення, тобто присвоюється значення нуля (гребеня) кожному пікселю зображення, якщо він нижчий порогового значення, і – одиниці (впадини) у протилежному випадку (рис. 3.22).

Рисунок 3.22 – Приклад нормалізованого та бінарного зображення (відповідно) після порогового оброблення

Отже, результати тестування програмного засобу дозволили зробити висновок, що запропоноване удосконалення методу є ефективним. Оскільки, опрацьоване зображення за удосконаленим методом має вищу якість, розпізнавання окремих локальних та глобальних ознак можна здійснювати на більш вищому рівні, відповідно і якість розпізнавання значно збільшується, а отже відбувається підвищення та покращення загальної роботи методу ідентифікації особи.

Під час використання даного методу що система біометричної ідентифікації характеризується достатньою точністю, ефективністю, має значну практичну цінність та може бути рекомендованою до практичного застосування.

Для тестування розробленого алгоритму було використано програмний засіб. Були розглянуто відбитки пальців двадцяти чоловік. Відбиток пальця був відсканований за допомогою ПК із наявним модулем сканера відбитка пальця.

На рисунку 3.23 зображено залежність числа правильно ідентифікованих користувачів (в %) від числа компонент моделі. Порівнюючи з результатами розпізнавання відбитку немодифікованим методом якість розпізнавання зросла на 1,7%.

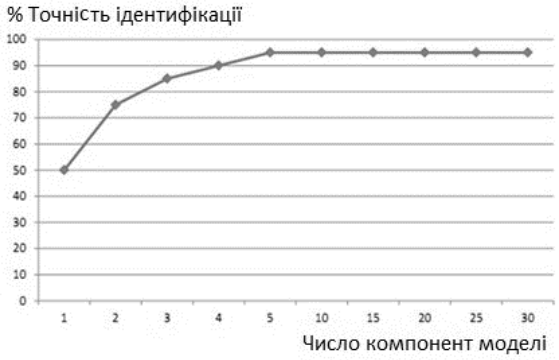


Рисунок 3.23 – Залежність числа правильно ідентифікованих користувачів (в %) від числа компонент моделі

Число компонент, що є оптимальним для ефективної роботи системи дорівнює п'яти. При цьому числі компонент точність ідентифікації мовця становить 96%, що свідчить про те, що реалізований алгоритм може бути з успіхом застосований для санкціонованого доступу до інформації до системи.

3.5 Висновки до розділу

Таким чином, у даному розділі було здійснено програмну реалізацію додатку для підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії. Під час написання магістерської роботи було здійснено проектування користувацького інтерфейсу програми, його практичну розробку, описано особливості програмних етапів реалізації, проведення тестування результатів удосконалення. У процесі тестування було доведено, що запропоноване удосконалення методу є ефективним. Оскільки, опрацьоване зображення за удосконаленим методом має вищу якість, розпізнавання окремих локальних та глобальних ознак можна здійснювати на більш вищому рівні, відповідно і якість розпізнавання значно збільшується, а, отже, відбувається підвищення загальної роботи методу.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Оцінювання комерційного потенціалу розробки ПЗ на основі біометричної ідентифікації

Метою проведення технологічного аудиту є оцінювання комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності [70].

Результатом магістерської кваліфікаційної роботи є розробка програмного засобу методу для підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії.

Для проведення технологічного аудиту залучено трьох незалежних експертів. У нашому випадку такими експертами є викладачі кафедри МБІС: Карпінець В. В. (к.т.н., доцент каф. МБІС ВНТУ), Шиян А. А. (к.ф.-м.н., доцент каф. МБІС ВНТУ) та Дьогтєва І.О. (асист. каф. МБІС ВНТУ).

Оцінювання комерційного потенціалу було здійснене за критеріями, що наведені в таблиці 4.1

Таблиця 4.1 – Критерії оцінювання комерційного потенціалу розробки бальна оцінка

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-терій	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів

Продовження таблиці 4.1

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Кри-тер.	0	1	2	3	4
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатацій ні витрати значно вищі, ніж в аналогів	Експлуатацій ні витрати дещо вищі, ніж в аналогів	Експлуатацій ні витрати на рівні експл. витрат аналогів	Експлуатацій ні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навч. наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовую ться у військово-промисловом у комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві

Продовження таблиці 4.1

11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої к-ті дозвільних документів на вир-во та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки пові-домлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання комерційного потенціалу експертами розробки зведено в таблицю 4.2.

Таблиця 4.2 - Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали, посада експерта		
	1 – Карпінець В.В.	2 – Шиян А.А.	3 – Дьогтєва І.О.
1	4	4	4
Ринкові переваги (недоліки):			
2	4	4	4
3	3	4	3
4	4	3	3
5	3	4	4
Ринкові перспективи			
6	4	3	4
7	4	4	4
Практична здійсненність			
8	5	4	5
9	3	3	4
10	4	4	4
11	3	3	4
12	4	4	3
Сума балів	$СБ_1 = 45$	$СБ_1 = 44$	$СБ_1 = 46$
Середньоарифметична сума балів $\overline{СБ}$	$\overline{СБ} = 45$		

За даними таблиці 4.2 можна зробити висновок, щодо рівня комерційного потенціалу розробки. Зважимо на результат й порівняємо його з рівнями комерційного потенціалу розробки, що представлено в таблиці 4.3.

Таблиця 4.3 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 48	Високий

Рівень комерційного потенціалу розробки, становить 45 балів, що відповідає рівню «високий».

Проаналізуємо суть технічної проблеми та розглянемо аналоги. Наукова новизна розробки полягає в удосконаленні методу розпізнавання відбитку пальця, що, на відміну від існуючих підходів, дозволяє підвищити точність розпізнавання відбитків пальців використовуючи метод дактилоскопії на основі оператора Собеля.

Розпізнавання відбитків пальців одна із перших біометричних методів. Він ґрунтується на визначенні структури ліній на подушечках пальців рук, інакше – папілярних візерунків. Після зчитування сканером унікальний малюнок трансформується на цифровий біометричний шаблон, за допомогою якого система визначає, хто перед нею знаходиться.

Автором запропоновано організувати таку систему контролю доступу, що складається з наступних етапів: етап автентифікації; етап оброки відбитків пальців; етап представлення результатів.

Ще однією складовою розроблюваної системи контролю доступу на основі біометричної ідентифікації є її функціональна структура, тобто набір певних операцій та зв’язків, які циклічно повторюються, та направлені на кінцевий результат роботи системи.

Враховуючи такі переваги розробленого методу, можемо порівняти його з основними аналогами.

У таблиці 4.4 наведені основні технічні показники аналога і нового програмного продукту.

Таблиця 4.4 – Основні технічні показники аналога і нового програмного продукту

Показники, %	Аналог	Нова розробка	Відношення параметрів нової розробки до параметрів аналога
Функціональність	90	100	1,11
Надійність	80	100	1,25
Сумісність	95	100	1,05
Супровід	80	100	1,25
Економія ресурсів і часу	95	100	1,05
Простота використання	75	100	1,33

Автором запропоновано організувати таку систему контролю доступу, що складається з наступних етапів: етап автентифікації; етап оброки відбитків пальців; етап представлення результатів.

В ході аналізу методів розпізнавання відбитків пальців було вирішено, що найбільш доцільним для застосування у даній роботі є метод порівняння по особливих точках. Проте, оскільки серед недоліків даного методу є високі вимоги до якості зображень, то для їх усунення (і в якості удосконалення даного методу) було обрано застосувати оператор Собеля для обробки зображень, за допомогою якого відбуватиметься покращення якості отриманого відбитку пальця.

На підставі вищевикладеного можна стверджувати, що нове технічне рішення, що пропонується для розробки, буде мати кращі показники, ніж у аналога та більшою мірою задовольнить потреби споживачів. Тому його розробка та впровадження є актуальним та доцільним.

Програмний засіб на сьогодні має перспективу та користь як для пересічних користувачів так і для спецслужб. Продукт, який пропонується є реалізованим засобом, що дозволяє проводити автентифікацію користувачів в системі. Готовий програмний продукт буде реалізовуватись на ринку програмних засобів шляхом щомісячної підписки за певну плату.

Під час встановлення ціни та попиту на новий програмний продукт основна увага повинна акцентуватися на унікальності об'єкта купівлі-продажу, цінах продуктів конкурентів, перевагах порівняно з аналогами, витратах, які зазнає покупець у разі заміни старого продукту новим, ступені терміновості та гостроті потреби.

Програмний засіб готовий для використання. Фахівці відповідної кваліфікації наявні, трудові та фінансові ресурси теж, обслуговування програми може відбуватись в режимі он-лайн, з будь-якої точки світу, оскільки немає проблем з передачею на нього прав. Комерціалізація розробки знаходиться на початковому етапі. Ведуться пошуки інвесторів та партнерів. Наявні зацікавлені особи, що готові першими випробувати програмний засіб в обмін на акт впровадження та подальшу рекламу від їх імені. Просування на ринок планується шляхом реалізації та продажу через спеціалізовані магазини програмного забезпечення.

