Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедрою
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційна робота

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Системи безпечного доступу на основі біометричних даних»

Виконавець: студент IV курсу, групи КБ-41

_____ **Софія ГАММА**
(підпис) (ім'я, прізвище)

	Підпис	**Прізвище, ініціали**
Керівник		Микола БРАЇЛОВСЬКИЙ
Нормоконтроль		Олександр ЛУКАШОВ

Київ 2025

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедрою
кібербезпеки та захисту
інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-41** (група) **Гаммі Софії Валеріївні** (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Системи безпечного доступу на основі біометричних даних

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол № 6 від «28».11.2024р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Архітектура та принцип дії біометричних систем аутентифікації, методи ідентифікації за анатомічними ознаками.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Теоретичні основи біометричної аутентифікації та класифікація методів, фізіологічне підґрунтя, переваги, обмеження венозної біометрії, проблеми впровадження, обґрунтування технічних удосконалень покращення системи зчитування, математичне обґрунтування, конструктивні особливості монтажної схеми, напрями впровадження модернізованої системи рекомендації.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність застосування технічних рішень для вдосконалення існуючої системи біометричної автентифікації, орієнтованого на потреби в умовах обмеженого бюджету.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: «29» листопада 2024 року

Завдання видав		Микола БРАІЛОВСЬКИЙ
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання		Софія ГАММА
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 27.12.2025	*виконано*
2	Аналіз літератури	03.01.2025 – 24.01.2025	*виконано*
3	Аналіз теоретичних основ біометричної автентифікації	27.01.2025 – 10.02.2025	*виконано*
4	Аналіз проблем реалізації венозної біометрії	11.02.2025 – 25.02.2025	*виконано*
5	Вибір базової моделі та оцінка її технічних характеристик	26.02.2025 – 12.03.2025	*виконано*
6	Розробка технічного рішення для покращення біометричного сканера	13.03.2025 – 25.04.2025	*виконано*
7	Реалізація оновленої моделі, проєктування монтажної схеми	28.04.2025 – 05.05.2025	*виконано*
8	Оцінка точності, надійності та енергоспоживання	06.05.2025 – 20.05.2025	*виконано*
9	Формулювання загальних висновків щодо застосування вдосконаленої системи	21.05.2025 – 04.06.2025	*виконано*
10	Оформлення пояснювальної записки	05.06.2025 – 08.06.2025	*виконано*
11	Підготовка до захисту	09.06.2025 – 13.06.2025	*виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Софія ГАММА
(підпис) (ініціали, прізвище)

Термін подання кваліфікаційної роботи до ЕК «13» червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 68 сторінок основного тексту, 5 таблиць та 9 рисунків. Список використаних джерел містить 31 найменування і займає 3 сторінки.

Метою роботи є покращення системи безпечного доступу з використанням венозної біометрії, як засобу ідентифікації особи.

Для досягнення поставленої мети у кваліфікаційній роботі передбачено виконання таких основних завдань:

- здійснити аналіз сучасного стану розвитку біометричних технологій автентифікації, з особливим акцентом на системи, що базуються на використанні венозного малюнка як фізіологічного ідентифікатора;
- розглянути анатомо-фізіологічні особливості венозної мережі долоні людини;
- провести порівняльний аналіз венозної біометрії з іншими видами біометричної автентифікації (зокрема, за відбитками пальців, райдужною оболонкою ока, обличчям) за критеріями точності, надійності, захищеності та зручності використання;
- проаналізувати технічні характеристики існуючого зразка сканера венозного малюнка, виявити його функціональні обмеження, можливі похибки зчитування, рівень чутливості до зовнішніх факторів, швидкість обробки даних, габаритні особливості та енергоспоживання;
- визначити та обґрунтувати напрямки вдосконалення функціональних характеристик пристрою, зокрема підвищення якості зображення, покращення стійкості до зовнішніх впливів (освітлення, положення кисті), оптимізація продуктивності та сумісності з іншими системами безпеки;
- запропонувати інженерне рішення, спрямоване на модернізацію сканера, з урахуванням сучасних тенденцій в області біометрії, енергоефективності, мініатюризації та інформаційної безпеки;

- розробити прототип вдосконаленого сканера венозної біометрії, а також здійснити попередню оцінку ефективності запропонованих рішень на основі порівняльного аналізу.

Об'єктом дослідження є процес аналізу, покращення та впровадження систем венозної біометрії.

Предметом дослідження є біометричні системи автентифікації, зокрема ті, що базуються на венозному малюнку долоні як фізіологічному ідентифікаторі.

Практичною цінністю отриманих результатів є можливість застосування розроблених технічних рішень для вдосконалення існуючої системи біометричної автентифікації на основі венозного малюнка.

Ключові слова: біометрія, венозний малюнок долоні, автентифікація, контроль доступу, інформаційна безпека, інфрачервоне сканування, шаблон біометрії, кіберзагрози.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

3D	−	3-dimensional – тривимірний;
ABS-пластик	−	термопластичний листовий конструкційний матеріал;
API	−	Application Programming Interface – прикладний програмний інтерфейс;
ASIFT	−	Affine Scale-Invariant Feature Transformation – афінне масштабно-інваріантне перетворення ознак;
CCD	−	Charge Couple Device – пристрій із зарядовим зв’язком;
CMOS	−	Complementary Metal-Oxide-Semiconductor – комплементарний метал-оксид-напівпровідник;
CNN	−	Convolutional Neural Network – згорткові нейронні мережі;
DLP	−	Digital Light Processing – цифрова обробка світла;
EMC	−	Enhanced Maximum Curvature – покращена максимальна кривизна;
FAR	−	False Accept Rate −рівень помилкового прийняття;
FRR	−	False Rejection Rate – рівень помилкового відхилення;
GDPR	−	General Data Protection Regulation – загальний регламент про захист даних;
IEEE	−	Institute of Electrical and Electronics Engineers – Інститут інженерів з електротехніки та електроніки;
ISO/IEC	−	Міжнародної Організації зі Стандартизації (ISO) та Міжнародної Електротехнічної Комісії (IEC);
NIR	−	Near Infrared – ближній Інфрачервоний;
NoIR	−	No Infrared filter − без інфрачервоного фільтра;
OLED	−	Organic Light-Emitting Diode − органічний світлодіод;
OpenCV	−	Open Source Computer Vision Library − бібліотека комп'ютерного зору з відкритим кодом;
OSDP	−	Open Supervised Device Protocol – протокол для комунікації між контролюючими пристроями та системами безпеки;
PCA	−	Principal Component Analysis – аналіз головних компонент;

PIN	−	Personal Identification Number – персональний ідентифікаційний номер;
PLA-пластик	−	біорозкладний термопластичний поліефір;
RFID	−	Radio Frequency Identification − радіочастотна ідентифікація;
SDK	−	Software Development Kit − комплект для розробки програмного забезпечення;
SIFT	−	Scale-Invariant Feature Transform − масштабно-інваріантне перетворення ознак;
SURF	−	Speeded Up Robust Features − прискорені стійкі ознаки;
USB	−	Universal Serial Bus − універсальна послідовна шина;
ДНК	−	дезоксирибонуклеїнова кислота;
ІТ	−	інформаційні технології;
ІЧ	−	інфрачервоне випромінювання;
НСД	−	несанкціонований доступ;
ПЗ	−	програмне забезпечення;
РК-дисплей	−	рідкокристалічний дисплей;
СКУД	−	система контролю і управління доступом.

ВСТУП

Актуальність. В сучасних умовах стрімкого розвитку інформаційних технологій та зростання обсягів оброблюваних даних особливого значення набувають питання забезпечення безпеки доступу до інформаційних ресурсів. Одним з найбільш перспективних напрямів у цій сфері є системи безпечного доступу на основі біометричних даних, які використовують унікальні фізіологічні або поведінкові характеристики користувачів для аутентифікації. Аналіз вітчизняної та зарубіжної науково-технічної літератури, монографії, статей, матеріалів конференцій і патентів свідчить про активний розвиток біометричних технологій у світі. Провідні фірми та наукові компанії розробляють та впроваджують різні методи біометричної ідентифікації, такі як розпізнавання відбитків пальців, райдужної оболонки ока, голосу, обличчя. Водночас існують невирішені проблеми, пов'язані з підвищенням точності, швидкості розпізнавання, захистом від спроб підробки та інтеграцією біометричних систем у сучасну інфраструктуру інформаційної безпеки. Особливо це важливо для України, де зростають потреби у захисті державних, комерційних і персональних даних у контексті кіберзагроз і розширення цифрових сервісів.

Сучасні системи аутентифікації базуються переважно на традиційних методах, таких як паролі, PIN-коди або смарт-карти. Однак і засоби мають суттєві обмеження і вразливості: паролі легко піддаються злому або викраденню, смарт-картки можуть бути втрачені чи підроблені. У зв’язку з цим біометричні системи доступу набувають все більшої популярності, оскільки вони забезпечують більш надійну ідентифікацію, що базується на індивідуальних, важкопідробних характеристиках людини. При цьому, розвиток обчислювальних потужностей та алгоритмів машинного навчання відкриває нові можливості для підвищення ефективності біометричних технологій.

Вітчизняні дослідники та розробники також активно працюють над удосконаленням біометричних систем, але на українському ринку ще бракує

комплексних рішень, адаптованих до умов і вимог інформаційної безпеки. Враховуючи зростання кількості кіберзагроз, зокрема спрямованих на державні установи, банківські структури, телекомунікаційні компанії, впровадження надійних біометричних систем контролю доступу є нагальною необхідністю. Окрім того, цифровізація послуг, впровадження електронного урядування та електронного документообігу вимагають високого рівня захисту ідентифікації користувачів для запобігання шахрайству і несанкціонованому доступу. Впровадження біометричних технологій створює нові виклики, пов’язані з юридичним регулюванням, етичним аспектами, захистом персональних даних та прав користувачів. У зв’язку з цим актуальними є дослідження, спрямовані не лише на технічне вдосконалення систем, але й на формування відповідної нормативної та організаційної бази для їх ефективного й безпечного використання.

Метою кваліфікаційної роботи є покращення системи безпечного доступу з використанням венозної біометрії, як засобу ідентифікації особи.

Для досягнення поставленої мети у кваліфікаційній роботі передбачено виконання таких основних завдань:

- здійснити аналіз сучасного стану розвитку біометричних технологій автентифікації, з особливим акцентом на системи, що базуються на використанні венозного малюнка як фізіологічного ідентифікатора;
- розглянути анатомо-фізіологічні особливості венозної мережі долоні людини;
- провести порівняльний аналіз венозної біометрії з іншими видами біометричної автентифікації (зокрема, за відбитками пальців, райдужною оболонкою ока, обличчям) за критеріями точності, надійності, захищеності та зручності використання;
- проаналізувати технічні характеристики існуючого зразка сканера венозного малюнка, виявити його функціональні обмеження, можливі похибки зчитування, рівень чутливості до зовнішніх факторів, швидкість обробки даних, габаритні особливості та енергоспоживання;

- визначити та обґрунтувати напрямки вдосконалення функціональних характеристик пристрою, зокрема підвищення якості зображення, покращення стійкості до зовнішніх впливів (освітлення, положення кисті), оптимізація продуктивності та сумісності з іншими системами безпеки;
- запропонувати інженерне рішення, спрямоване на модернізацію сканера, з урахуванням сучасних тенденцій в області біометрії, енергоефективності, мініатюризації та інформаційної безпеки;
- розробити прототип вдосконаленого сканера венозної біометрії, а також здійснити попередню оцінку ефективності запропонованих рішень на основі порівняльного аналізу.

Об’єкт дослідження: процес аналізу, покращення та впровадження систем венозної біометрії.

Предмет дослідження: біометричні системи автентифікації, зокрема ті, що базуються на венозному малюнку долоні як фізіологічному ідентифікаторі.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. Біометричні технології, зокрема системи ідентифікації за венозним малюнком долоні, стрімко розвиваються як у науковому, так і в прикладному аспектах. За останнє десятиріччя спостерігається зростаючий інтерес до венозної біометрії через її складність підробки та високу точність при ідентифікації особи. У зарубіжній науковій літератури особливу увагу приділено дослідженням надійності та ефективності розпізнавання венозного малюнка в умовах змінного середовища. Так, у роботі Wang, Li та Zhang (2023) [1] розглядаються новітні глибокі нейронні мережі, адаптовані до змін освітлення, температури шкіри та інших факторів, що впливають на якість зображення вен. Особливої актуальності набувають дослідження впливу фізіологічних змін на результати біометричної ідентифікації. Lee, Kim і Park (2024) [2] дослідили методи компенсації варіації кровотоку, температури тіла та інших біологічних чинників, які можуть знижувати точність ідентифікації. Подібні дослідження підтверджують необхідність адаптивних систем, здатних

враховувати змінні параметри людського організму. Практичні аспекти реалізації технології розкривається у роботах Aratek (2023) [3] та компаній на ринку, таких як Hitachi (PalmSecure) [4] і CardPlus [5], які описують технічні складності інтеграції біометричного обладнання у вже наявну IT-інфраструктуру. Зокрема, увагу звернено на потребі стандартизації протоколів, уніфікації апаратних рішень і забезпечення сумісності з системами захисту персональних даних. Демонструє високу точність підхід, що поєднує текстурну ознаки з CNN-архітектурами та представлений у роботі Babalola, Bitirim та Toygar [6]. Біометрія часто використовується як інструмент соціального контролю, що викликає занепокоєння щодо приватності та прав людини, особливо у вразливих груп населення, наголошується у статті Mirca Madianou «The Biometric Assemblage».