4.2 Прогнозування витрат на виконання наукової роботи та впровадження її результатів

Прогнозування витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи складається з таких етапів:

1-й етап: розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи;

2-й етап: розрахунок загальних витрат на виконання даної роботи;

3-й етап: прогнозування загальних витрат на виконання та впровадження

результатів даної роботи.

Виконаємо розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи, за такими статтями та формулами, приймаючи до уваги те, що для розробки інформаційної технології було залучено одного розробника програмного забезпечення.

1. Основна заробітна $З_о$:

$$З_о = \frac{М}{Т_р} \cdot t, \text{грн.} \quad (4.1)$$

де $М$ – місячний посадовий оклад – $22\,000$ грн.;

$Т_р$ – число робочих днів в місяці; приблизно $Т_р = 22$ дня;

t – число робочих днів роботи – 22 дня.

Таким чином:

$$З_о = \frac{22000}{22} \cdot 22 = 22\,000 \text{ (грн.)}$$

Таблиця 4.5 – Витрати по заробітній платі

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату
Розробник	22 000	1000	22	22 000
Всього				22 000

2. Додаткова заробітна плата $З_д$ працівників розраховується як 12% від основної заробітної плати:

$$З_д = 0{,}12 \cdot 20\,000 = 2\,640 \text{(грн.)} - \text{для розробника}$$

3. Нарахування на заробітну плату $Н_{зп}$ розробника становить:

$$Н_{зп} = (З_о + З_д) \cdot \frac{\beta}{100} \quad (4.2)$$

де $З_о$ – основна заробітна плата розробника;

$З_д$ – додаткова заробітна плата розробника;

β – ставка єдиного внеску на загальнообов'язкове державне соціальне страхування – 22%.

$$Н_{зп} = (22\,000 + 2\,640) \cdot 0{,}22 = 5\,420 \text{ (грн.)}$$

4. Амортизація обладнання, комп'ютерів та приміщень, які використовувались під час виконання даного етапу роботи розраховуємо за формулою:

$$А = \frac{Ц \cdot Т}{12 \cdot Т_В} \quad (4.3)$$

де Ц – загальна балансова вартість обладнання, приміщення тощо, грн.;

Т – фактична тривалість використання, міс;

$Т_В$ – термін використання обладнання, приміщень тощо, роки.

Розробка програмного забезпечення ведеться 1місяць.

Розрахунки зведено до таблиці 4.6:

Таблиця 4.6 – Амортизаційні відрахування

Найменування	Балансова вартість (грн.)	Термін використання (років)	Фактична тривалість використання, (міс.)	Величина амортизацій - них відрахувань, (грн..)
Офісне приміщення	35 000	10	1	450
Комп'ютер	15 000	5	1	250
Монітор	5 000	5	1	150
Принтер	10 000	3		400
			Всього	1 250

5. Витрати на комплектуючі К, що були використані під час виконання даного етапу роботи, розраховуються за формулою:

$$К = \sum_{1}^{n} Н_i \cdot Ц_i \cdot К_i \text{ (грн.)} \quad (4.4)$$

де $Н_i$ – кількість комплектуючих *i*-го виду, шт.;

$Ц_i$– ціна комплектуючих *i*-го виду, грн.;

$К_i$ – коефіцієнт транспортних витрат, $К_i$ = (1,1…1,15);

n – кількість видів комплектуючих.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектувальних	Кількість	Ціна за штуку, грн.	Сума, грн.	Примітка
Клавіатура (тип 1)	1	500 грн.	500 грн.	
Блок БЖ	1	1200 грн.	1200 грн.	
Портативний сканер	1	2500 грн.	2 500 грн.	
Всього:			$К_i = 1,2$	5040 грн.

6. Витрати на силову електроенергію $В_е$ розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п \text{ (грн.)} \quad (4.5)$$

Де В – вартість 1 кВт-год.;

П – установлена потужність обладнання – 0,8 кВт;

Ф – фактична кількість годин роботи обладнання – 440 годин,

$К_п$ – коефіцієнт використання потужності.

$$В_е = 3,5 \cdot 0,8 \cdot 440 \cdot 0,14 = 173 \text{ (грн).}$$

7. Інші витрати $В_{ін}$ охоплюють:

– витрати на управління організацією;

– оплату службових відряджень;

– витрати на утримання, ремонт та експлуатацію основних засобів;

– витрати на опалення, освітлення, водопостачання, охорону праці тощо.

Інші витрати $В_{ін}$ можна прийняти як 100% від суми основної заробітної плати розробника:

$$В_{ін} = 22\,000 \cdot 1 = 22\,000 \text{ (грн)}$$

Послуги Інтернету – 500 грн., інше – 1500 грн. Загальна вартість становить:

$$500 + 1000 = 1\,500 \text{ (грн.)}$$

8. Сума всіх попередніх статей витрат дає витрати на виконання даної частини роботи – В.

$$В = 22\,000 + 2\,640 + 5\,420 + 1\,250 + 5\,040 + 173 + 22\,000 + 1\,500 = 60\,023 \text{ (грн.)}$$

9. Проведемо прогнозування загальних витрат ЗВ на виконання та впровадження результатів виконаної наукової роботи. Прогнозування здійснюється за формулою:

$$ЗВ = \frac{В_{заг}}{\beta}, \text{грн.} \quad (4.6)$$

де β – коефіцієнт, який характеризує етап (стадію) виконання даної роботи.

Так, якщо розробка знаходиться:

– на стадії науково-дослідних робіт, то $\beta \approx 0{,}1$;

– на стадії технічного проектування, то $\beta \approx 0{,}2$;

– на стадії розробки конструкторської документації, то $\beta \approx 0{,}3$;

– на стадії розробки технологій, то $\beta \approx 0{,}4$;

– на стадії розробки дослідного зразка, то $\beta \approx 0{,}5$;

– на стадії розробки промислового зразка, $\beta \approx 0{,}7$;

– на стадії впровадження, то $\beta \approx 0{,}9$.

$В_{заг}$ – загальна вартість всієї наукової роботи.

$$В = 60\ 023\ (грн.)$$

$$ЗВ = \frac{60\ 023}{0{,}7} = 85\ 747\ (грн.)$$

Отже, прогноз загальних витрат ЗВ на виконання та впровадження результатів виконаної наукової роботи складає $85\ 747$ (грн.)

4.3 Прогнозування комерційних ефектів від реалізації результатів розробки

У даному підрозділі проведемо кількісне прогнозування, яку вигоду, зиск можна отримати у майбутньому від впровадження результатів виконаної наукової роботи.

В умовах ринку узагальнюючим позитивним результатом, що його отримує підприємство від впровадження результатів тієї чи іншої розробки, є збільшення чистого прибутку підприємства. Зростання чистого прибутку можна оцінити у теперішній вартості грошей.

Зростання чистого прибутку забезпечить інвестору надходження додаткових коштів, які дозволять покращити фінансові результати діяльності.

Виконання даної наукової роботи та впровадження її результатів складає приблизно 1 рік. Позитивні результати від впровадження розробки очікуються вже в перші місяці після впровадження.

Проведемо детальне прогнозування позитивних результатів та кількісне їх оцінювання по роках.

Обчислимо збільшення чистого прибутку підприємства $\Delta П_i$ для кожного із років, протягом яких очікується отримання позитивних результатів від впровадження розробки, розраховується за формулою:

$$\Delta П_i = \sum_{1}^{n} (\Delta П_я \cdot N + П_я \cdot \Delta N)_i \quad (4.7)$$

де $\Delta П_я$ – покращення основного якісного показника від впровадження результатів розробки у даному році;

N – основний кількісний показник, який визначає діяльність підприємства у даному році до впровадження результатів наукової розробки;

ΔN – покращення основного кількісного показника діяльності підприємства від впровадження результатів розробки;

$П_я$ – основний якісний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки;

n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки.

Припустимо, що внаслідок впровадження результатів наукової розробки чистий прибуток підприємства збільшиться на 110 грн., а кількість одиниць реалізованої послуги збільшиться:

– протягом першого року – на 500 од.,

– протягом другого року – ще на 720 од.,

– протягом третього року – ще на 900 од.

Орієнтовно: реалізація продукції до впровадження результатів наукової розробки складала 1 шт., а прибуток, що його отримувало підприємство на одиницю продукції до впровадження результатів наукової розробки – 70 грн.

Потрібно спрогнозувати збільшення чистого прибутку підприємства від впровадження результатів наукової розробки у кожному році відносно базового.

Збільшення чистого прибутку підприємства $\Delta П_1$ протягом першого року складе:

$$\Delta П_1 = 70 \cdot 1 + (70 + 110) \cdot 500 = 90\,070 \text{ (грн.)}$$

Обчислимо збільшення чистого прибутку підприємства $\Delta П_2$ протягом другого року:

$$\Delta П_2 = 70 \cdot 1 + (70 + 110) \cdot (500 + 720) = 219\,670 \text{ (грн.)}$$

Збільшення чистого прибутку підприємства $\Delta П_3$ протягом третього року становитиме:

$$\Delta П_3 = 70 \cdot 1 + (70 + 110) \cdot (500 + 720 + 900) = 381\,670 \text{ (грн.)}$$

Отже, розрахунки показують, що відповідно прогнозуванню комерційний ефект від впровадження розробки виражається у значному збільшенні чистого прибутку підприємства.

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Основними показниками, які визначають доцільність фінансування наукової розробки певним інвестором, є абсолютна і відносна ефективність вкладених інвестицій та термін їх окупності.

Розрахунок ефективності вкладених інвестицій передбачає:

1-й крок. Розрахунок теперішньої вартості інвестицій PV, що вкладаються в наукову розробку.

Такою вартістю ми можемо вважати прогнозовану величину загальних витрат ЗВ на виконання та впровадження результатів НДДКР, тобто $ЗВ = PV = 83\,439 \text{ (грн.)}$

2-й крок. Розрахуємо очікуване збільшення прибутку$\Delta П_i$, що його отримає підприємство (організація) від впровадження результатів наукової розробки, для кожного із років, починаючи з першого року впровадження. Таке збільшення прибутку також було розраховане нами раніше та становить:

$$\Delta П_1 = 90\,070 \text{ (грн)}, \Delta П_2 = 219\,670 \text{(грн)}, \Delta П_3 = 381\,670 \text{(грн)}.$$

3-й крок. Будуємо вісь часу, на якій відображаємо всі платежі (інвестиції та прибутки), що мають місце під час виконання науково-дослідної роботи та впровадження її результатів.

Рисунок 4.1 характеризує рух платежів (інвестицій та додаткових прибутків).

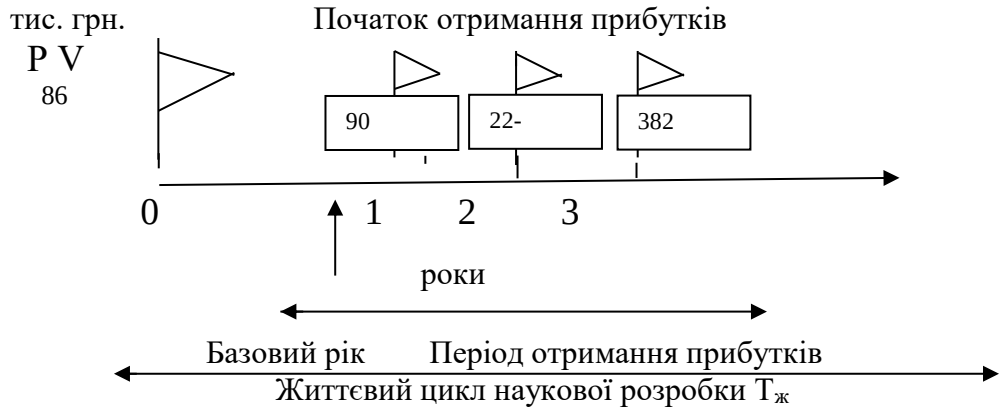


Рисунок 4.1 – Вісь часу з фіксацією платежів, що мають місце під час розробки та впровадження результатів НДДКР

4-й крок. Розрахуємо абсолютну ефективність вкладених інвестицій $Е_{абс}$ за формулою:

$$Е_{абс} = (ПП - PV), (грн.) \quad (4.8)$$

де ПП – приведена вартість всіх чистих прибутків, що їх отримає підприємство (організація) від реалізації результатів наукової розробки, грн.;

PV – теперішня вартість інвестицій $PV = ЗВ$, грн.

Приведена вартість всіх чистих прибутків ПП розраховується за формулою:

$$ПП = \sum_{1}^{Т} \frac{\Delta П_i}{(1+\tau)^t}, (грн) \quad (4.9)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом

яких виявляються результати виконаної та впровадженої НДДКР, грн.;

Т – період часу, протягом якого виявляються результати впровадженої НДДКР, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні – 0,1;

t – період часу (в роках) від моменту отримання чистого прибутку до точки «0»;

$$ПП = \frac{90\,070}{(1+0{,}1)^1} + \frac{219\,670}{(1+0{,}1)^2} + \frac{381\,670}{(1+0{,}1)^3} = 550\,182\ (\text{грн.})$$

$$Е_{абс} = 550\,182 - 85\,747 = 464\,435\ (\text{грн.})$$

Оскільки $Е_{абс} > 0$, результат від проведення наукових досліджень щодо розробки програмного продукту та їх впровадження принесе прибуток, тобто є доцільним, проте це ще не свідчить про те, що інвестор буде зацікавлений у фінансуванні даної програми.

5-й крок. Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $Е_в$ за формулою:

$$Е_в = \sqrt[Т_ж]{1 + \frac{Е_{абс}}{PV} - 1} \qquad (4.10)$$

де $Е_{абс}$ – абсолютна ефективність вкладених інвестицій, грн.;

PV – теперішня вартість інвестицій $PV = ЗВ$, грн.

$Т_ж$ – життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{1 + \frac{464\,435}{85\,747}} - 1 = \sqrt[3]{6{,}4} - 1 = 0{,}82 \text{ або } 82\%$$

Порівняємо $E_в$ з мінімальною (бар'єрною) ставкою дисконтування τ_{min},

яка визначає ту мінімальну дохідність, нижче за яку інвестиції вкладатися не будуть.

Спрогнозуємо величину τ_{min}.

У загальному вигляді мінімальна (бар'єрна) ставка дисконтування τ_{min}визначається за формулою:

$$\tau_{min} = d + f \tag{4.11}$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; $d = 0{,}2$;

f – показник, що характеризує ризикованість вкладень; величина $f = 0{,}5$.

$$\tau_{min} = 0{,}2 + 0{,}5 = 0{,}7$$

Оскільки

$$E_{\text{в}} = 82\% > \tau_{min} = 70\%,$$

то у інвестора є потенційна зацікавленість у фінансуванні даної наукової розробки.

6-й крок. Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій $\text{Т}_{\text{ок}}$ за формулою:

$$\text{Т}_{\text{ок}} = \frac{1}{\text{Е}_{\text{в}}}, \text{рік} \tag{4.12}$$

$$\text{Т}_{\text{ок}} = \frac{1}{0{,}82} = 1{,}3 \text{ (року)}$$

Оскільки термін окупності вкладених у реалізацію наукового проекту інвестицій менше трьох років

$$(\text{Т}_{\text{ок}} < 3 \text{ років}),$$

то фінансування нової розробки є доцільним.

4.5 Висновки до розділу

В даному розділі було виконано оцінювання комерційного потенціалу розробки програмного засобу для підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії.

Проведено технологічний аудит з залученням трьох незалежних експертів. Визначено, що рівень комерційного потенціалу розробки вище середнього. Проведено порівняння з аналогом. Згідно з проведеним оцінюванням нова розробка є якісною та конкурентоспроможною.

Рівень комерційного потенціалу розробки, становить 45 балів, що відповідає рівню «високий».

Згідно із розрахунками всіх статей витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи загальні витрати на розробку складають 85 747 (грн.). Розрахована абсолютна ефективність вкладених інвестицій в сумі 464 435 (грн.) свідчить про отримання прибутку інвестором від комерціалізації програмного продукту.

Щорічна ефективність вкладених в наукову розробку інвестицій складає 82%, що вище за мінімальну бар'єрну ставку дисконтування, яка складає 70%. Це означає потенційну зацікавленість інвесторів у фінансуванні розробки.

Термін окупності вкладених у реалізацію проекту інвестицій становить 1,3 (року), що також свідчить про доцільність фінансування нової розробки.

Отже, проаналізувавши отримані економічні показники, можна вважати, що запропонована розробка програмного засобу має високий комерційний потенціал, а тому є доцільною для подальшого впровадження.

ВИСНОВОК

У магістерській дипломній роботі розроблено програмний додаток для підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії (на основі оператора Собеля).

Одна з причин популярності біометричних систем зводиться до об'єктивної потреби замовників організувати сучасну, грамотно побудовану систему безпеки у себе на підприємстві, офісі компанії або приватному будинку. Більшість прогнозів зводиться до того, що використання біометричних систем безпеки на вітчизняний ринок набуде незабаром лавинного характеру. Інтенсивний розвиток мультимедійних, цифрових технологій і, як наслідок, їх здешевлення дозволяють не лише розробити принципово нові підходи у проблемі ідентифікації особистості, а й запровадити в широке використання. Зараз удосконалення біометричних технологій відбувається прискореними темпами. А тому актуальність роботи над даною темою лише зростає оскільки, деякі методи дактилоскопії мають недоліки, що полягають у їх складності в реалізації та великій математичній базі, неможливості підключення до деяких баз даних та, зокрема, недостатній точності. Такі проблеми методу зумовлюють актуальність застосування оператора Собеля при реалізації біометричної ідентифікації методу дактилоскопії з метою підвищення достовірності ідентифікації користувачів.