На вітчизняному рівні також відзначається зростання інтересу до венозної біометрії. У колективній монографії «Біометричні технології в XXI столітті» (Львів,2015) [7] аналізується досвід використання таких систем у правоохоронних органах України, зокрема під час ідентифікації особи за відбитками руки або в процесі контролю доступу до інформативних ресурсів. Вказується на потребу створення єдиної нормативно-правової бази для регулювання зборку, зберігання та обробки біометричних даних.

Галузь застосування**.** Покращений апаратний модуль для біометричної ідентифікації на основі венозного малюнка долоні може застосовуватися у сфері інформаційної безпеки для забезпечення контролю доступу до об’єктів з підвищеними вимогами до автентифікації.

Новизна. Проведено вдосконалення низьковартісного біометричного сканера венозного малюнка долоні, орієнтованого на потреби в умовах обмеженого бюджету.

Практичною цінністю отриманих результатів є можливість застосування розроблених технічних рішень для вдосконалення існуючої системи біометричної автентифікації на основі венозного малюнка.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ВЕНОЗНОЇ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

1.1 Біометричні системи автентифікації: класифікація, принципи функціонування та сфери застосування.

Термін «біометрія» походить від грецьких слів «bios» - життя та «metron» - вимірювання, що буквально означає «вимірювання життя». Біометрична система — це автоматизована система, що забезпечує процес реєстрації користувачів та їх верифікацію за допомогою біометричних даних.

Біометричні технології являють собою сукупність автоматизованих методів і засобів ідентифікації/верифікації людини, що можуть бути засновані на поведінкових або фізіологічних її характеристиках. До статичних методів (фізіологічних характеристик) можна віднести відбиток пальця, форма долоні, розташуванням вен на тильній стороні долоні, сітківка ока, райдужка, форма обличчя та інші унікальні особливості тіла людини (наприклад, ДНК). Вони є незмінними або мало змінними з часом та мають виразну індивідуальність. Динамічні методи (поведінкові характеристики) - ґрунтуються на особливостях, що характерні для підсвідомих рухів у процесі відтворення якої-небудь дії. Наприклад, рукописний почерк, динаміка набору кодового слова, голос, рух губ, динаміка повороту ключа в дверному замку тощо. Оптимальна біометрична характеристика повинна характеризуватися простотою збору, універсальністю серед популяції, високим ступенем унікальності для кожного індивіда та стабільністю в часі. Таблиця 1 «Порівняльна характеристика біометричних методів за ключовими ознаками» дозволяє провести порівняльний аналіз біометричних методів ідентифікації за ключовими критеріями, що визначають їхню придатність до використання в системах захисту інформації.

Таблиця 1

Порівняльна характеристика біометричних методів за ключовими ознаками

Метод	**Універсальність**	**Унікальність**	**Сталість**	**Вимірюваність**
Відбиток пальця	+++	+++	+++	+++
Форма долоні	++	++	++	++
Вени на долоні	++	+++	+++	++
Сітківка ока	++	+++	+++	+
Райдужка	++	+++	+++	++
Форма обличчя	+++	++	++	+++
ДНК	+	+++	+++	+
Рукописний почерк	++	++	+	++
Динаміка набору кодового слова	++	++	+	++
Голос	+++	++	+	+++
Рух губ	++	++	+	++

Найбільш збалансованим і практично доцільним методом є ідентифікація за відбитком пальця — вона поєднує високу унікальність, сталість, універсальність та вимірюваність, що робить її придатною для захищених, але доступних систем. Методи, засновані на ДНК або сітківці ока, мають високу точність, проте обмежену вимірюваність, що стримує їх використання в широких масштабах. Поведінкові методи демонструють нижчу сталість і більше піддаються впливу зовнішніх умов, тому мають допоміжний характер у багатофакторній аутентифікації.

Вибираючи спосіб аутентифікації, важливо враховувати кілька основних факторів: цінність інформації, що визначає важливість захисту даних, зважаючи на рівень конфіденційності та можливі наслідки витоку інформації; вартість програмно-апаратного забезпечення аутентифікації, що включає витрати на впровадження та обслуговування технологій аутентифікації, зокрема придбання відповідних засобів та ліцензій; продуктивність системи, яка враховує необхідність забезпечення високої швидкості та ефективності обробки запитів користувачів без значних затримок у роботі системи; відношення користувачів

до аутентифікації, що включає зручність використання для кінцевих користувачів, а також рівень їх довіри до обраної технології; специфіка (призначення) інформаційної системи, що зумовлює вибір методу аутентифікації, враховуючи характер даних, що обробляються, та особливості функціонування самої системи.

Принцип біометричного розпізнавання однаковий для всіх систем та включає в себе функції персоналізації/реєстрації користувачів в системі, фіксації біометрично релевантних характеристик осіб, створення наборів даних, так званих шаблонів, а також порівняння найновіших даних з раніше збереженими даними. Типова біометрична система складається з кількох ключових компонентів:

1. Сенсор для зчитування даних — це пристрій, який здійснює початковий етап збору інформації. Наприклад, це може бути сканер відбитків пальців, камера для зчитування райдужної оболонки ока або мікрофон для запису голосу;
2. Програмне забезпечення для обробки та аналізу — спеціалізовані алгоритми, які перетворюють отриману інформацію у цифровий формат, виділяють унікальні характеристики (наприклад, особливості малюнка відбитка пальця або голосу) і готують ці дані для порівняння з іншими;
3. База даних шаблонів — це сховище, де зберігаються біометричні дані (так звані шаблони), створені на основі попередніх зчитувань. Всі нові дані, зібрані системою, будуть порівнюватися саме з цими шаблонами для подальшої перевірки;
4. Система ухвалення рішень — програмний модуль, що здійснює порівняння отриманих даних із шаблонами в базі даних. Він визначає, наскільки точно нові зчитані дані співпадають з наявними шаблонами, що дозволяє здійснити ідентифікацію чи автентифікацію особи.

Збір біометричних даних відбувається на двох етапах: спочатку під час створення бази даних, коли система фіксує біометричні характеристики (наприклад, відбитки пальців або риси обличчя), а потім, коли ці дані використовуються для подальшого розпізнавання. Для цього можуть

використовуватись різні сенсори, зокрема камери (для розпізнавання обличчя), мікрофони (для розпізнавання голосу), клавіатури (для аналізу особливостей набору тексту), датчики тиску (для ідентифікації по малюнку відбитків пальців), сенсори запаху або інші спеціалізовані пристрої. Для захоплення особи в біометричній системі спочатку створюється та записується зображення оригінальної характеристики, яке є сирими даними в процесі. Наступним кроком застосовується алгоритм — зазвичай специфічний для виробника — для перетворення оригінального зображення в набір даних, що називається шаблоном. Шаблон формується шляхом обробки інформації, отриманої під час первинного зчитування біометричної ознаки. У деяких випадках для забезпечення більшої точності зберігається не узагальнений шаблон, а саме вихідне зображення, яке використовується як еталон. Під час автентифікації новий зразок зіставляється з раніше зафіксованим еталоном, що дозволяє визначити збіг та підтвердити особу. Якщо є співпадіння, пристрій підтверджує, що користувача було розпізнано. Однак процес захоплення, оцінки та порівняння біометричних характеристик підлягає помилкам вимірювання, оскільки характеристики можуть змінюватися з часом. Це можуть бути природні зміни, як наприклад зміни, пов'язані з віком, а також зовнішні впливи, такі як травми чи захворювання. Крім того, зовнішні зміни в зовнішньому вигляді, такі як зміни волосся (стиль зачіски, борода), носіння окулярів, контактних лінз або зміни в косметиці, також можуть вплинути. Окрім цього, користувачі не завжди подають характеристику в однаковий спосіб. Наприклад, положення пальця на датчику відбитків пальців або кут обличчя може трохи змінюватися під час кожного використання. Це означає, що два цифрових зображення біометричної характеристики ніколи не будуть абсолютно однаковими.

Біометричні характеристики є притаманними кожній людині, що робить біометричну ідентифікацію особливо важливою для представників окремих соціальних та демографічних груп — зокрема дітей, осіб літнього віку, людей з порушеннями зору або слуху, а також для тих, хто має труднощі з читанням і

письмом. У багатьох випадках для таких осіб біометричні технології стають не лише зручним, але й чи не єдиним способом засвідчення особи або підтвердження її ідентичності. Поряд із біометрією, у системах ідентифікації також застосовують смарт-карти та токени — спеціальні пристрої або носії з вбудованими мікрочіпами. У більшості країн такі технології активно впроваджуються в офіційні документи, які підтверджують особу, — закордонні паспорти, посвідчення, ID-картки тощо. Замість звичних паперових документів дедалі частіше використовують електронні аналоги з вбудованими модулями, що підтримують шифрування, електронний підпис, штрих-коди, RFID-технології та біометричну ідентифікацію. В Україні прикладами таких новітніх засобів є біометричні паспорти, банківські картки нового зразка та електронні перепустки на об’єкти з підвищеним рівнем безпеки. Біометричні системи використовуються у таких випадках, як:

- проходження паспортного та прикордонного контролю;
- підтвердження спеціального статусу або професійних повноважень (водійські права, посвідчення моряка, студентський квиток, тощо);
- звернення до систем медичного, соціального забезпечення та страхування;
- доступ до культурних і наукових установ;
- участь у виборах, референдумах та інших формах волевиявлення;
- взаємодія з органами державної влади, включно з електронним урядуванням;
- користування фінансовими послугами, програмами лояльності, транспортними сервісами тощо.

Сьогодні безпеку даних забезпечують різні засоби: шифрування, одноразові паролі, електронні підписи та цифрові сертифікати. Але найвищий рівень надійності досягається тоді, коли ці технології застосовуються в комплексі з біометричними системами.

1.2 Венозна біометрія як метод автентифікації особи

В останні роки венозний візерунок долоні привернув значну увагу наукової спільноти у сфері біометричних технологій (рис. 1.1).

Рисунок 1.1 - Венозний візерунок долоні

Ця структура являє собою густу мережу вен, що охоплює всю поверхню долоні, по якій кров відтікає від кінчиків пальців у проксимальному напрямку. Частина венозної мережі розташована поверхнево, інша — глибоко в підшкірних тканинах. Саме поверхнево розташовані вени становлять інтерес для ідентифікаційних систем, оскільки можуть бути візуалізовані за допомогою інфрачервоної технології та використані для автентифікації особи. Протягом останнього десятиліття венозний малюнок долоні знайшов широке застосування у системах безпечного доступу. Ефективність цієї біометричної характеристики як засобу індивідуального розпізнавання підтверджена в численних дослідженнях, які демонструють її порівнювану точність із уже впровадженою технологією ідентифікації за венами пальців.

Водночас особливістю венозного малюнка долоні є його велика площа покриття, що вимагає відповідних технічних характеристик зчитувальних пристроїв — зокрема, широкоформатних сенсорів. У випадках мініатюрності обладнання існує ймовірність того, що пристрій не зможе охопити всю анатомічну область долоні за один сеанс сканування, що вплине на точність розпізнавання. Інші судинні біометричні технології, зокрема ідентифікація за венами пальців, демонструють співставну ефективність з традиційними

біометричними методами — такими як відбитки пальців, малюнок долоні та розпізнавання обличчя. Проте венозний малюнок пальця менш щільний і займає значно меншу площу порівняно з венозною сіткою долоні. За орієнтовною оцінкою, розмір малюнка вен пальця становить 0,071 частину площі венозної сітки долоні (рис.1.2-1.3).