Таким чином, у магістерській дипломній роботі автором запропоновано організувати таку систему контролю доступу, що складається з таких етапів: автентифікація, оброблення відбитків пальців, представлення результатів.

У першому розділі роботи було проаналізовано теоретичні засади досліджуваної галузі знань, а саме: переваги та недоліки біометричної ідентифікації, її особливості, сфери застосування, існуючі методи ідентифікації особистості на основі біометричних даних, детально розглянуто метод ідентифікації – дактилоскопію.

У другому розділі роботи було розроблено систему ідентифікації

користувачів. У ході аналізу методів розпізнавання відбитків пальців було доведено, що найбільш доцільним є дактилоскопічний метод порівняння по особливих точках. Проте, оскільки серед недоліків даного методу є високі вимоги до якості зображень, то для їх усунення автором магістерської роботи було запропоновано застосувати оператор Собеля для оброблення зображень, за допомогою якого відбуватиметься покращення якості отриманого відбитку пальця.

У третьому розділі було здійснено програмну реалізацію додатку для підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії. Для тестування розробленого алгоритму було використано програмний засіб. Були розглянуто відбитки пальців двадцяти чоловік. Відбиток пальця був відсканований за допомогою ПК із наявним модулем сканера відбитка пальця. Порівнюючи з результатами розпізнавання відбитку немодифікованим методом якість розпізнавання зросла на 1,7%. Число компонент, що є оптимальним для ефективної роботи системи дорівнює п'яти. При цьому числі компонент точність ідентифікації мовця становить 96%, що свідчить про те, що реалізований алгоритм може бути з успіхом застосований для санкціонованого доступу до інформації до системи.

У четвертому розділі роботи було проаналізовано деякі отримані економічні показники, за результатами аналізу яких, можна вважати, що запропонована розробка програмного засобу має високий комерційний потенціал, а тому є доцільною для подальшого впровадження. На базі запропонованого методу було розроблено відповідний програмний продукт, що може використовуватися разом із методом ідентифікації користувачів на основі зчитування образу обличчя. Таке комплексне застосування надає можливість системі захисту точніше аналізувати та розпізнавати користувачів, що, відповідно, підвищує її надійність. Отже, автором було досягнуто поставлену мета роботи, а саме, розроблено та практично реалізовано програмний додаток для підвищення достовірності ідентифікації користувачів із використанням удосконаленого методу дактилоскопії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Домарев В.В. Захист інформації та безпека комп’ютерних систем. 2007.

2. Сафронов В.В. Современные биометрические методы идентификации.: URL: http://habrahabr.ru/blogs/infosecurity/126144/

3. Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.. Комплексні системи захисту інформації : навчальний посібник / Вінниця: ВНТУ, 2017. – 120 с.

4. Данилюк І. І., Карпінець В. В., Приймак А. В., Яремчук Ю. Є., Костюченко О. І. Метод ідентифікації користувача за клавіатурним почерком на основі нейромереж / Вінниця: ВНТУ, 2017. 120 с.

5. Азарова А. О., Гудзь В. О., Блонський В. О. Управління інформаційною безпекою в державних установах на основі біометричної аутентифікації відбитків пальців для захисту інформації від несанкціонованого доступу. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm2019/paper/view/7429

6. Борзенко А. Биометрические системы распознавания внешности URL: http://www.bytemag.ru/articles/detail.php? ID=8520

7. Попов М., Задорожный В. Биометрические системы безопасности: URL:www.BRE.ru

8. Азарова А.О., Безмощук О. В.Причини відмови від делегування повноважень / Тези доповіді «Всеукраїнської науково-прак-тичної Інтернет-конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи»». 2020. URL: https://conferences.vntu.edu.ua/index.php/mn/mn2020/paper/view/9965

9. Безмощук О. В. Ідентифікація критичних станів суспільства за даними з соціальних мереж / Тези доповіді «Всеукраїнської науково-практичної Інтернет-конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи»». 2021. URL: https:// conferences.vntu.edu.ua/index.php/mn/mn2021/paper/view/10957/9161

10. Азарова А. О, Богачук В. В., Безмощук О. В. Автентифікації користувачів засобами технології Face ID на основі вдосконаленого методу фільтрування зображення/ Тези доповіді/ Всеукраїнська науково-практична Інтернет-конференція студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи (МН-2022) [Електронний ресурс] // Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/14176/11988

11. Азарова А. О, Безмощук О. В., Богачук В. В. Ідентифікація користувачів на основі удосконаленого методу дактилоскопії/ Тези доповіді/ Всеукраїнська науково-практична Інтернет-конференція студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи (МН-2022) [Електронний ресурс] // Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2022/paper/viewFile/14177/11992

12. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. К. : Изд-во Юниор, 2003. 504 с.

13. Задонский А. Ю. Вопросы аутентификации всовременных информационных системах. – URL:http://www.compserv.ru

14. Чала Л. Е. Методи динамічної ідентифікації користувачів розподілених інформаційних систем. / Л. Е. Чала. – Харків, 2006. – 20 с.

15. Дудатьєв А. В., Каплун В. А., Семеренко В. П. Захист програмного забезпечення. Частина 1. Навчальний посібник. Вінниця : ВНТУ, 2005. 140 с.

16. Рудаков, О. М. Метод биометрической аутентификации, основанный на анализе клавиатурного почерка URL: https://moluch.ru/archive/115/30980/

17. Лакин Г.Ф. Биометрия. Учебное пособие. – М.: Высшая школа. – 1990. – 223 с.

18. Абламейко С.В. Обробка зображень: технології, методи, застосування / С.В. Абламейко. – М.: Амалфея, 2000. – 304 с.

19. Анісімов Б.В. Розпізнавання і цифрова обробка зображень / Б.В. Анісімов, В.Д. Курганов, В.К. Злобін. – М.: Висш.шк., 1983. – 295 с.

20. Сойфер В.А. Методи комп'ютерної обробки зображень / В.А. Сойфер. – 2-е изд. – М.: ФИЗМАТЛИТ, 2003. – 784 с.

21. Canny J. A Computational Approach To Edge Detection / J. Canny // IEEE Trans. Pattern Analysis and Machine Intelligence, 1986. – P. 679-698.

22. Дубчак О.В., Підгайна К.І., Порівняльний аналіз сучасних біометричних методів аутентифікації. / «Захист інформації в інформаційно-комунікаційних системах». Київ: НАУ, 2010. 87 с.

23. Wikipedia. USA «Биометрия» URL: http://ru.wikipedia.org/wiki/

24. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом». Учебное пособие. – М.: Горячая линия – Телеком. – Серия «Обеспечение безопасности объектов». Книга 2. 2010 -272 с.:ил.

25. Татарченко Н.В., Тимошенко С.В. Биометрическая идентификация в интегрированных системах безопасности. Специальная техника, №2, 2002.

26. Минаев В.А. Современные технологии обеспечения информационной безопасности. «Биометрический квартал»

27. Дахва М.С. Идентификация по геометрии кисти руки. 2012.

28. Джонатан П., Филипс и др. Введение в оценку биометрических систем. «Открытые системы», №3. 2000.

29. А. Гинце. Новые технологии в СКУД. Системы безопасности, №6. 2005.

30. Pentland, A. & Turk, M. (1991). Eigenfaces for Recognition. Journal of Cognitive Neuroscience 3(1): 71-86.

31. Бастрикін А. І. Дактилоскопія. Знаки руки. / Бастрикін А. І., 2004.

32. Девід Ліон. Товариство спостереження: Моніторинг повсякденного життя / Девід Ліон. – Філадельфія, 2001.

33. Туляков С. Симетричні хеш-функції для мініцій відбитків пальців / С. Туляков, Ф. Фарук, Г. В.., 2005.

34. Хагхигат М. Дискриминантний кореляційний аналіз: Fusion в режимі реального часу для мультимодального біометричного розпізнавання / М. Хагхигат, М. Абдель-Мотталеб, В. Аналлабі., 2016.

35. Science Daily. Запитання, що виникли про системи Розпізнавання Іриси. – 12.

36. N. K. Ratha. Enhancing security and privacy in biometrics-based authentication systems, IBM systems Journal / N. K. Ratha, J. H. Connell, R. M. Bolle. – №40.

37. Шаров В. Біометричні методи комп'ютерної безпеки/ Владислав Шаров // ByteMag. – 2005. URL: https://www.bytemag.ru/articles/detail.php

38. Попов М. Біометричні системи безпеки / Попов М.., 2011.

39. Клімакін С.П. Ера біометрії / Клімакін С.П, Петруненко А.А., Черномордик О.М.., 2006.

40.Задорожний В. Ідентифікація за відбитками пальців. Частина 1 / Задорожний В. // PC Magazine. – 2004. URL: https://bms.ucoz.ru/statii/

41. Задорожный В., "Идентификация по отпечаткам пальцев", Часть 1, 2004

42. Задорожный В., "Идентификация по отпечаткам пальцев", Часть 2, 2007

43. Давлетханов М., "Способы идентификации по отпечаткам пальцев", 2004

44. Кухарев Г. А., материалы из монографии "Биометрические системы"/ СПб.: Политехника, 2001, 240 с.

45. Вакуленко А., Юхин А., "Биометрические методы идентификации личности: обоснованный выбор и внедрение", 2007;

46. Зиятдинов А. И., "Принципы построения систем биометрической аутентификации"/ МФТИ, 2005, 8 с.

47. A.K. Jain, S. Prabhakar, L. Hong, "A Multichannel Approach to Fingerprint Classification"/ IEEE TRANSACTIONS ON PATTERN ANALYSIS and MACHINE INTELLIGENCE, 1999, p.348-359

48. L. Hong, Y. Wan, A.K. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation"/ IEEE TRANSACTIONS ON PATTERN ANALYSIS and MACHINE INTELLIGENCE, 1998, p. 777-789

49. A. Senior, "A Combination Fingerprint Classifier"/ ieee transactions on pattern analysis and machine intelligence, 2001, p. 1165-1174

50. D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, "Handbook of Fingerprint Recognition"/ Springer, New York, 2003.

51. Bieri M. Wethmar A. Wey N. Quantitative analysis of Alzheimer plaques in mice using virtual microscopy // First European Workshop on Tissue Imaging and Analysis – Germany, 2009 – P.31-38

52. Егорова О. В., Клыкова Е. И., Пантелеев В. Г. Компьютерная микроскопия. – М.: Техносфера, 2005. – 304 с.

43. Pratt W. K. Digital Image Processing: PIKS Inside, Third Edition. – NY, USA.: John Wiley & Sons, Inc., 2001 – 758 p.

54. Форсайт Д. Компьютерное зрение. Современный поход /. Понс Дж – СПб.: Вильямс, 2004. – 928 с.

55. Гонсалес Р., Вудс Р.. Цифровая обработка зображений. – М.: Техносфера, 2005. – 1072 с.

56. Введение в контурный анализ; приложения к обработке изображений и сигналов / Я.А.Фурман, А.В Кревецкий, А.К. Передреев, А.А. Роженцов, Р.Г. Хафизов, И.Л Егошина, А.Н. Леухин. – М.: ФИЗМАТЛИТ, 2003. – 592 с.

57. Haralick R.M and. Shapiro L.G. Image Segmentation Techniques // Computer Vision, Graphics and Image Processing, – 1985. – Vol.29 – P.100-132

58. Fu K. Mui J. A survey on image segmentation // Pattern Recognition – 1981- Vol.13 – P.3-16

59. Байгарова Н.С., Бухштаб Ю.А., Евтеева Н.Н., Корягин Д.А. Некоторые подходы к организации содержательного поиска изображений и видеоинформации.– Москва: Институт прикладной математики им. Келдыша РАН, 2002.– 24 с.

60. Гончаров А., Мельниченко А. Pseudometric Approach to Content Based Image Retrieval and Near Duplicates Detection.– РОМИП, 2008.– 34 с.

61. Пономаренко Н.Н., Лукин В.В., Абрамов С.К. Устойчивый поиск изображений по полному и тематическому подобию с использованием

многопараметровой классификации.– Харьков: «ХАИ», 2003.– 13с.

62. Джон Скит. C# для профессионалов: тонкости программирования, 3-е издание, новый перевод = C# in Depth, 3rd ed.. – М.: «Вильямс», 2014. –608 с.

63. Кристиан Нейгел и др. C# 5.0 и платформа .NET 4.5 для профессионалов = Professional C# 5.0 and .NET 4.5. – М.: «Диалектика», 2013. – 1440 с.

64. А. Хейлсберг, М. Торгерсен, С. Вилтамут, П. Голд. Язык программирования C#. Классика Computers Science. 4-е издание = C# Programming Language (Covering C# 4.0), 4th Ed. – СПб.: «Питер», 2012. — 784 с.

65. Э. Стиллмен, Дж. Грин. Изучаем C#. 2-е издание = Head First C#, 2ed. –СПб.: «Питер», 2012. — 704 с.

66. Эндрю Троелсен. Язык программирования C# 5.0 и платформа .NET 4.5, 6-е издание = Pro C# 5.0 and the .NET 4.5 Framework, 6th edition. – М.: «Вильямс», 2013. – 1312 с.

67. Джозеф Албахари, Бен Албахари. C# 6.0. Справочник. Полное описание языка = C# 6.0 in a Nutshell: The Definitive Reference. – М.: «Вильямс», 2018. – 1040 с.

68. Герберт Шилдт. C# 4.0: полное руководство = C# 4.0 The Complete Reference. – М.: «Вильямс», 2010. – с. 1056.

69. Visual Studio URL: https://docs.microsoft.com/ru-2019

70. Методичні вказівки до виконання студентами-магістрантами економічної частини магістерських кваліфікаційних робіт / Уклад. В. О. Козловський – Вінниця: ВНТУ, 2012. – 22 с.

ДОДАТКИ

Додаток А. Технічне завдання

Вінницький національний технічний університет

Факультет менеджменту та інформаційної безпеки

Кафедра менеджменту та безпеки інформаційних систем

ЗАТВЕРДЖУЮ
Голова секції «Управління інформаційною
безпекою» кафедри МБІС
д.т.н., професор
_____ Ю. Є. Яремчук

«24» вересня 2021 р.

ТЕХНІЧНЕ ЗАВДАННЯ

до магістерської кваліфікаційної роботи на тему:

Підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії

08-42.МКР.002.00.00 ТЗ

Керівник магістерської кваліфікаційної роботи
проф. каф. МБІС Азарова А.О.
_____

Вінниця – 2021 р.

1 Найменування та область застосування

Програмний засіб підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії.

Область застосування: забезпечення захищеного доступу до системи шляхом біометричної ідентифікації користувачів.

2 Підстави для розробки

Розробка виконується на основі наказу ректора ВНТУ 24 вересня 2021 року №277.

3 Мета та призначення розробки

3.1 Мета розробки

Метою роботи є розробка та реалізація програмного засобу для підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії.

3.2 Призначення

Розроблений програмний продукт забезпечує можливість достовірної ідентифікації користувачів з використанням удосконаленого методу дактилоскопії.

4 Джерела розробки

1. Домарев В.В. Захист інформації та безпека комп’ютерних систем. 2007.

2. Борзенко А. Биометрические системы распознавания внешности URL: http://www.bytemag.ru/articles/detail.php? ID=8520

3. Сафронов В.В. Современные биометрические методы идентификации.: URL: http://habrahabr.ru/blogs/infosecurity/126144/

4. Попов М., Задорожный В. Биометрические системы безопасности: URL:www.BRE.ru

5. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К.: Изд-во Юниор, 2003. – 504 с.

5 Вимоги до програми

5.1 Вимоги до функціональних характеристик

5.1.1 Програмний додаток призначений для забезпечення захищеного доступу до системи шляхом використання методу дактилоскопії.

5.1.2 Реалізація методу не повинна вимагати спеціальних ліцензійних програмних додатків.

5.1.3 Програмний додаток повинен мати зручний, легкий у розумінні користувача інтерфейс.

5.2 Вимоги до надійності:

5.2.1 Програмний додаток повинен бути працездатним продуктом, функціонувати без помилок.

5.2.2 Програмний додаток повинен працювати без помилок, у випадку виникнення критичних ситуацій необхідно передбачити виведення відповідних повідомлень.

5.4 Вимоги до складу і параметрів технічних засобів:

– оперативна пам'ять – не менше 512 Mb.

5.5 Вимоги до інформаційної та програмної сумісності – будь-яка операційна система.

6 Вимоги до програмної документації

6.1 Обов’язкова поетапна інструкція для майбутніх користувачів, наведена у пункті 3.3

7 Вимоги до технічного захисту інформації

6.1 Необхідно забезпечити контроль до системи на основі біометричної ідентифікації користувачів в додатку.

8 Техніко-економічні показники

7.1 Програмний додаток має бути простим у використанні, легко змінюваним, мати можливість швидкого введення змін.

7.2 Витрати на програмні продукти, що використовуються в ході розробки мають бути мінімальними.