Рисунок 1.2 – Венозний малюнок пальця

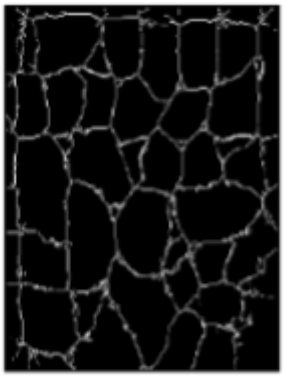

Рисунок 1.3 - Венозна сітка долоні

Оскільки щільність венозного малюнка пальця менша, кількість унікальних ознак, які можна виділити для автентифікації, також є обмеженою, що знижує стійкість до підробок, оскільки при несанкціонованому доступі до частини венозного зображення існує ризик імітації або підміни даних. На противагу цьому, венозна сітка долоні чи її фрагменти містять велику кількість характерних ознак, що робить її більш надійною для ідентифікації особи. При цьому використання часткових зображень дозволяє зменшити розміри сенсорного пристрою, що сприяє підвищенню зручності та поширенню таких систем серед користувачів. Сучасні дослідження у сфері біометричної ідентифікації за венозним малюнком долоні застосовують широкий спектр методів виділення ознак — від традиційних, створених вручну (hand-crafted), до алгоритмів на основі штучних нейронних мереж. Розглянемо наступні методи виділення ознак:

- *Методи, що базуються на венозному малюнку.*

Цей метод спрямований на виокремлення власне венозного шаблону зображення. В аналізі поперечного профілю венозні точки мають нижчу яскравість (сірий рівень) порівняно з оточуючими пікселями, що дозволяє

виявити судинну структуру. Zhang та інші співавтори наукової роботи «Вилучення та зіставлення вен долоні для особистої автентифікації» запропонували використання багатомасштабних узгоджених фільтрів Гауса для покращеного виявлення вен. Однак ефективність цього методу залежить від правильно підібраного масштабу фільтрів, що ускладнює його реалізацію. Ще один метод EMC із застосуванням дескриптора гістограми орієнтованих градієнтів враховує проблеми, пов'язані з варіаціями освітлення, однак точність цього підходу також залежить від ретельного налаштування параметрів. Інші дослідження проводилися з використанням матриць Гессе , що дозволяють аналізувати власні значення зображення без попередньої фільтрації. Метод забезпечує отримання локальної статистичної інформації з текстури венозного малюнка, але за низької якості текстури не може відтворити геометричну структуру вен.

- *Текстурні методи*

Ці методи аналізують текстурні особливості зображення долоні, використовуючи статистичні характеристики, такі як локальні бінарні шаблони та локальні похідні шаблони. Вони виявляють унікальні текстурні патерни, які можуть бути використані для ідентифікації особи. Такі методи досить прості в реалізації та швидкі, але можуть помилково включати неінформативні елементи – зморшки чи лінії долоні – що знижує точність розпізнавання.

- *Методи, інваріантні до локальних змін*

Вони зосереджені на виявленні ключових точок, які залишаються стабільними при зміні масштабу, повороту або освітлення. Для цього застосовуються алгоритми SIFT, SURF або ASIFT. Перевагою є стійкість до змін у положенні руки, проте ці методи є обчислювально складними та вимагають багато ресурсів, що може уповільнити обробку.

- *Субпросторові методи*

Вони проєктують зображення вен у зменшений простір ознак, використовуючи такі техніки, як аналіз головних компонент (PCA), двовимірний PCA або лінійний дискримінантний аналіз. Це дозволяє скоротити

обсяг даних, пришвидшити обробку та зменшити споживання пам’яті. Однак, для ефективного навчання таких моделей необхідна велика кількість навчальних зображень, що не завжди можливо.

- *Методи на основі глибокого навчання*

Ці методи використовують штучні нейронні мережі, переважно згорткові (CNN), які здатні автоматично навчатися й вилучати найважливіші ознаки венозного малюнка. Завдяки цьому забезпечується висока точність розпізнавання, навіть в умовах поганого освітлення чи спотворень. Але ці методи вимагають великої кількості якісних навчальних даних, потужних обчислювальних ресурсів та можуть мати проблеми з перенавчанням або залежністю від якості моделі. Крім того, часто виникає проблема відсутності еталонного набору для верифікації результатів.

У сучасних дослідженнях з біометричної аутентифікації все частіше застосовують комбіновані підходи, які поєднують кілька методів виділення ознак для підвищення точності розпізнавання. У дослідженні [6] використано стратегію об’єднання рішень, поєднавши два різні підходи. Перший підхід базувався на виділенні текстурних ознак з п’яти перекривних підобластей зображення вен долоні. Для цього застосовується метод бінаризованих статистичних ознак зображення, який дозволяє ефективно виявляти унікальні структури в текстурі шкіри. Інший підхід ґрунтувався на згортковій CNN, яка навчається на повному зображенні долоні для виявлення характерних ознак. Після обробки кожного зображення обома методами результати поєднуються, і на їх основі система ухвалює остаточне рішення щодо ідентифікації особи. Такі гібридні методи дозволяють поєднати переваги кожного з підходів і мінімізувати їх недоліки.

1.3 Технічні засоби зчитування венозного малюнка

Базова модель пристрою для візуалізації вен складається з потужного джерела інфрачервоного випромінювання (ІЧ-світлодіода), компактної камери,

чутливої до ІЧ-випромінювання, сенсора для фіксації та форматування зображення, а також фільтра для усунення небажаних світлових перешкод (рис.1.4).

Рисунок 1.4 – Базова модель пристрою для візуалізації вен

У деяких експериментальних моделях конструкцію доповнюють додатковими компонентами для покращення функціональності, зокрема — цифровим проєктором на основі технології DLP, що дозволяє проєкціювати венозний малюнок безпосередньо на поверхню шкіри.

Існують два основні методи освітлення, що застосовуються в пристроях для візуалізації вен: відбите світло та просвічування. У першому випадку інфрачервоне світло від джерела відбивається від поверхні, зокрема долоні, після чого зображення фіксується камерою. Цей принцип найчастіше реалізується у комерційних венозних сканерах. У методі просвічування ІЧ-світло проходить крізь шкірні та підшкірні тканини, а зображення вен формується завдяки присутності дезоксигемоглобіну у венозній крові, який ефективно поглинає червоне світло. Це забезпечує контрастне зображення вен у вигляді темних ліній на тлі оточуючих тканин, що полегшує їхнє виявлення. Отримане зображення обробляється спеціалізованим програмним забезпеченням, яке виділяє венозний малюнок і перетворює його на цифровий шаблон для подальшого порівняння з еталонними даними.

Прикладом пристрою, що застосовує метод відбитого світла, є ManuScan (рис.1.5). Він складається з таких функціональних компонентів: потужного інфрачервоного джерела випромінювання (ІЧ-світлодіодів), ІЧ-камери, чутливої до довжини хвиль у межах 760–940 нм, оптичних фільтрів для усунення паразитного видимого світла, цифрових сенсорів з високою роздільною здатністю, а також процесора або мікроконтролера зі спеціалізованим програмним забезпеченням для обробки зображень. ІЧ-світло випромінюється на поверхню долоні, проходить через тканини руки, частково відбивається або поглинається, після чого формується зображення венозного малюнка. Камера фіксує це зображення, а система програмно обробляє його для порівняння з еталонними біометричними шаблонами.

Рисунок 1.5 - Система ManuScan

У склад пристрою входять інфрачервоні світлодіоди, цифрові сенсори з високою просторовою роздільною здатністю, оптичні фільтри для усунення впливу видимого спектра, мікроконтролер або процесор для обробки даних, а також спеціалізоване ПЗ для побудови та порівняння біометричних шаблонів.
ManuScan реалізується у вигляді зовнішніх і внутрішніх сканерів, які можуть застосовуватись як у складі централізованих систем контролю та управління доступом (СКУД), так і в автономному режимі. Зовнішні модулі встановлюються на вхідних групах до об'єктів, тоді як внутрішні — на входах до окремих приміщень. Усі модулі мають однакове функціональне призначення — здійснення точкової біометричної ідентифікації з метою обмеження несанкціонованого доступу.

У автономному режимі контролер ManuScan здатен здійснювати керування до чотирьох пристроїв (електрозамки, сигналізація тощо) через інтерфейс USB-I/O Box, при цьому обробляючи дані з чотирьох незалежних сканерів. За потреби масштабування, кілька контролерів об’єднуються в єдину мережу, що забезпечує централізований доступ до загальної бази даних та дозволяє проводити реєстрацію нових користувачів лише на одному з елементів системи. Така архітектура забезпечує гнучкість і розширюваність системи без втрати функціональної узгодженості.

У контексті інтеграції до СКУД, кожна сканована позиція долоні (права, ліва або обидві руки) отримує унікальний біометричний ідентифікатор, що дозволяє створювати складні сценарії управління: наприклад, відкриття/закриття дверей, активація охоронної сигналізації або інші керуючі дії, залежно від пред’явленої долоні.

Типовим прикладом пристрою, що реалізує метод просвічування у візуалізації вен, є сканер Veinlite LED+ (рис. 1.6), який використовує кільце світлодіодів для створення бокового світлового потоку, що проникає в підшкірні тканини та формує візуальний контраст між венозними структурами й навколишніми тканинами. Пристрій оснащений 28 світлодіодами: 22 оранжевими для візуалізації поверхневих вен та 6 червоними для покращення видимості глибших судин або вен у пацієнтів із темним кольором шкіри . Користувач може окремо або одночасно активувати ці світлодіоди, що дозволяє адаптувати освітлення до конкретних клінічних потреб.

Рисунок 1.6 - Veinlite LED+

Ергономічна С-подібна форма Veinlite LED+ не лише забезпечує зручне розміщення на шкірі, але й дозволяє механічно натягувати її, стабілізуючи вену та запобігаючи її зміщенню під час венепункції . Це особливо корисно при роботі з пацієнтами, у яких вени важко пальпуються або мають схильність до "скочування".

Технічні характеристики пристрою включають компактні розміри (99 × 57 × 21 мм), малу вагу (приблизно 77 г) та вбудований літій-іонний акумулятор, що забезпечує до 350 хвилин безперервної роботи на одному заряді . Для забезпечення гігієнічності використання передбачені одноразові пластикові накладки, а також додаткові аксесуари, такі як педіатричний адаптер та світловий щиток для роботи в умовах яскравого освітлення.

Veinlite LED+ широко застосовується в різних галузях медицини, включаючи педіатрію, екстрену медицину, онкологію та флебологію. Його використання сприяє зменшенню кількості невдалих спроб венепункції, зниженню рівня больових відчуттів у пацієнтів та скороченню часу, необхідного для проведення внутрішньовенних маніпуляцій. Завдяки поєднанню технологічних інновацій та практичної ефективності, Veinlite LED+ є важливим інструментом у сучасній клінічній практиці.

Розмір глобального ринку сканерів вен долоні, за прогнозами, зросте з 416 мільйонів доларів США у 2020 році до 1,150 мільйонів доларів США до 2025 року, зі середньорічним темпом зростання (CAGR) 22,6% у період з 2020 по 2025 рік. Основними факторами, що сприяють зростанню цього ринку, є переваги сканерів вен долоні порівняно з іншими біометричними технологіями, зростаюча потреба у забезпеченні конфіденційності інформації та даних для організацій, а також стрімке впровадження біометричних систем ідентифікації в сферах фінансових послуг, охорони здоров’я та комерційного сектору. Крім того, розширення підтримки урядів Європи для внутрішніх біометричних технологій у зв’язку з дотриманням вимог GDPR та зростаючі партнерства та колаборації серед постачальників в екосистемі сприяють подальшому розвитку ринку.

До основних компаній входять: Fujitsu Ltd., Hitachi, Ltd., NEC Corporation, M2SYS Technology, BioSec Group Ltd., Recogtech B.V., iDLink Systems Pte Ltd., ePortation, Inc., Mofiria Corporation, BioEnable Technologies, Dakar Software Systems. Вони активно впроваджують різноманітні стратегії розвитку, зокрема шляхом інноваційних розробок, формування партнерських альянсів, укладання угод та співпраці з іншими організаціями. Такий комплексний підхід дозволяє їм не лише зміцнювати свої конкурентні позиції, а й адаптуватися до динамічного ринкового середовища, сприяючи таким чином стійкому розвитку та впровадженню новітніх технологічних рішень у сфері біометрії.

Fujitsu Ltd. є лідером на ринку сканерів вен долоні з 2019 року. Компанія фокусується на розробці та виробництві біометричних систем, зокрема на основі технології розпізнавання вен долоні. Продукти компанії пропонують різноманітні конфігурації, що дозволяють їх застосування в різних сферах.

PalmSecure F-Pro Suit (рис.1.7) - це високопродуктивна лінійка біометричних пристроїв від Fujitsu. Ця серія є результатом еволюції попередніх моделей PalmSecure і надає значні переваги в порівнянні з попередніми поколіннями. Пристрій має висоту всього 13 мм, що є значно менше порівняно з попередніми моделями, що дозволяє легко інтегрувати його в компактні пристрої без втрати функціональності. Завдяки вдосконаленому сенсору, час захоплення зображення значно скорочено, що забезпечує швидку реєстрацію та автентифікацію користувачів, навіть при повільному русі руки.

Рисунок 1.7 - PalmSecure F-Pro Suit

Пристрій здатний працювати в широкому температурному діапазоні від -40°C до +85°C і має підвищену стійкість до сонячного світла, що дозволяє його використання в різних умовах освітлення. Однією з ключових характеристик є можливість автентифікації до 10 000 долонь (що еквівалентно 5 000 особам при реєстрації обох рук), що забезпечує значну гнучкість при впровадженні в масштабні системи. Завдяки своїй високій точності, надійності та здатності до безконтактної біометричної автентифікації, PalmSecure F-Pro Suite знайшла широке застосування в різних галузях.