9 Стадії та етапи розробки

№	Назва етапів МКР	Початок	Закінчення
1	Визначення напрямку магістерської роботи, формулювання та затвердження теми	01.09.2021	26.09.2021
2	Аналіз предметної області обраної теми	27.09.2021	05.10.2021
3	Апробація отриманих результатів	06.10.2021	15.10.2021
4	Розробка алгоритму роботи	16.10.2021	31.10.2021
5	Написання магістерської роботи на основі розробленої теми	01.11.2021	14.11.2021
6	Розробка економічної частини	15.11.2020	21.11.2021
7	Передзахист магістерської кваліфікаційної роботи	22.11.2021	25.11.2021
8	Виправлення, уточнення, корегування магістерської кваліфікаційної роботи	26.11.2021	19.12.2021
9	Захист магістерської кваліфікаційної роботи	20.12.2021	21.12.2021

10 Порядок контролю та прийому

10.1 До приймання магістерської кваліфікаційної роботи надається:

– ПЗ до магістерської кваліфікаційної роботи;

– демонстрація результату магістерської кваліфікаційної роботи;

– презентація;

– відзив керівника роботи;

– відзив рецензента.

Технічне завдання до виконання прийняв _____ Безмощук О.В.

Додаток Б. Лістинг (запуск виконуваного файлу)

```
using DetectionAndRecognition;
using System.Windows;

namespace Recognize
{
   public partial class CommonPage : Window
   {
      public CommonPage()
      {
         InitializeComponent();
      }

      private void AboutButton_Click(object sender, RoutedEventArgs e)
      {
         WFAbout wfAbout = new WFAbout();
         wfAbout.ShowDialog();
      }

      private void Login_Click(object sender, RoutedEventArgs e)
      {
         var w = Application.Current.Windows[0];
         w.Hide();

         Login login = new Login();

         login.ShowDialog();
         w.Close();
      }

      private void Exit_Click(object sender, RoutedEventArgs e)
      {
         Login.Visibility = Visibility.Visible;
         Exit.Visibility = Visibility.Hidden;

         AuthUserName.Content = "Не авторизовано";
      }

      private void RichTextBox_TextChanged(object sender,
System.Windows.Controls.TextChangedEventArgs e)
      {

      }
   }
}
```

Додаток В. Лістинг (реєстрація)

```
using DetectionAndRecognition.Context;
using DetectionAndRecognition.Models;
using Microsoft.Win32;
using Newtonsoft.Json;
using PatternRecognition.FingerprintRecognition.Core;
using PatternRecognition.FingerprintRecognition.FeatureExtractors;
using PatternRecognition.FingerprintRecognition.Matchers;
using SpeechEyeRecognize;
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Drawing;
using System.IO;
using System.Linq;
using System.Text;
using System.Timers;
using System.Windows;
using System.Windows.Media;
using System.Windows.Media.Imaging;

namespace FaceDetectionAndRecognition
{
   public partial class Login : Window, INotifyPropertyChanged
   {
      public Login()
      {
         InitializeComponent();
      }
      public string score;
      public string qry;
      public string temp;

      private RecognizeContext _context = new RecognizeContext();
      private string ResourceImage = $"{
Path.GetDirectoryName(AppDomain.CurrentDomain.BaseDirectory)}/ResourceImage";

      #region Properties

      public event PropertyChangedEventHandler PropertyChanged;


      private List<string> nameList = new List<string>();

      private bool active = true;
      private bool enableAutoNavigate = true;
```

```
        private Timer captureTimer;
        private Type type;


        #endregion

        #region CameraCaptureFaceImage


        public void OnLoad()
        {
            if (!Directory.Exists(ResourceImage))
                Directory.CreateDirectory(ResourceImage);

            var path = $"{
Path.GetDirectoryName(AppDomain.CurrentDomain.BaseDirectory)}/ResourceFile.json";

            if (!File.Exists(path))
                File.Create(path);
        }

        private void Window_Loaded(object sender, RoutedEventArgs e)
        {
            OnLoad();
        }
        #endregion

        #region Method

        public enum Type
        {
            Login,
            Registration
        }

        #endregion
        private string RegisterFingerPrint(string personName)
        {

            var extension = Path.GetExtension(pathToFile.Text);
            var newFileName = $"{Guid.NewGuid()}{extension}";
            var resPath = $"{ResourceImage}\\{newFileName}";

            var encoder = new PngBitmapEncoder();

encoder.Frames.Add(BitmapFrame.Create((BitmapSource)fingerPrintImage.Source));
            using (FileStream stream = new FileStream(resPath, FileMode.Create))
                encoder.Save(stream);
```

```
            return newFileName;
        }

        private void Button_Click_1(object sender, RoutedEventArgs e)
        {
            if (type != Type.Registration)
            {
                LoginVoid();
            }
            else
            {
                RegistrationVoid();
            }
        }

        private void RegistrationVoid()
        {
            try
            {
                if (!VerifyData())
                {
                    MessageBox.Show("Не вдала спроба реєстрації");
                    return;
                }

                var fileName = RegisterFingerPrint(UserName.Text);

                var user = new User()
                {
                    UserName = UserName.Text,
                    FingerPrintName = fileName,
                };

                var users = GetUsers();

                if (users == null)
                {
                    users = new List<User>() { user };
                }
                else
                {
                    users.Add(user);
                }
                string json = JsonConvert.SerializeObject(users);
                File.WriteAllText($"{
Path.GetDirectoryName(System.AppDomain.CurrentDomain.BaseDirectory)}/ResourceFile.json",
json);

                var w = Application.Current.Windows[0];
```

```
            w.Hide();
            captureTimer.Stop();

            CommonPage commonpage = new CommonPage();
            commonpage.AuthUserName.Content = user.UserName;
            commonpage.Login.Visibility = Visibility.Hidden;
            commonpage.Exit.Visibility = Visibility.Visible;

            commonpage.ShowDialog();

            MessageBox.Show("Успішно зареєстровано нового користувача");

            w.Close();
        }
        catch (Exception exception)
        {
            Console.WriteLine(exception);
            MessageBox.Show("Не вдала спроба реєстрації");
        }
    }

    private void LoginVoid()
    {
        if (!VerifyData())
            return;

        var user = GetUsers().FirstOrDefault(x => x.UserName == UserName.Text);

        if (user == null)
            MessageBox.Show("Кориистувача не було знайдено");

        var score = Convert.ToDecimal(CompareFingerPrint(user));

        if (score > 60)
        {
            var w = Application.Current.Windows[0];
            w.Hide();

            MessageBox.Show("Спроба входу була вдалою!");

            CommonPage commonpage = new CommonPage();
            commonpage.AuthUserName.Content = user.UserName;

            commonpage.Login.Visibility = Visibility.Hidden;
            commonpage.Exit.Visibility = Visibility.Visible;

            commonpage.ShowDialog();

            captureTimer = null;
```

```
                active = false;
                enableAutoNavigate = false;

                w.Close();
            }
            else
            {
                MessageBox.Show("Спроба входу була не вдалою!");
            }
        }

        private string CompareFingerPrint(User user)
        {
            Change_ResolutionByPath(Path.Combine(ResourceImage, user.FingerPrintName));
            var tempFile = SaveToTempDir();
            Change_ResolutionByPath(tempFile);

            var fingerprintImg1 = ImageLoader.LoadImage(Path.Combine(ResourceImage,
user.FingerPrintName));

            var fingerprintImg2 = ImageLoader.LoadImage(tempFile);

            //// Building feature extractor and extracting features
            var featExtractor = new PNFeatureExtractor() { MtiaExtractor = new
Ratha1995MinutiaeExtractor() };
            var features1 = featExtractor.ExtractFeatures(fingerprintImg1);
            var features2 = featExtractor.ExtractFeatures(fingerprintImg2);

            // Building matcher and matching
            var matcher = new PN();
            double similarity = matcher.Match(features1, features2);
            score = similarity.ToString("0.000");
            System.Windows.Forms.MessageBox.Show(similarity.ToString("0.000"));

            return score;
        }

        private string SaveToTempDir()
        {
            var path = Path.GetTempFileName();
            var encoder = new PngBitmapEncoder();

encoder.Frames.Add(BitmapFrame.Create((BitmapSource)fingerPrintImage.Source));
            using (FileStream stream = new FileStream(path, FileMode.Create))
                encoder.Save(stream);

            return path;
        }
```

```
private Bitmap Change_ResolutionByPath(string file)
{
   using (Bitmap bitmap = (Bitmap)Image.FromFile(file))
   {
      using (Bitmap newBitmap = new Bitmap(bitmap))
      {
         newBitmap.SetResolution(500, 500);
         return newBitmap;
      }
   }
}
private void Change_ResolutionImage()
{
   var source = (BitmapSource)fingerPrintImage.Source;
   var bitmap = new TransformedBitmap(source,
      new ScaleTransform(
         500 / source.PixelWidth,
         500 / source.PixelHeight));
}
```