Сканер вен долоні M2-PalmVein (рис. 1.8) від компанії M2SYS Technology. реалізує безконтактну біометричну ідентифікацію шляхом аналізу унікального малюнка венозної системи внутрішньої частини долоні за допомогою інфрачервоного випромінювання. Роздільна здатність сканера становить 500 dpi, що забезпечує високу точність сканування, а рівень помилкового прийняття не перевищує 0,00008%, тоді як рівень помилкового відхилення є меншим за 0,01%. Такі характеристики дозволяють суттєво знизити ймовірність як несанкціонованого доступу до інформаційних ресурсів або фізичних об’єктів, так і помилкової відмови в доступі авторизованим користувачам, що, у свою чергу, підвищує загальну ефективність системи автентифікації та мінімізує ризики операційних збоїв. Пристрій працює в температурному діапазоні від 0°C до +60°C, а зберігається без втрати працездатності в умовах від –20°C до +70°C, що забезпечує надійність його використання в широкому спектрі операційних середовищ, включаючи критичну інфраструктуру, де стабільність функціонування є ключовим фактором.

Рисунок 1.8 - M2-PalmVein

Інтерфейс підключення через USB 2.0 або 1.1 гарантує швидку передачу даних. Пристрій ефективно функціонує у складі мобільних рішень для польових умов. Однією з ключових переваг цієї технології є її стійкість до зовнішніх пошкоджень шкіри, що унеможливлює зниження точності при наявності шрамів, сухості або інших дерматологічних особливостей.

Сучасний ринок біометричних технологій, зокрема систем, що ґрунтуються на аналізі венозного малюнка долоні, демонструє стійку тенденцію до зростання. Такий розвиток обумовлений зростаючими вимогами до безпеки, гігієнічності та зручності у процесах ідентифікації. Постійні інновації у цій сфері сприяють підвищенню ефективності та адаптивності технологій, що, у свою чергу, сприяє їх широкому впровадженню в критично важливі галузі — від фінансових установ і закладів охорони здоров'я до органів державного управління. У цьому контексті доцільним є комплексний аналіз можливостей, перспектив і викликів, пов'язаних із впровадженням венозної біометрії як одного з найбільш надійних і сучасних засобів автентифікації.

1.4 Переваги та обмеження венозної ідентифікації

Сканування вен долоні є однією з найбільш перспективних біометричних технологій сучасності, що пропонує надійне та безпечне рішення для ідентифікації особи. Унікальність венозного малюнка, сформованого ще до народження, забезпечує надзвичайно високий рівень точності: навіть однояйцеві близнюки мають відмінний візерунок вен, який зберігається незмінним протягом усього життя. Завдяки цьому, технологія демонструє мінімальні показники хибнопозитивних та хибнонегативних результатів, що підтверджено як лабораторними випробуваннями, так і впровадженням у таких секторах, як фінансові установи, медицина та об'єкти з обмеженим доступом.

Суттєвою перевагою венозної ідентифікації є її високий рівень захисту від фальсифікації. Зчитування здійснюється лише за наявності активного кровотоку, що унеможливлює створення штучних копій чи використання підроблених зразків. Крім того, відсутність фізичного контакту під час сканування робить цю технологію більш гігієнічною, особливо в умовах поширення інфекційних захворювань або у клінічних середовищах. Безконтактність також підвищує зручність використання та зменшує зношування обладнання.

Довготривала сталість венозного малюнка знижує потребу в повторній реєстрації користувачів, що оптимізує експлуатаційні витрати в довгостроковій перспективі. Водночас венозні шаблони неможливо зібрати дистанційно без участі користувача, що посилює захист приватності й надає особі більший контроль над власними біометричними даними.

Водночас впровадження цієї технології супроводжується низкою об’єктивних обмежень. Одним із ключових чинників, що стримують широке застосування, є висока вартість обладнання. Сканери вен долоні потребують інфрачервоних сенсорів, спеціалізованих процесорів та програмного забезпечення, що суттєво підвищує початкові витрати, особливо для малих і середніх підприємств. Також слід враховувати фізіологічні чинники, які можуть впливати на ефективність розпізнавання: порушення периферійного кровообігу, підвищення температури тіла або судинні патології здатні ускладнювати процес зчитування.

Ще одним викликом є обмежена сумісність з існуючими системами безпеки. Впровадження венозної біометрії вимагає адаптації або повної модернізації програмного та апаратного забезпечення. Крім того, відсутність уніфікованих міжнародних стандартів для обміну, обробки та зберігання венозних даних створює перешкоди для інтеграції систем різних виробників і знижує гнучкість впровадження в мультисистемні середовища.

Нарешті, незважаючи на високу захищеність шаблонів від несанкціонованого доступу, ризики кібератак залишаються актуальними.

Біометричні дані, на відміну від паролів, не можна змінити у разі їх витоку. Тому питання безпечного зберігання та шифрування таких даних набуває критичного значення у контексті кібербезпеки.

Хоча вважається, що на відміну від багатьох традиційних біометричних методів сканування вен демонструє підвищену стійкість до зовнішніх впливів — таких як волога, забруднення, пошкодження шкіри чи зношення епідермісу, — наразі бракує достатньої кількості незалежних емпіричних досліджень, які б остаточно підтвердили цю тезу. В окремих джерелах зазначається, що технологія працює стабільно навіть у складних виробничих або зовнішніх середовищах, однак інші аналітики звертають увагу на те, що наявність бруду, вологи чи фізичних ушкоджень може негативно впливати на якість сканування й точність розпізнавання. Таким чином, питання реальної стійкості цієї технології до зовнішніх факторів залишається відкритим і потребує додаткових досліджень за різних умов експлуатації.

Висновки за розділом 1

У першому розділі кваліфікаційної роботи було здійснено комплексний теоретичний аналіз біометричних систем автентифікації з акцентом на технології розпізнавання за венозним малюнком долоні. Розглянуто базові поняття біометрії, класифікацію її методів, технічні та анатомо-фізіологічні основи побудови систем ідентифікації, а також проаналізовано сучасні комерційні рішення й технологічні тренди, що визначають перспективи розвитку галузі.

Аналіз існуючих методів автентифікації дозволив виокремити основні критерії, за якими оцінюється ефективність біометричних технологій: унікальність, сталість, вимірюваність, зручність використання, швидкість та безпека. У цьому контексті ідентифікація за венозним малюнком долоні посідає провідне місце завдяки поєднанню високої точності, безконтактності, складності підробки та гігієнічності. Венозний візерунок є унікальним для

кожної особи та стабільним упродовж життя, що дозволяє зменшити потребу в повторній реєстрації користувачів і підвищити довготривалу ефективність систем.

Особливу увагу приділено технічним аспектам реалізації цієї технології, зокрема оптичним системам на основі інфрачервоного випромінювання, типам сенсорів (CCD, CMOS), та способам формування біометричних шаблонів. Встановлено, що інфрачервоне сканування дозволяє виявити малюнок вен без необхідності прямого контакту зі шкірою, що знижує ризик поширення інфекцій та підвищує зручність користування системою в умовах високої прохідності.

Порівняння венозної біометрії з іншими методами (відбитки пальців, райдужка ока, розпізнавання обличчя) виявило низку переваг, таких як: зменшення впливу зовнішніх факторів, підвищена точність при низькому рівні FAR/FRR, а також значна стійкість до шахрайських дій. У той же час, було встановлено, що повністю об’єктивних висновків щодо стійкості технології до впливу факторів довкілля поки що недостатньо через обмежену кількість незалежних досліджень. Деякі джерела вказують на можливі похибки при наявності вологи, забруднення або несприятливих фізіологічних станів (наприклад, поганий кровообіг).

У рамках аналізу комерційних рішень (Fujitsu PalmSecure, M2-PalmVein) встановлено, що сучасні біометричні системи на основі венозної ідентифікації демонструють високу адаптивність до різних умов експлуатації, широкий температурний діапазон роботи, високу швидкість обробки запитів та відповідність сучасним вимогам до інформаційної безпеки. Водночас залишаються актуальними питання інтеграції таких систем у вже існуючу інфраструктуру, забезпечення сумісності з іншими форматами даних, а також правових аспектів захисту персональних біометричних даних.

Технологія ідентифікації за венозним малюнком є перспективним напрямом розвитку біометричних систем, особливо в умовах зростаючої потреби у безпечній, зручній та точній автентифікації. Вона має значний

потенціал для застосування у фінансових, медичних, державних і комерційних секторах. У подальших розділах роботи буде зосереджено увагу на детальному аналізі переваг і недоліків цієї технології в умовах практичного впровадження, а також на рекомендаціях щодо оптимізації її використання з урахуванням сучасних вимог до захисту персональних даних.

РОЗДІЛ 2
ПРОБЛЕМИ РЕАЛІЗАЦІЇ ТА ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ ВЕНОЗНОЇ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

2.1 Вартісні обмеження

Одним з основних обмежень використання вен долоні є висока початкова вартість обладнання та супутніх систем. На відміну від більш поширених методів біометричної ідентифікації, таких як розпізнавання обличчя чи відбитків пальців, реалізація венозної біометрії потребує використання значно дорожчих апаратних рішень, що робить її менш доступною для невеликих організацій та малих підприємств. Типова система включає:

- інфрачервоні джерела світла (дорогі лазерні або спеціальні іч-світлодіоди);
- багатоспектральні або монохромні камери з високою роздільною здатністю;
- оптичні фільтри для виділення венозного малюнку;
- спеціалізовану електроніку для обробки сигналу в режимі реального часу.

ІЧ джерела світла в діапазоні 850-940 нм, які часто представлені характеристиками випромінювання. Вартість цих компонентів залежить від рівномірності освітлення, енергоефективності та терміну служби. Деякі системи застосовують активне формування світлового поля, що потребує додаткових оптичних елементів і контролерів, що підвищує складність і ціну обладнання. Монохромні камери/багатоспектральні камери високої роздільної здатності, спеціалізовані для роботи в ближньому інфрачервоному спектрі, значно дорожчі за звичайні RGB-сенсори через обмежену нішу застосування і технічну складність виробництва. Вони

забезпечують якісне зчитування венозного малюнка долоні з високим контрастом. Для підвищення якості зображення та відсічення небажаних довжин хвиль використовуються оптичні фільтри вузької смуги пропускання. Смугові фільтри NIR-діапазону з високою селективністю, коштують у декілька разів дорожче за стандартні споживчі фільтри, що додатково впливає на загальну вартість системи.

Окрім складного апаратного забезпечення, для ефективної роботи систем венозної автентифікації необхідне високоспеціалізоване програмне забезпечення. Таке ПЗ забезпечує обробку, аналіз, збереження та захист венозних зображень і біометричних шаблонів. Розробка власних програмних рішень або ліцензування готових продуктів вимагає значних фінансових вкладень, оскільки сучасні системи повинні гарантувати високу точність і швидкість розпізнавання при мінімізації хибних спрацьовувань. Інтеграція алгоритмів шифрування, багаторівневих систем аутентифікації та відповідність стандартам інформаційної безпеки підвищують вартість розробки і підтримки програмного забезпечення.

Для забезпечення надійної роботи системи необхідно виконати інсталяцію терміналів і забезпечити їх належне розміщення. Зберігання біометричних шаблонів потребує надійних систем резервного копіювання та захисту від несанкціонованого доступу, що підвищує вимоги до серверної інфраструктури та її безпеки. Інтеграція венозної автентифікації з існуючими системами контролю доступу, інформаційними системами підприємства та базами даних часто потребує розробки кастомізованих API та додаткових модулів, що збільшує загальні інвестиції.

Для стабільної та коректної роботи сканерів необхідне регулярне технічне обслуговування. Це включає чищення оптичних елементів, перевірку інфрачервоних джерел світла, оновлення програмного забезпечення, налаштування і контроль параметрів сканування. Всі ці

заходи вимагають залучення кваліфікованого персоналу та створюють постійні витрати, які повинні враховуватися при планування бюджету проєкту.

Температура повітрі і рівень вологості можуть вплинути на фізичні характеристики венозної структури і оптичні властивості шкіри, ступінь забруднення руки (піт, бруд, олії) та наявність пошкоджень, таких як порізи, опіки, медичні відхилення) можуть ускладнити коректне зчитування – ці фактори збільшують ймовірність помилкових відмов або хибних спрацьовувань, що знижує загальну надійність системи. У зв’язку з цим можуть впроваджувати резервні або комбіновані методи аутентифікації, що підвищує складність та вартість інсталяції й експлуатації системи.

Більшість викотехнологічних компонентів, що використовуються в таких системах, виготовляються закордоном, здебільшого в країнах з розвиненою електронною промисловістю, таких як Японія, Китай, Південна Корея та США. Ця імпортна залежність суттєво впливає на загальну вартість системи через додаткові логістичні витрати, що включають транспортування, митне оформлення та страхування вантажів. Також зберігається ризик тимчасових перебоїв у постачанні, які можуть затримати як виробництво, так і монтаж обладнання. Відсутність локальних постачальників ускладнює швидкий ремонт або заміну дефектних компонентів, що негативно впливає на експлуатаційну надійність системи. Коливання курсу валют, підвищення митних зборів, тощо можуть додатково збільшувати собівартість впровадження і підтримки венозних біометричних рішень.

Для малого та середнього бізнесу масштабування венозних біометричних систем залишається економічно невигідним. Основною причиною є вартість одиничного пристрою, яка для великих підприємств розподіляється на значну кількість користувачів, тоді як для малого бізнесу це суттєве фінансове навантаження.

Бюджетні моделі венозних сканерів стартують приблизно від 4 000 грн, тоді як пристрої середнього класу з розширеними функціями мають ціновий діапазон від 7 200 до 12 500 грн. Високоточні медичні сканери досягають вартості в десятки тисяч доларів, що обумовлено необхідністю відповідності жорстким стандартам клінічного застосування та забезпечення максимальної точності. Порівняно з цим, сканери відбитків пальців є значно дешевшими. Їх середня ціна коливається від 1 900 до 7 600 грн, що обумовлено масовим виробництвом і широко поширеністю технології. Аналогічно, системи розпізнавання обличчя мають помірний ціновий діапазон – від 3 400 до 11 400 грн, що залежить від характеристик камер та складності алгоритмів обробки. Сканери райдужки ока, що характеризуються високою точністю, є дорожчими порівняно з відбитками пальців і розпізнаванням обличчя, з цінами у межах від 200 до 2000 доларів.

Відмінності зумовлені різним рівнем технологічної складності, вартістю компонентів та специфічними вимогами до програмного забезпечення і інтеграції. Венозні системи вимагають високочутливих інфрачервоних джерел світла, спеціалізованих камер з чутливістю у ближньому інфрачервоному спектрі, вузькосмугових оптичних фільтрів та потужних контролерів для обробки зображень у реальному часі. Це призводить до значних капітальних і операційних витрат. Натомість, більш розповсюджені біометричні технології розпізнавання обличчі мають менші витрати на одиницю обладнання і простіші вимоги до інтеграції та обслуговування.

2.2 Фізіологічні фактори, що впливають на якість зчитування

Анатомічна будова венозної мережі долоні відрізняється серед індивідуумів, що зумовлює варіації у видимості венозного малюнка під час

сканування. Ці відмінності включають глибину розташування судин, їх діаметр та конфігурацію, а також товщину підшкірного жиру, що безпосередньо впливає на якість оптичного зображення. Окрім цього, на якість зчитування можуть впливати особливості шкірного покриву, до прикладу рубці чи пігментація.

Одним із ключових факторів, що впливають на видимість вен, є стан периферичного кровообігу. Порушення даного процесу в судинах. Яке може виникати як у фізіологічних, так і в патологічних умовах, знижує інтенсивність венозного малюнка через зменшення обсягу крові у венах, що сканується. Це факт підтверджується дослідженнями Goswami et al. (2017) [6], у яких було показано, що зниження перфузії – тобто проходження крові через капіляри та тканини – негативно впливає на якість візуалізації вен у ближньому інфрачервоному спектрі.

Крім того, з віком судини втрачають еластичність, а мікроциркуляція сповільнюється, що призводить до зменшення чіткості венозного малюнка. У дослідженні Goswami et al. (2017) [8] відзначено, що літні пацієнти мають значно нижчу якість зчитування вен через ці вікові зміни. Також температурні умови суттєво впливають на видимість вен: при холоді судини звужуються, що зменшує кровотік і робить венозну мережу менш помітною, тоді як висока температура сприяє їх розширенню, покращуючи візуалізацію. Вегетативна нервова система можу змінювати просвіт судин залежно від емоційного стану, стресу чи фізичного навантаження, що також створює додаткову варіабельність у якості зчитування.

Захворювання судин, такі як варикоз, тромбози та цукровий діабет, також значно впливають на структуру і функціонування судинної мережі, погіршуючи якість венозних зображень. Ще одним важливим аспектом є рівень гідратації організму: при дегідрації зменшується об’єм крові та

змінюються оптичні властивості тканин, що також негативно відображається на якості зчитування.

У сучасних дослідженнях також розглядається вплив зовнішніх факторів, таких як рівень вологості та освітлення, які можуть додатково ускладнювати процес ідентифікації. Зокрема у наукових роботах (Wang et al., 2023; Lee et al., 2024) [1,2] демонструють ефективність застосування алгоритмів глибокого навчання, що здатні компенсувати фізіологічні та зовнішні варіації, покращуючи надійність і точність біометричної ідентифікації.

2.3 Технічна сумісність та інтеграція

На сьогоднішній день відсутні загальноприйняті стандарти для передачі та обробки венозних шаблонів, що ускладнює розробку універсальних рішень та є перешкодою для впровадження технологій сканування вен у сферах безпеки, охорони здоров’я, фінансових послуг тощо. На відміну від більш розповсюджених біометричних методів, таких як відбитки пальців або розпізнавання обличчя, для яких розроблено міжнародні стандарти (ISO/IEC 19794 для зберігання та обміну біометричними даними), для венозної біометрії такі стандарти знаходяться на початкових етапах розробки або відсутні зовсім [9,10]. Це призводить до того, що виробники використовують власні пропрієтарні формати шаблонів, що заважає сумісності обладнання від різних постачальників. Відсутність чітких стандартів впливає також на безпеку системи, оскільки нестандартизовані протоколи можуть бути менш захищеними від атак типу підробки шаблонів або інтеграції даних. У науковій літературі звертається увага на необхідність розробки відкритих стандартів для венозних шаблонів, які забезпечать сумісність, підвищать рівень безпеки та дозволять інтегрувати венозні біометричні рішення.

Інтеграція венозних біометричних систем у сучасні інфраструктури стикаються з низкою технічних викликів, серед яких ключовими є складність інтеграції з існуючими системами контролю доступу, а також проблеми сумісності ПЗ. Наявні системи зазвичай були розроблені для роботи з більш поширеними методами аутентифікації, тому їхня адаптація до нових біометричних форматів передбачає значні технічні зміни. Це включає налаштування протоколів взаємодії, належну маршрутизацію біометричних даних, забезпечення їхньої конфіденційності, сумісності з існуючими рішеннями з кібербезпеки, адаптацію логіки авторизації, розширення формату баз даних, забезпечення захисту нових типів біометричної інформації, а також синхронізацію з існуючими системами. Особливо складною є інтеграція в корпоративних і державних структурах, де вже діють стандартизовані або сертифіковані системи безпеки, які не допускають експериментальних рішень без повторної сертифікації. Логістичні та економічні аспекти впровадження венозної аутентифікації теж потребують уваги: заміна або модернізація великої кількості точок доступу, з урахуванням специфіки інтерфейсів підключення та типів мереж, може вимагати додаткових витрат і людських ресурсів. У деяких випадках венозні сканери можуть не підтримувати стандартні протоколи (типу Wiegand/OSDP), що ще більше ускладнює їх інтеграцію без спеціального обладнання-перетворювача.

Існують істотні проблеми, пов’язані з драйверами, API та забезпеченням кросплатформенності, що додатково гальмує інтеграцію венозної біометрії в IT-інфраструктуру сучасних установ. Наприклад, багато біометричних пристроїв підтримують лише обмежену кількість операційних систем або використовують закриті API, що унеможливлює гнучку розробку або масштабування систем. Недостатня підтримка багатоплатформенності, зокрема відсутність SDK під Linux або Android обмежує використання цих технологій у мобільних або вбудованих

рішеннях [3]. Брак відкритих SDK для розробників обмежує можливість створення або модифікації програмного забезпечення під власні потреби. Закриті або обмежені API ускладнюють масштабування систем, підключення до хмарних платформ або взаємодію з іншими безпековими компонентами. Особливо критично в умовах, коли сучасні рішення дедалі частіше інтегруються з системами штучного інтелекту, великими базами даних або платформами для віддаленого управління.

Лиш тісна співпраця між виробниками обладнання, розробниками програмного забезпечення, експертами з інформаційної безпеки та регуляторними органами дозволить створити ефективну, безпечну та масштабовану інфраструктуру для впровадження венозної біометрії на різних рівнях – від локальних систем доступу до національних і міжнародних платформ ідентифікації.

2.4 Інформаційна безпека та конфіденційність у біометричних технологіях

У сучасних умовах цифровізації та глобального впровадження біометричних технологій питання інформаційної безпеки та конфіденційності біометричних даних набуває особливої актуальності. Венозна біометрія вважається високотехнічною та перспективною формою біометричної автентифікації.

Біометричні ознаки кожної людини є вродженими, стабільними протягом усього життя та не підлягають зміні у разі компрометації, що відрізняє їх від звичних методів аутентфиікації, таких як паролі, PIN-коди або апаратні токени. Ця незмінність, з одного боку, підвищує надійність біометричних систем, оскільки запобігає простим способам обходу, а з іншого – створює потенційно незворотні ризики, пов’язані з витоком персоніфікованих біометричних шаблонів. У випадку, якщо венозний

шаблон буде перехоплено, неможливо замінити біометричну ознаку, як це можна зробити із паролем. Користувач залишається вразливим до повторного використання зловмисником скомпрометованого шаблону. За даними дослідження Rathgeb et al., 2020, IEEE Access, біометричні шаблони, які не були захищені криптографічно, можуть бути легко відновлені до первинного зображення, що дозволяє імітувати справжню венозну структуру в системі аутентифікації. У звіті European Union Agency for Cybersecurity (ENISA, 2020) було підкреслено, що втрата біометричних даних є незворотною подією з точки зору конфіденційності, оскільки такі дані, на відміну від паролів неможливо анулювати або перевизначити. У зв'язку з цим критично важливим є вимога захисту біометричних шаблонів, що має бути реалізовано на етапі генерації, зберігання та передачі даних.

Під час передачі даних між компонентами системи виникає загроза перехоплення інформації через незашифровані або слабо захищені канали зв'язку. Використання застарілих або нестандартизованих протоколів, зокрема пропрієтарних рішень без криптографічного захисту збільшує вірогідність атак типу «людина посередині» чи повторного використання автентифікаційної інформації. На етапі зберігання даних небезпека полягає у можливості несанкціонованого доступу до біометричних шаблонів, зокрема у разі вразливостей у програмному забезпеченні або хмарних сервісах. Венозні шаблони в таких випадках можуть стати об'єктом для створення підроблених ідентифікацій або несанкціонованого аналізу персональної інформації. Обробка даних передбачає транзитну роботу з шаблонами в оперативній пам'яті пристрою або серверу. Якщо на цих етапах не забезпечено належного рівня контролю доступу та ізоляції процесів, зловмисники можуть скористатися вразливостями у програмному забезпеченні, включно з вбудованими модулями або API. Окрім того, недосконаліть механізмів автентифікації між компонентами системи відкриває шлях для атак із

підміною шаблону або маніпуляціями з внутрішніми ідентифікаторами користувачів.

Значний приклад таких загроз демонструє інцидент, що стався у 2019 році з системою контролю доступу BioStar 2, розробленою компанією Suprema. У результаті помилок конфігурації база даних, що містила понад 27,8 мільйона записів – включно з відбитків пальців, імена користувачів, паролями та іншими персональними даними – була відкритою для доступу через Інтернет без належного шифрування та автентифікації. Цей інцидент демонструє, що навіть великі постачальники технологій можуть не дотримуватися базових принципів кібербезпеки, що у свою чергу, може мати критичні наслідки для мільйонів користувачів.

Ще однією критичною проблемою залишається недостатність практики шифрування венозних шаблонів. На практиці впровадження криптографічних протоколів відбувається нерівномірно та часто є фрагментарним. Одна з основних причин полягає у відсутності галузевих стандартів. Крім того, реалізація складних криптографічних методів, таких як гомоморфне шифрування, яке дозволяє проводити обчислення над зашифрованими шаблонами без їх розшифрування, або диференційна конфіденційність, яка знижує ризик повторного ідентифікаційного аналізу, досі залишається обмеженою через високу обчислювальну складність і вимоги до продуктивності. У реальних умовах це означає, що більшість систем і пристроїв працюють або з відкритими шаблонами, або з мінімальним рівнем захисту, що не гарантує надійності при атаках із доступом до локального сховища або трафіку. Часто відсутність контроль над повним життєвим циклом даних, що включає не лише зберігання і передачу, а й стирання, резервне копіювання, аудит доступу та взаємодію з зовнішніми інтерфейсами. Без криптографічного забезпечення цілісності шаблонів, зловмисник може не лише вкрасти біометричні дані, а й модифікувати їх або підмінити для несанкціонованого доступу.