Додаток Г. Лістинг (авторизація)

```
private bool VerifyData()
{
   if (String.IsNullOrEmpty(UserName.Text))
   {
      MessageBox.Show("Введіть логін");
      return false;
   }
   if (fingerPrintImage.Source == null)
   {
      MessageBox.Show("Необхвдно прикріпити зразок відбитка пальця");
      return false;
   }

   return true;
}

private void Auth_OnClosed(object sender, EventArgs e)
{

}

private void Button_Click(object sender, RoutedEventArgs e)
{
   LoginBtn.Background = new SolidColorBrush(Colors.LightGray);
   RegButton.Background = new SolidColorBrush(Colors.White);

   type = Type.Login;
}

private void Button_Click_2(object sender, RoutedEventArgs e)
{
   RegButton.Background = new SolidColorBrush(Colors.LightGray);
   LoginBtn.Background = new SolidColorBrush(Colors.White);

   type = Type.Registration;
}

private List<User> GetUsers()
{
   List<User> users = new List<User>();

   var path = $"{
Path.GetDirectoryName(AppDomain.CurrentDomain.BaseDirectory)}/ResourceFile.json";

   using (var fs = new FileStream(path, FileMode.Open, FileAccess.Read,
FileShare.ReadWrite))
```

```
            using (var sr = new StreamReader(fs, Encoding.Default))
            {

                string json = sr.ReadToEnd();
                users = JsonConvert.DeserializeObject<List<User>>(json);
            }

            return users;
        }

        private void Button_Click_3(object sender, RoutedEventArgs e)
        {
            OpenFileDialog dlg = new OpenFileDialog();
            //   dlg.InitialDirectory = "c:\\";
            //   dlg.Filter = "Image files (*.jpg)|*.jpg|All Files (*.*)|*.*";
            dlg.RestoreDirectory = true;

            if (dlg.ShowDialog() == true)
            {
                string selectedFileName = dlg.FileName;
                pathToFile.Text = selectedFileName;
                BitmapImage bitmap = new BitmapImage();
                bitmap.BeginInit();
                bitmap.UriSource = new Uri(selectedFileName);
                bitmap.EndInit();
                fingerPrintImage.Source = bitmap;
            }

        }
    }
}
```

Додаток Д. Інтерфейс додатку

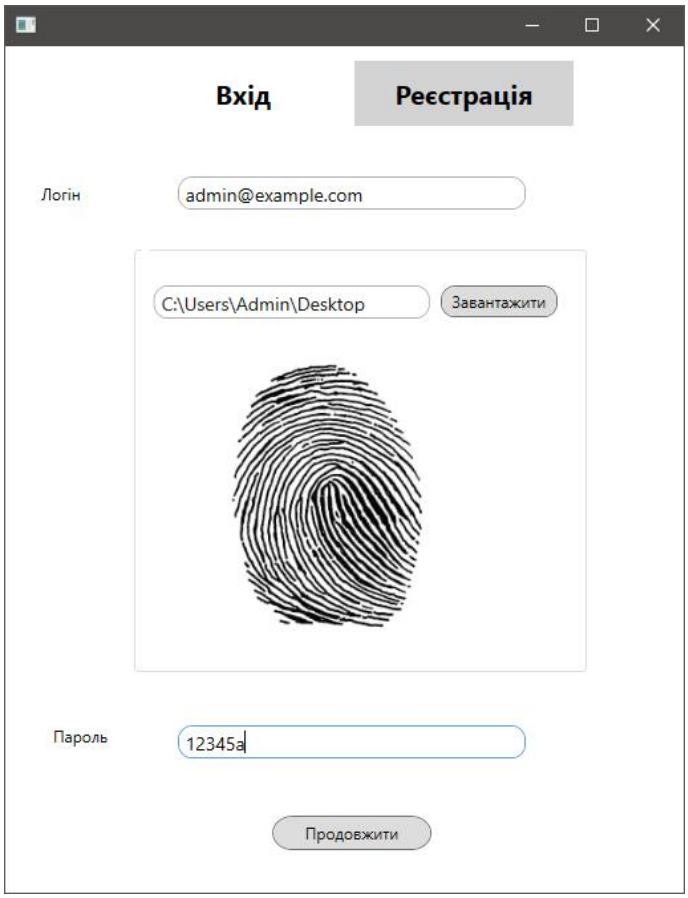


Рисунок 1 – Вигляд вікна реєстрації / авторизації в системі

Рисунок 2 – Вигляд вікна додатку неавторизованого користувача

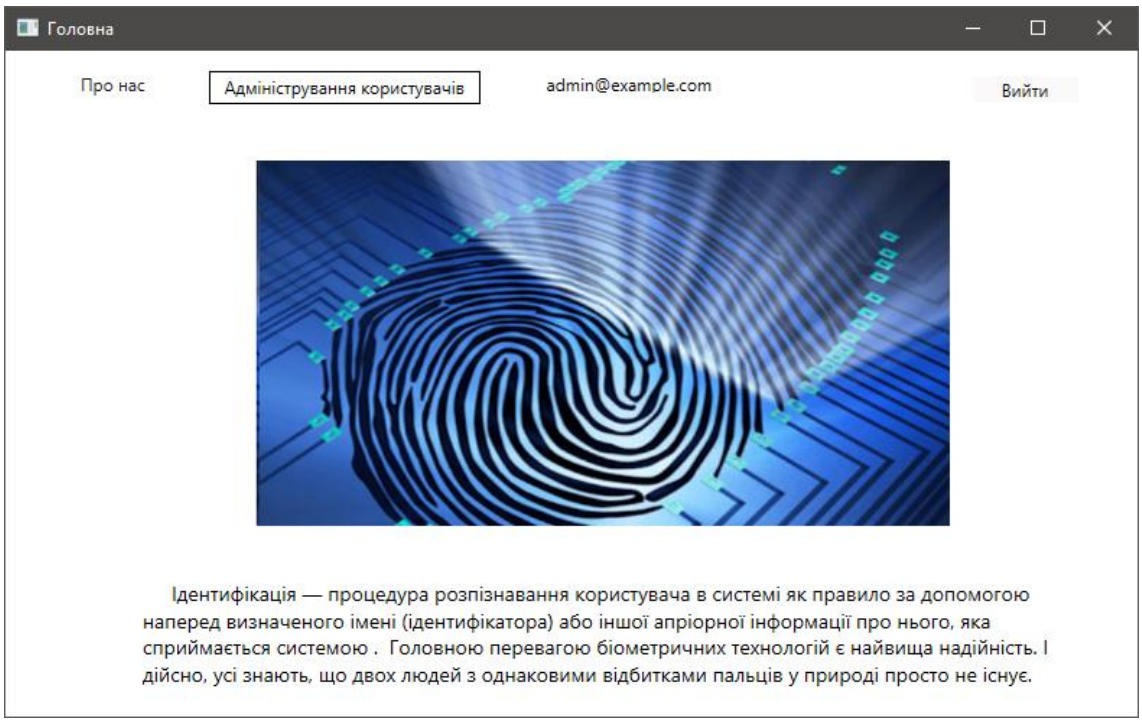


Рисунок 3 – Вигляд вікна додатку авторизованого адміністратора

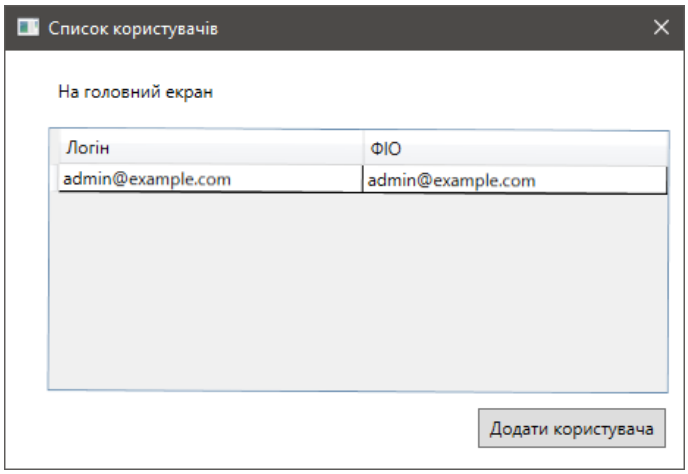


Рисунок 4 – Вигляд вікна списку корисутвачів системи

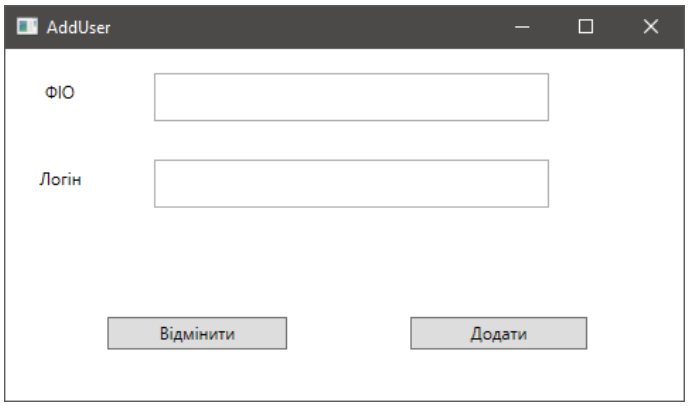


Рисунок 5 – Вигляд вікна додавання нового корисутвача

Додаток Е. Ілюстративний матеріал

Підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії

Виконала ст. гр. УБ – 20м Безмощук О.В.
Керівник проф. каф. МБІС Азарова А.О.