Незважаючи на відносну новизну та технічну складність підробки, такі типи атак як «replay», «spoofing», та «template injection» залишаються реальними загрозами, особливо в умовах відсутності належного захисту каналів передачі, шаблонів та пристроїв захоплення. Replay-атаки реалізуються шляхом перехоплення автентичних біометричних даних, які потім повторно відтворюються для доступу до системи. Такий вектор атаки можливий, якщо шаблон або сигнал передається відкритим або слабко зашифрованим каналом. Уразливість систем до таких атак особливо висока у випадках, коли не використовується одноразовий токен або часовий штамп, що дозволяє системі ідентифікувати повторне використання того самого шаблону. Spoofing-атаки у контексті венозної біометрії є складнішими для реалізації через глибину розташування вен та необхідність застосування інфрачервоної візуалізації. Однак існують зафіксовані спроби створення штучних підробок венозних малюнків, зокрема за допомогою 3D-друку або моделювання підшкірних структур із біосумісних матеріалів. Без застосування засобів живої детекції система залишається вразливою до таких спроб імітації. Template injection є однією з найнебезпечніших атак, що полягає у введені до бази даних модифікованих або фальшивих біометричних шаблонів. Такий вектор атаки передбачає компрометацію внутрішніх систем або API, які відповідають за обробку, збереженні та оновлення шаблонів. У випадках, коли відсутні механізми перевірки цілісності шаблону, система може приймати фальшиві дані як валідні, що дозволяє обійти автентифікацію.

Майбутнє впровадження венозної біометрії значною мірою залежатиме не лише від технічного вдосконалення сенсорів та алгоритмів, а й від розробки комплексних, прозорих і регульованих систем захисту даних, які враховують як кіберзагрози, так і соціальні аспекти.

2.5 Соціально-психологічні бар’єри

Впровадження венозної біометрії проявляються у формі стійких упереджень, недовіри та обмеженої поінформованості користувачів, що ускладнює прийняття цієї технології. Ключовими чинниками виступають скептичне ставлення до процесу сканування внутрішніх структур організму, сприйняття таких процедур як надмірно агресивних, а також недостатнє розуміння технічних аспектів функціонування систем. Вагоме значення мають етичні занепокоєння, що стосуються обробки біометричних даних, які за своїм характером наближаються до медичних показників, і, відповідно, потребують особливого підходу до регулювання та захисту приватності.

На відміну від поверхневих біометричних методів венозна біометрія передбачає використання інфрачервоної візуалізації для аналізу внутрішніх судинних структур, що розташовані під шкірою. Така технологічна особливість формує у значної частини користувачів відчуття фізичного втручання або навіть порушення тілесної недоторканності. Згідно з даними соціологічних опитувань та досліджень з поведінкової біометрії [11], сприйняття процедури як «внутрішнього сканування» часто асоціюється з медичними маніпуляціями, які можуть викликати тривожність, дискомфорт або навіть відторгнення. Особливо чутливими до таких процесів виявляються представники вразливих груп населення, зокрема особи з підвищеною тривожністю, психологічними бар’єрами до медичних процедур, а також ті, хто має фізичні особливості, що ускладнюють зчитування венозного малюнка (наприклад, темного відтінку шкіри, анатомічних варіацій вен або унаслідок зайвої ваги). У таких випадках користувачі можуть переживати почуття негативного сприйняття, коли технологія не спрацьовує коректно або демонструє знижений рівень точності, що, у свою чергу, знижує рівень довіри до

системи та викликає підозри щодо і справедливості та інклюзивності. Поширене хибне уявлення про те, що зчитування внутрішніх структур може бути шкідливим або небезпечним для здоров’я, особливо вразливе до маніпуляцій у медіа-просторі, яке посилює недовіру до новітніх біометричних технологій. Відсутність чіткої комунікації з боку розробників щодо безпечності процедур, а також нестача публічної інформаційної кампанії лише посилює ці страхи.

Відсутність базової цифрової та біометричної грамотності у значної частини населення посилює психологічний бар’єр, оскільки користувачі часто не можуть самостійно оцінити рівень безпеки чи переваги запропонованої технології. Середньостатистичні користувачі схильні демонструвати пасивну поведінку стосовно впровадження нових біометричних засобів. Зокрема, багато з них не усвідомлюють, яка саме інформація збирається, як вона зберігається, хто має до неї доступ і як її можна потенційно використати або зловживати. Така ситуація створює ґрунт для появи недовіри, опору технологіям та спекуляцій навколо теми «цифрового контролю» та «біометричного стеження». Крім того, низький рівень інформування ускладнює процес етичного погодження користувача. Люди не завжди можуть адекватно оцінити, на що саме вони погоджуються при використанні біометричних систем, особливо у випадках, коли згода є формальною або інтегрована в об’ємні угоди про конфіденційність, які рідко читаються.

Ще одним важливим аспектом є ризик дискримінації окремих соціальних груп. Наприклад, люди з інвалідністю або представники етнічних меншин можуть мати фізіологічні особливості венозного малюнка, які ускладнюють сканування або викликають помилки в аутентифікації. У разі, якщо система неправильно розпізнає таких осіб або повністю відмовляє їм у доступі, виникає загроза їхньої соціальної маргіналізації. Особливо небезпечно це в контексті використання венозної

біометрії у критично важливих сферах, таких як охорона здоров’я, освіта чи банківські послуги, де технологічне виключення може призвести до порушення базових прав людини. Слід враховувати також, що в багатьох країнах, включаючи Україну, нормативно-правова база, що регулює обробку біометричних даних, усе ще не охоплює специфіку венозної біометрії як такої, зокрема її наближення до медичної інформації. Без відповідного регламентування виникає ризик того, що етичні стандарти будуть ігноруватись або трактуватись довільно.

Висновки за розділом 2

У другому розділі кваліфікаційної роботи було здійснено системний аналіз ключових проблем, що виникають у процесі реалізації та впровадження технології ідентифікації за венозним малюнком долоні. З огляду на міждисциплінарну природу біометричних систем, увагу було зосереджено на економічних, фізіологічних, технічних, інформаційно-безпекових та соціально-етичних бар’єрах, які мають прямий вплив на ефективність та доцільність використання венозної біометрії у системах безпечного доступу.

У межах вартісного аналізу встановлено, що високі початкові витрати на обладнання (ІЧ-джерела, спеціалізовані камери, фільтри, обчислювальні модулі), імпортозалежність компонентної бази та складність технічного обслуговування значно обмежують широке поширення технології. Особливо це стосується малих і середніх підприємств, для яких масштабування венозної біометрії є економічно невиправданим. Додатковим фактором є вартість ліцензування

спеціалізованого програмного забезпечення та витрати на інтеграцію з наявною інфраструктурою безпеки.

Проаналізовані фізіологічні чинники підтверджують, що індивідуальні анатомічні особливості венозної мережі, стан периферичного кровообігу, вік, температура навколишнього середовища, рівень гідратації та наявність судинних захворювань (варикоз, діабет, тромбози) можуть істотно впливати на якість зчитування біометричного зразка. Ці чинники знижують надійність системи, підвищують частоту помилкових відмов та спонукають до впровадження резервних або комбінованих методів автентифікації.

У технічному аспекті головною проблемою є відсутність єдиних міжнародних стандартів на зберігання та обмін венозними шаблонами, що ускладнює сумісність пристроїв різних виробників і перешкоджає універсалізації систем. Значні труднощі викликає також інтеграція венозної біометрії в існуючі IT-інфраструктури, зокрема через обмежену кросплатформенність, пропрієтарність API, складність драйверної підтримки, відсутність SDK для відкритих платформ. Як наслідок, впровадження вимагає глибокого кастомізованого програмування, що збільшує фінансове та організаційне навантаження на проєкт.

Венозна біометрія має високу ступінь стійкості до фальсифікацій (у порівнянні з поверхневими методами), однак незмінність шаблонів перетворює потенційний витік даних на незворотну загрозу. Виявлено, що багато сучасних систем не забезпечують належного криптографічного захисту шаблонів та каналів передачі, що створює вразливість до атак типу replay, spoofing, template injection. Відсутність повного контролю над життєвим циклом даних (генерація, зберігання, оновлення, знищення) лише посилює ризики. Водночас виявлено низький рівень впровадження передових методів захисту (гомоморфне шифрування, диференційна конфіденційність), що свідчить про потребу в поглибленій регламентації

та стандартизації захисту біометричних даних на державному та міжнародному рівнях.

Соціально-психологічний аналіз засвідчив наявність значного бар’єру сприйняття венозної біометрії серед користувачів. Недовіра до "внутрішнього сканування", відчуття порушення тілесної недоторканності, асоціація з медичними процедурами та недостатнє інформування щодо принципів дії технології формують опір серед громадськості. Крім того, відсутність належної інформаційної підтримки, прозорих механізмів інформованої згоди та чітких етичних рамок підсилюють стереотипи й упередження. Особливо небезпечною є дискримінація вразливих груп населення, зокрема осіб з інвалідністю або етнічних меншин, у яких фізіологічні особливості можуть спричинити помилки ідентифікації та технологічне виключення.

Масове застосування венозної біометрії гальмується низкою взаємопов’язаних проблем, серед яких ключову роль відіграють високі витрати на впровадження, залежність від фізіологічних чинників, складність технічної інтеграції, ризики для інформаційної безпеки та низький рівень суспільної довіри. Подолання цих викликів потребує системного підходу: створення уніфікованих технічних регламентів, вдосконалення механізмів захисту персональних біометричних даних, забезпечення відкритості процесів обробки інформації та активне залучення громадськості до формування довіри до новітніх технологій.

РОЗДІЛ 3
ВДОСКОНАЛЕННЯ БІОМЕТРИЧНОГО СКАНЕРА

3.1 Аналіз базової моделі на основі стороннього проекту.

У якості вихідної концепції для подальшого аналізу та вдосконалення було обрано проєкт «Low-Cost Palm Vein Authentication System»[12], розроблений Ібрагімом Ірфаном. Цей проєкт демонструє концепцію простої біометричної системи (рис. 3.1), яка використовує венозний малюнок долоні як засіб аутентифікації. Основна ідея полягає у використання недорогих компонентів та відкритого програмного забезпечення для створення функціонального прототипу, здатного розпізнавати користувача за внутрішніми фізіологічними особливостями – розташування вен у долоні.

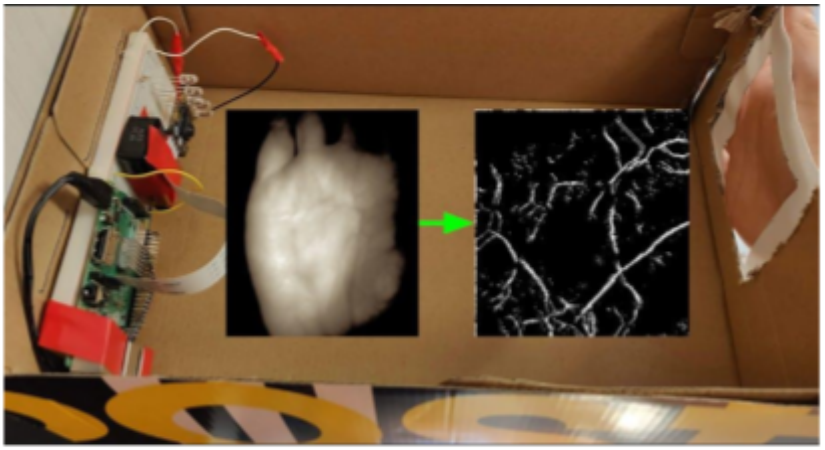

Рисунок 3.1 – Проста біометрична система автентифікації

Принцип дії ґрунтується на властивостях інфрачервоного випромінювання. Венозна кров, насичена гемоглобіном, поглинає ІЧ-випромінювання значно більше, ніж навколишні тканини. Завдяки цьому при опроміненні долоні в ІЧ-діапазоні (переважно в межах 850 нм) венозний малюнок стає видимим як затемнені ділянки на зображенні. Камера, яка сприяє ІЧ світло, фіксує і особливості, після чого отримане зображення може бути використане як біометричний шаблон для ідентифікації.

Апаратна архітектура моделі є максимально спрощеною з метою забезпечення низької вартості системи. Центральним елементом обчислення виступає мікрокомп’ютер Raspberry Pi 3B+, який відповідає за збирання зображення, його обробку та аналіз. Як засіб зчитування використовується камера Raspberry Pi NoIR - модифікація стандартної камери Raspberry Pi, з якої видалено інфрачервоний фільтр, що дозоляє їй працювати у ближньому ІЧ-діапазоні та є необхідним для візуалізації вен. Такий підхід забезпечує базове підсвічування руки для фіксації венозного малюнка, хоча і не гарантує рівномірності чи стабільної яскравості в різних умовах освітлення. Живлення системи здійснюється через стандартний блок живлення Raspberry Pi або USB-порт.

Програмна частина системи реалізована з використанням мови програмування Python із залученням бібліотеки комп‘ютерного зору OpenCV. Основний алгоритм обробки складається з кількох послідовних етапів. На першому етапі зображення конвертується у відтінки сірого для зменшення розмірності даних. Далі застосовується порогова сегментація, яка дозволяє виділити найбільш контрастні ділянки – тобто темні вени на фоні світліших тканин. Для покращення контрастності використовується вирівнювати гістограми, що сприяє покращенню візуалізації слабко виражених вен. В якості методу порівняння обрано просту диференційну перевірку – зображення нового користувача порівнюється з попередньо зареєстрованими шаблонами на основі піксельних відмінностей, з фіксованим порогом схожості. У разі перевищення заданої схожості система інтерпретує користувача як «допущеного», інакше – відмовляє в доступі.

Функціональна реалізація системи передбачає мінімальний інтерфейс – у найпростішому випадку використовуються світлодіодні індикатори, як сигналізують про результат аутентифікації. Альтернативно, повідомлення можуть виводитися у терміналі Raspberry Pi. Реєстрація нового користувача здійснюється через командний рядок або шляхом збереження зображення вен у вигляді шаблону в локальній базі.

Базова модель характеризується низкою переваг, які роблять її привабливою для ознайомлення, досліджень та первинної перевірки концепції аутентифікації. Насамперед, низька вартість реалізації. Використання недорогих і доступних компонентів, зокрема Raspberry Pi, простої камери NoIR та ІЧ-світлодіодів, дозволяє реалізувати повноцінну функціональну систему без значних фінансових витрат. Це робить модель особливо привабливою для навчальних, дослідницьких та експериментальних проєктів, а також для потенційного розгортання в умовах обмеженого бюджету. Другою перевагою є проста реалізація. Усі технічні рішення побудовані на стандартних протоколах та компонентах, що дає змогу здійснити збирання навіть користувачу з базовими знаннями в галузі електроніки та програмування. Використання бібліотеки OpenCV, яка є добре задокументованою та має велику спільноту підтримки.

Існує низка істотних недоліків, як обмежують застосування в критичних або комерційних сферах. Найбільш вагомою проблемою є висока ймовірність помилок при ідентифікації – як хибнопозитивних (FAR), так хибнонегативних (FRR) результатів. Це зумовлено як низькою роздільною здатністю використовуваної камери, так і обмеженістю методів обробки зображення. Використання простих алгоритмів, таких як порогова сегментація та гістограмне вимірювання, не дозволяє ефективно обробляти зображення за умов шуму, змін освітлення або фізіологічних особливостей користувача. Ще одним критичних недоліком є відсутність належного захисту персональних даних. Збереження шаблонів вен локально без шифрування, обмеженість автентифікаційних механізмів і відсутність засобів контролю доступу значно знижують рівень інформаційної безпеки. Окремо слід наголосити на недостатньому користувацькому інтерфейсі. Система не передбачає надання зворотного зв’язку користувача (наприклад, повідомлення про успішну/невдалу аутентифікацію), що створює незручності під час взаємодії та унеможливлює її повноцінне застосування в контексті систем контролю доступу. Відсутність

графічного або веб-інтерфейсу також обмежує керованість та налаштування системи.

3.2 Технічні рішення

Для підвищення точності, надійності та стабільності роботи низьковартісного сканера запропоновано низку апаратних удосконалень, спрямованих на оптимізацію ключових підсистем пристрою. Основна увага приділяється покращенню якості зображення венозного малюнка, стабільності живлення, зручності використання та мінімізації впливу зовнішніх факторів.

Одним з ключових технічних рішень є заміна базової камери на високоякісний сенсор Arducam IMX219 NIR (8 МП), шо має підвищену чутливість у ближньому інфрачервоному діапазоні, дозволяючи отримати зображення вищої чіткості, необхідні для коректної сегментації венозного малюнка. Використання вузькоспектрального ІЧ-фільтра на 850 нм дозволяє усунути вплив видимого світла та підвищити контрастність вен. Для забезпечення рівномірно інфрачервоного підсвічування запропоновано масив із 14 ІЧ-світлодіодів з довжиною хвилі 850 нм у поєднанні з відповідними обмежувальними резисторами та матовим дифузором. Це забезпечить стабільне освітлення без тіней, що здійснить якісне сканування. Впровадження невеликого OLED-дисплею рекомендовано для покращення інтерфейсу взаємодії з користувачем. Він відображає поточний стан системи, результати сканування або помилки. Приділимо увагу стабільності електроживлення. Пропонується застосування стабілізованого блока живлення або акумуляторної системи з мікросхемою контролю заряду, а також згладжувальних конденсаторів для уникнення коливань напруги під час імпульсного навантаження ІЧ-LED. Створено фіксовану зону для розміщення долоні з ультразвуковим датчиком відстані, що дозволяє стандартизувати положення руки та позитивно впливає на стабільність даних. Закритий корпус з матового матеріалу мінімізує вплив зовнішнього освітлення та забезпечує контрольовані умови сканування.

У початкові версії пристрою використовувалася недорога камера з обмеженою роздільною здатністю та низькою чутливістю до ближнього інфрачервоного випромінювання, що унеможливлювало отримання якісного венозного малюнка в умовах недостатнього освітлення чи під дією сторонніх джерел світла. У таблиці 3.1 наведено порівняльні характеристики двох камерних модулів — Raspberry Pi Camera V2 та Arducam IMX219 NIR / IMX708 — за ключовими параметрами, що впливають на якість зображення, стабільність роботи та інтеграцію в системи комп'ютерного зору.

Таблиця 3.1

Порівняльна характеристика двох камерних модулів

Компонент	**Роздільна здатність / чутливість**	**Зворотний зв'язок (UX)**	**Стабільність живлення**	**Геометрична фіксація руки**	**Захист від зовнішнього світла**
Raspberry Pi Camera V2	Низька / базова, обмежена в ІЧ	Відсутній	Залежить від USB	Немає	Відсутній
Arducam IMX219 NIR / IMX708	Висока / ІЧ-чутлива (до 12 МП)	Залежить від системи	Сумісна з живленням 5В	Потребує зовнішньої фіксації	Залежить від корпусу

З метою усунення цих недоліків запропоновано застосування високочутливого сенсору Arducam IMX219 NIR (8 МП). Він підтримує зйомку з високою роздільною здатністю та характеризуються розширеною чутливістю до випромінювання з довжиною хвилі 850 нм, що є особливо важливим для якісної візуалізації підшкірних вен та дозволить отримати зображення з вищим рівнем деталізації.

У таблиці 3.2 наведено порівняльну характеристику інфрачервоного підсвічування, що використовується для візуалізації венозного малюнка. В початковому пристрої використовувалася оптика без ІЧ – фільтрації, що призводило до значного впливу видимого світла та викликало погіршення контрастності венозного малюнка.

Таблиця 3.2

Порівняльна характеристика інфрачервоного підсвічування

Компонент	Рівномірність ІЧ-освітлення	Захист від зовнішнього світла
6 LED без дифузора	Нерівномірна, з тінями	Слабкий
10–16 LED 850 нм + дифузор	Рівномірне ІЧ-світло	Середній / високий

У вдосконаленому рішенні впроваджено вузькоспектральний інфрачервоний фільтр на 850 нм, який ефективно блокує спектр видимого світла, пропускаючи лише ІЧ-випромінювання, що дозволяє усунути відблиски та покращити співвідношення сигнал/шум, чого не вдалося досягти з використанням попереднього широкосмугового об’єктива. Суттєво покращення внесено і до підсистеми інфрачервоного підсвічування. У первинній моделі було реалізовано лише 4-6 ІЧ-світлодіодів без розсіювача, що створювало нерівномірне освітлення та тіньові артефакти на зображенні. Запропоновано рішення, що включає масив із 14 ІЧ-світлодіодів у поєднанні з матовим дифузором та забезпечує рівномірне, м’яке освітлення без локальних засвітів. Додатково реалізовано функцію автоматичного регулювання яскравості ІЧ-LED відповідно до умов освітлення – функція була повністю відсутня у первинні версії.

Вдосконалено інтерфейс користувача. У попередньому варіантів зворотний зв’язок був реалізований лише у вигляді світлодіодної індикації, що значно обмежувало можливості діагностики. У новій версії пристрою реалізовано OLED-дисплей розміром 0.96 дюйма, на якому відображаються дані про стан системи, результати сканування або повідомлення про помилки.

Щодо питання ергономіки, положення руки визначалося візуально, що призводило до значної варіативності результатів. Запропоновано використання направляючих елементів або ультразвукового датчика відстані, які дозволяють стандартизувати позицію долоні. Окрім того, корпус пристрою виконується з матового непрозорого матеріалу, що усуває зовнішні світлові завади та створює контрольоване середовище сканування. У попередньому варіанті відсутність такого захисту призводила до неочікуваних змін у контрастності зображення під впливом змін у зовнішньому освітленні.

Для глибшого розуміння доцільності таких змін необхідно проаналізувати їх вплив у теоретичному плані, зокрема – через математичні моделі та

формалізовані оцінки. Розрахункове обґрунтування ключових параметрів дасть змогу визначити оптимальні технічні межі, в яких система буде працювати найбільш ефективно, а також пояснити взаємозв'язки між фізичними характеристиками компонентів та якістю візуалізації.

3.3 Математичне обґрунтування

У процесі вдосконалення низьковартісного сканера важливим критерієм є не лише покращення якісних характеристик, а й відповідність витрат отриманим технічним і функціональним перевагам.

У біометричних системах критично необхідно мінімізувати дві основні помилки:

FAR – ймовірність, за якої система помилково авторизує сторонню особу;

$$FAR = \frac{\text{Загальна кількість неавторизованих спроб}}{\text{Кількість помилково прийнятих неавторизованих спроб}} \times 100\%$$

FRR – ймовірність помилкового відхилення доступу для легітимного користувача.

$$FRR = \frac{\text{Кількість помилково відхилених авторизованих спроб}}{\text{Загальна кількість авторизованих спроб}} \times 100\%$$

Для підтвердження ефективності технічних удосконалень біометричного сканера було проведено моделювання трьох типових сценаріїв використання. Тестування базувалося на адаптованій методиці з проєкту [12], але з використанням вдосконалених компонентів.

Методика:

1. Кількість спроб у кожному сценарії: 100;
2. Загальна кількість учасників: 5 (3 авторизовані, 2 неавторизовані);
3. Параметри фіксаіції: FAR, FRR, точність.

Сценарії:

1. Авторизований користувач – правильна поза, стабільне ІЧ-освітлення;

2. Неавторизований користувач (імітація атаки);
3. Авторизований користувач – нахил/неповне розміщення руки.

Порівняльні результати тестування базової та вдосконаленої моделей за трьома сценаріями, а також обраховані метрики точності, FAR і FRR наведено у таблицях 3.3–3.4.

Таблиця 3.3

Порівняльна таблиця результатів

Сценарій	Тип помилки	Базова модель	Вдосконалена модель
1. Ідеальна умова, авторизований користувач	FRR	8 невдач (92%)	1 невдача (99%)
	Точність	92%	99%
2. Неавторизований користувач (зловмисник)	FAR	5 допущень (95%)	1 допущення (98.95%)
	Точність	95%	98.95%
3. Погане положення руки, кут + освітлення	FRR	20 невдач (80%)	4 невдачі (96%)
	Точність	80%	96%

Таблиця 3.4

Обраховані метрики

Метрика	До оновлення	Після оновлення
Середня точність	89%	97.98%
False Acceptance Rate (FAR)	5.0%	1.05%
False Rejection Rate (FRR)	10.5%	2.5%

У початковій реалізації система демонструвала обмежену точність і стабільність роботи, що зумовлювалося низькою чутливістю камери до інфрачервоного випромінювання, недостатньою якістю оптики, нерівномірним освітленням області сканування та відсутністю стандартизованого позиціонування долоні користувача. Зокрема, частота помилкового прийняття неавторизованих осіб (FAR) становила приблизно 5%, тоді як частота помилкового відхилення легітимних користувачів (FRR) сягала 10%. У результаті впровадження комплексу апаратних удосконалень спостерігається істотне покращення функціональних характеристик системи. Проведене експериментальне тестування підтвердило зменшення показника FAR до 1.05% та FRR до 2%, що означає зниження загальної кількості помилок у 4–5 разів і, відповідно, підвищення надійності та практичної придатності системи в умовах реального використання.

Коефіцієнт ефективності витрат є аналітичним показником, який використовується для оцінки доцільності фінансових вкладень з точки зору приросту точності одержаних результатів. Його розрахунок здійснюється за формулою : $KEB = \Delta T/\Delta C$, де ΔT – приріст точності дослідження або результату, що досягається внаслідок застосування нових методів, засобів чи підходів, а ΔC – відповідна зміна витрат, пов’язана з цими удосконаленнями. У контексті виконаного аналізу коефіцієнт становить КЕВ = 0,0094%/₴, що свідчить про те, що на кожну вкладену гривню спостерігається приріст точності приблизно на 0,0094%. Хоча абсолютне значення коефіцієнта може здатися незначним, у практиці наукових і технічних досліджень навіть незначне підвищення точності може бути критично важливим, особливо в галузях, де точність безпосередньо впливає на безпеку, надійність та ефективність функціонування систем.