Актуальність:

- Із розвитком сучасних ІТ доступ до системи з використанням біометричного методу дактилоскопії для ідентифікації користувачів стає все більш поширеним. Разом із тим, деякі методи дактилоскопії мають недоліки, що полягають, зокрема, у недостатній точності. Такі проблеми методу зумовлюють актуальність застосування оператора Собеля при реалізації біометричної ідентифікації методу дактилоскопії з метою підвищення достовірності ідентифікації користувачів.

Новизна роботи:

- Наукова новизна дослідження полягає в удосконаленні методу розпізнавання відбитку пальця, що, на відміну від існуючих підходів, дозволяє підвищити точність розпізнавання відбитків пальців, використовуючи метод дактилоскопії на основі оператора Собеля.

Біометричні засоби захисту інформації

- Типові системи автентифікації за сучасних умов не завжди задовольняють вимогам політики інформаційної безпеки підприємства чи компанії, які до них висувають. Саме тому все більшої популярності набирає біометрична автентифікація користувача, що дозволяє автентифікувати користувача за допомогою зчитування його фізіологічних даних.

Оператор Собеля

- Ідея методу Собеля полягає у накладенні на кожну точку зображення двох масок обертання. Ці маски є двома ортогональними матрицями, розмір-ністю 3x3.
- Для вирішення питання інваріантності щодо повороту використовуються так звані діагональні маски, призначені виявлення розривів у діагональних напрямах.

-1	0	+1
-2	0	+2
-1	0	+1

+1	+2	+1
0	0	0
-1	-2	-1

+1	0	-1
+2	0	-2
+1	0	-1

-1	-2	-1
0	0	0
+1	+2	+1

Маски Собеля (вертикальна, горизонтальна)

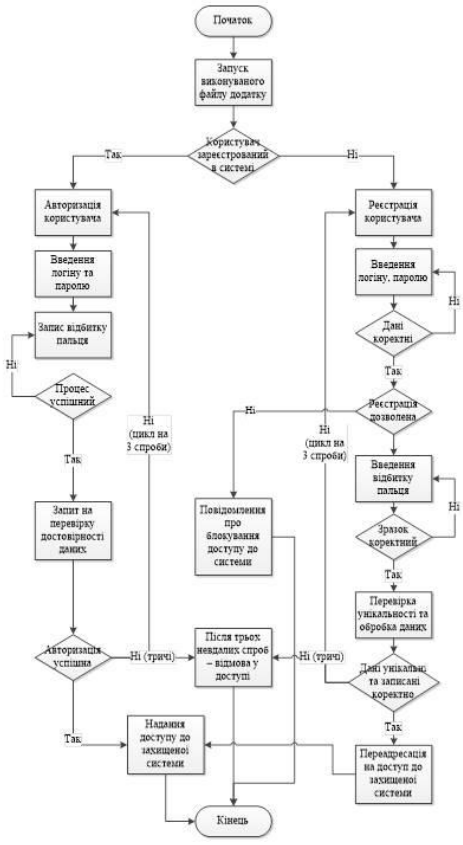
0	+1	+2
-1	0	+1
-2	-1	-0

2	+1	0
+1	0	-1
0	-1	-2

Маски Собеля (діагональні)

Алгоритм розпізнавання відбитка пальця

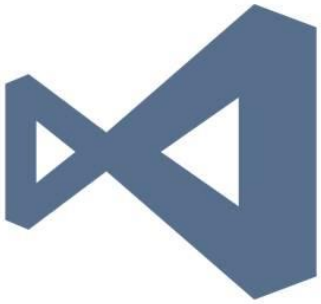
Блок – схема алгоритму роботи додатку



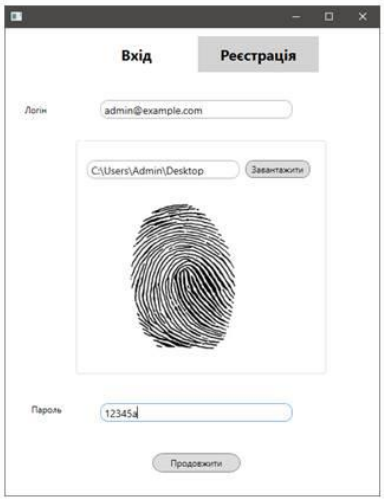
Мова програмування та середовище розробки

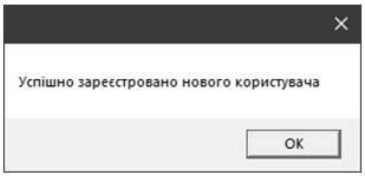
Враховуючи особливості та задачі обраної теми, для програмної реалізації було обрано такі засоби програмування:

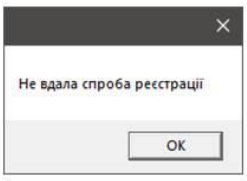
- мова об'єктно-орієнтованого програмування C#;
- середовище програмування Visual Studio.



Користувацький інтерфейс







Авторизація / реєстрація користувача

Користувацький інтерфейс

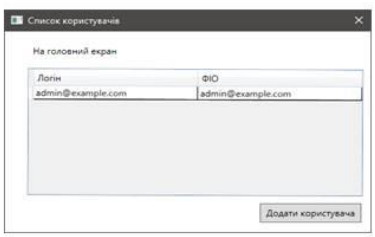
Інформаційне вікно

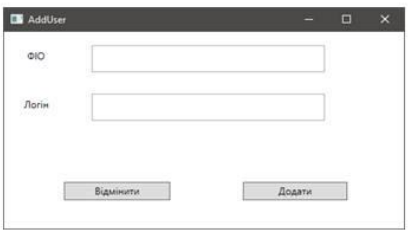
Вікно додатку авторизованого користувача (зверху)

Вікно додатку не авторизованого користувача (внизу)

Користувацький інтерфейс

Авторизація адміністратора. Додавання адміністратором нового користувача.

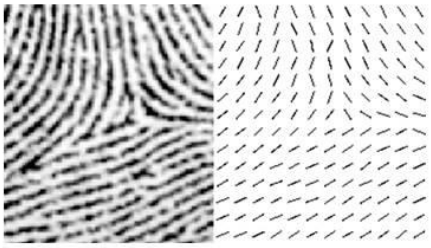




Тестування роботи

Вигляд відбитка пальця (початковий та нормалізований рисунок)

Вигляд відбитка пальця (початковий та нормалізований рисунок)



Частина полів напрямку для окремого рисунка відбитка пальця

Приклад нормалізованого та бінарного зображення після оброблення

Результати роботи

- У магістерській дипломній роботі розроблялася система для підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії з використанням оператора Собеля.
- На базі запропонованого методу було розроблено відповідний програмний продукт, що може використовуватися разом із методом ідентифікації користувачів на основі зчитування образу обличчя. Таке комплексне застосування надає можливість системі захисту точніше аналізувати та розпізнавати користувачів, що, відповідно, підвищує її надійність.

Дякую за увагу!

Додаток Ж. Протокол перевірки

ПРОТОКОЛ ПЕРЕВІРКИ НАВЧАЛЬНОЇ (КВАЛІФІКАЦІЙНОЇ) РОБОТИ

Назва роботи: Підвищення достовірності ідентифікації користувачів з використанням удосконаленого методу дактилоскопії
Тип роботи: Магістерська кваліфікаційна робота
Підрозділ: Факультет МІБ, кафедра менеджменту та безпеки інформаційних систем,
гр. УБ-20м
Науковий керівник Азарова А.О., професор кафедри МБІС, доцент, к.т.н.

Показники звіту подібності

Plagiat.pl (StrikePlagiarism)		Unicheck	
КП1			
КП2		Оригінальність	90 %
Тривога/Білі знаки	/	Схожість	10 %

Аналіз звіту подібності (відмінити подібне)

- ☐ Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.
- ☐ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.
- ☐ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений(-на) з повним звітом подібності, який був згенерований Системою щодо роботи (додається)

Автор _____ Безмощук О.В.
(підпис) (прізвище, ініціали)

Опис прийнятого рішення

Ступінь оригінальності роботи відповідає вимогам, що висуваються до МКР
Особа, відповідальна за перевірку_____ Коваль Н.П.
(підпис) (прізвище, ініціали)

Експерт _____ _____
(за потреби) (підпис) (прізвище, ініціали)