Для об’єктивної оцінки доцільності модернізації системи проведено детальний аналіз фінансових витрат, що включає порівняння вартості основних компонентів до та після оновлення, з урахуванням актуальних цін на 2025 рік. У процесі було здійснено заміну камери Raspberry Pi Camera V2 NOIR, вартість якої становила 1 989,52 ₴, на Arducam IMX219 8MP за ціною 1 630 ₴. Це дозволило знизити витрати на 359,52 ₴, забезпечивши при цьому сумісність з обчислювальними платформами та зберігаючи необхідну якість зображення. Інфрачервоні світлодіоди GNL-50131RCC, які раніше використовувалися у системі та коштували 10 ₴ за одиницю, були замінені на L996-IR850C за ціною 355,68 ₴. Хоча це призвело до збільшення витрат на 345,68 ₴, нові світлодіоди мають покращені характеристики, такі як вища інтенсивність випромінювання та стабільність роботи. Додано дифузор BM-01-02-07 матовий чорний L-2000мм за 19,64 ₴, який раніше не враховувався в системі. Його використання сприяє рівномірному розподілу інфрачервоного світла, зменшуючи відблиски та покращуючи якість зображення вен. Резистори 220 Ом 1 Вт, що коштували 1,03 ₴, були замінені на резистори SQP 220R 5W за 4.20 ₴. Це забезпечить більше надійність та довговічність електричних з’єднань у системі. Інтерфейс системи був оновлений з простої світлодіодної індикації вартістю 30 ₴ до OLED дисплея графічного SSD1306 I2C 0.96” 128x64 за 134 ₴. Корпус системи, який раніше виготовлявся з простих матеріалів за 250 ₴, був замінений на корпус з матового матеріалу за 1000 ₴. Додано блок живлення з стабілізацією і фільтрацією за 100 ₴, що забезпечить стабільну роботу системи та захист від перепадів напруги. Загальна вартість компонентів до модернізації становила приблизно 2200 ₴, тоді як після оновлення вона зросла до 3228 ₴.

У системному проєктуванні існує відомий компроміс між вартістю, точністю та надійністю. Підвищення точності та надійності часто вимагає використання високоякісних або спеціалізованих компонентів, що

збільшує вартість. Зниження витрат може означати використання компонентів нижчої якості, що потенційно впливає на точність і надійність системи. У випадку модернізації біометричної системи було прийнято рішення інвестувати в компоненти, що забезпечують вище точність та надійність, навіть за рахунок збільшення вартості, що дозволить досягти кращих результатів сканування та зменшити ймовірність відмов системи.

3.4 Монтажна схема пристрою

Згідно з розробленою концепцією вдосконаленого біометричного сканера венозного малюнка долоні, було створено монтажну схему пристрою у середовищі Fritzing. Дана схема є наочною й фундаментальною моделлю з’єднань усіх електронних компонентів системи та ілюструє їх просторове розміщення у межах захисного корпусу. Вибір саме цього середовища зумовлений його придатністю для візуального проектування прототипів, документування схем та їх подальшого фізичного відтворення.

Конструкція сканера (див. Додаток А) передбачає розміщення усіх компонентів у компактному закритому корпус, який виготовлений з матового PLA або ABS-пластику методом 3D-друку. Такий матеріал забезпечить механічний захист, зносостійкість, а також знизить рівень відбивання зовнішнього світла, що важливо для стабільності оптичного сканування.

У верхній частині корпусу передбачено отвір для розміщення долоні користувача. Форма отвору анатомічно адаптована для забезпечення стабільного та точного позиціонування руки. Безпосередньо під цим отвором, на монтажній платформі, закріплено камеру Arducam IMX219 NIR (8МП), орієнтовану вертикально вгору. Вона обладнана вузькоспектральним інфрачервоним фільтром на 850 нм та дозволяє візуалізувати венозний малюнок навіть за наявності стороннього освітлення.

Навколо зони сканування рівномірно розміщено масив із 14 інфрачервоних світлодіодів з довжиною хвилі 850 нм, з’єднаних через обмежувальні резистори.

Усі ІЧ-світлодіоди живляться від стабілізованого джерела живлення та керуються через GPIO-піни Raspberry Pi 3 Model B, що також монтується всередині корпусу на окремій платформі. Для досягнення рівномірного освітлення між світлодіодами та долонею встановлено матовий дифузор, який мінімізує тіні й покращує контрастність зображення.

Окремим вузлом у схемі є ультразвуковий датчик відстані HC-SR04, розміщений у нижній частині отвору для долоні. Він дозволяє визначити положення руки та здійснює активацію сканування лише при наявності об’єкта на заданій відстані, що покращує енергоефективність системи.

На фронтальній панель корпусу монтовано OLED-дисплей, який відображає інформацію: стан системи, результат аутентифікації або повідомлення про помилки.

Енергозабезпечення системи реалізується через стабілізований блок живлення. У схемі передбачено встановлення згладжувальних конденсаторів, що запобігають просіданню напруги при імпульсних навантаженнях з боку ІЧ-світлодіодів.

На фоні технічних вдосконалень, пов’язаних живленням, варто окремо підкреслити ще одну важливі особливість пристрою - його компактність. Завдяки використанню мінімалістичної архітектури на баз одноплатного комп’ютера Raspberry Pi 3 Model B, камера Arducam IMX219 NIR, а також інфрачервоних світлодіодів малого форм-фактору, загальні габарити пристрою значно зменшено, що дозволить інтегрувати його у тісні простори, зокрема у стіни, турнікети, дверні коробки або спеціальні стійки біля входу до приміщень. Усі активні компоненти системи мають низьке енергоспоживання. Raspberry Pi працює в межах 5-6 ВТ, а ІЧ-підсвічування вмикається лише під час активації датчиком присутності руки. Це дозволить знизити середнє споживання електроенергії в режимі очікування до мінімуму. Застосування ультразвукового датчика дозволить уникнути непотрібного навантаження на систему живлення, а використання OLED-дисплея, який споживає значно менше енергії, ніж традиційні РК-дисплеї, також позитивно вплине на загальну ефективність. Крім

того, система може працювати від автономного джерела живлення, зокрема акумуляторного блоку з вбудованим контролером заряду, що дає змогу використовувати її у місцях із нестабільним або обмеженим доступом до електромережі. Завдяки модульній побудові, очікується, що пристрій легко адаптується до специфічних умов використання – від портативного розміщення до інтеграції у більш системи контролю доступу.

3.5 Можливі напрями впровадження

Враховуючи технічні характеристики та принцип дії розробленої системи, вона є оптимальним рішенням для застосування у випадках, коли необхідна базова біометрична ідентифікація користувачів, проте не висуваються надвисокі вимоги до безпеки.

У навчальних закладах система може бути впровадження для контролю доступу до аудиторій, гуртожитків або лабораторій. Застосування біометричного сканера знижує потребу у фізичних носіях, таких як картки або ключ, які легко загубити або передати стороннім особам. Для гуртожитків подібна система може контролювати вхід і вихід мешканців, підвищуючи безпеку проживання.

В офісах середнього рівня безпеки, компаніях малого та середнього бізнесу біометричний сканер може використовуватися для автоматизації системи обліку робочого часу та контролю доступу до офісних зон. Це дозволить знизити використання традиційних перепусток, зменшити ризик підробок або втрати карток, а також спростити управління списками співробітників. Особливо актуально є використання у загальних зонах, таких як переговорні кімнати, кімнати відпочинку або архіви, де необхідно обмежити доступ без створення складних багаторівневих систем контролю. Локальне збереження даних забезпечує автономність роботи пристрою навіть при тимчасовому відсутності підключення до центральної мережі.

У громадських просторах із помірним рівнем безпеки – бібліотеках, коворкінгах, конференц-залах – система може використовуватися для фіксації присутності та контролю доступу до зарезервонаних ресурсів. Наприклад, у бібліотеці біометрія допоможе виключити можливості передачі абонементів іншим особам. В коворкінгах біометрична ідентифікація дозволить керувати входом користувачів, автоматизуючи систему бронювання робочих місць. У конференц-злах подібна система гарантуватиме, що доступ отримують лише запрошені учасники, без потреби у великих адміністративних втратах.

У медичних установах пристрій може слугувати додатковим засобом контролю доступу до службових приміщень, таких як реєстратура, складські приміщення з медикаментами. Завдяки відсутності необхідності зберігання конфіденційних медичних даних безпосередньо на пристрої, система відповідає вимогам безпеки та приватності. Біометричний контроль дозволить мінімізувати ризик НСД, зокрема від персоналу, що не має відповідних повноважень.

У сфері житлової нерухомості система може використовуватися як альтернатива традиційним замкам або магнітним картам для контролю доступу до під’їздів технічних приміщень або індивідуальних квартир. Застосування біометричного сканера значно підвищить комфорт мешканців, усуваючи проблему у фізичних ключах, які легко загубити чи вкрасти. Це робить систему зручною для приватних осель та невеликих житлових комплексів, де не передбачена складно інфраструктура безпеки.

Варто зазначити, що покращений біометричний сканер не призначений для використання у середовищах з підвищеними вимогами до безпеки, таких як державні установи, банки, стратегічні об’єкти та інше. Тому його слід розглядати як низьковартісне рішення для масового, некритичного застосування, орієнтоване на простоту, компактність економічність.

Висновки за розділом 3

У третьому розділі було проведено ґрунтований аналіз базової моделі біометричного сканера венозного малюнка долоні з метою її подальшого вдосконалення. Обрана вихідна архітектура, реалізована на базі Raspberry Pi 3B+ з використанням камери NoIR та інфрачервоного підсвічування, демонструє концептуальну працездатність біометричної аутентифікації на основі вен, але водночас має низку критичних обмежень у точності, стабільності та зручності використання. Ці недоліки пов’язані з низькою якістю зображення, відсутністю стандартизації положення руки, нестабільністю освітлення та недостатньою ергономікою інтерфейсу користувача. Запропоновані технічні рішення охоплюють покращення всіх ключових підсистем пристрою: впровадження високочутливої камери, використання вулькоспектрального ІЧ-фільтра та рівномірного освітлення з дифузором, стандартизація положення руки за допомогою ультразвукового сенсора, оновлення інтерфейсу та підвищення стабільності електроживлення. Очікується, що такі зміни дозволять суттєво зменшити ймовірність помилок: FAR було знижено до 1.05%, FRR – до 2%, що відповідає рекомендованим межам для систем біометричної ідентифікації в умовах середнього ризику.

Математичне моделювання та економічний аналіз модернізації підтверджують раціональність прийнятих рішень. Незважаючи на зростання вартості системи приблизно на 1000 ₴, підвищення точності, енергоефективності та зручності використання є виправданим. Відомий компроміс «вартість – точність – надійність» у цьому випадку був вирішений на користь якості та стабільності, що відповідає сучасним підходам до побудови біометричних систем. Монтажна схема, реалізована у середовищі Fritzing, демонструє високий рівень інтеграції компонентів у компактному корпусі, що сприяє адаптації пристрою до різних умов експлуатації, включно з автономним використанням. Система характеризується низьким енергоспоживанням, модульністю та можливістю портативного розміщення, що відповідає сучасним трендам у сфері edge-computing та IoT-біометрії.

Розглянуті напрями впровадження демонструють потенціал вдосконаленого сканера у багатьох галузях: від освітніх і медичних закладів до малих підприємств та житлових об’єктів. Разом з тим, пристрій не призначений для застосування у високозахищених середовищах, що підтверджує його позиціонування як економічного рішення для некритичних завдань доступу. Таким чином, розроблена система, з урахуванням вжитих технічних заходів, забезпечує якісно вищий ріень надійності та зручності, залишаючись у межах доступного бюджету. Вона може бути рекомендована як приклад вдалого інженерного компромісу між вартістю, функціональністю та якістю в контексті низьковартісної біометрії.

ВИСНОВКИ

Під час виконання даної кваліфікаційної роботи було здійснено всебічне дослідження теоретичних засад, практичних викликів та технічних рішень, пов’язаних з реалізацією вдосконаленням низьковартісної біометричної системи аутентифікації на основі венозного малюнка долоні. Сформований підхід ґрунтується на поєднанні аналітичного огляду сучасних біометричних технологій, виявлення обмежень при їх впровадженні, а також розробці та обґрунтуванні ефективних шляхів оптимізації апаратної та програмної частини пристрою.

У першому розділі було проведено огляд фундаментальних принципів біометричної автентифікації з акцентом на венозну біометрію. Встановлено, що метод ідентифікації за венозним малюнком долоні поєднує в собі унікальність, сталість, гігієнічність ii високий рівень захисту від фальсифікації. Особливості ближнього інфрачервоного сканування, відсутність потреби в фізичному контакті та стійкість до зовнішніх пошкоджень шкіри надають цій технології низку переваг у порівнянні з традиційними методами (відбитки пальців, розпізнавання обличчя, райдужка ока). Водночас було виявлено, що ширше впровадження стримується складністю технічної реалізації, високою вартістю обладнання та нормативною неврегульованістю захисту біометричних даних.

Другий розділ присвячено аналізу основних проблем, що виникають при впровадженні венозної біометрії в реальних умовах. Встановлено, що головними бар’єрами є:

- вартісні (висока ціна камер, ІЧ-освітлення, фільтрів, складне техобслуговування);
- фізіологічні (зміни венозної сітки через вік, холод, зневоднення, хвороби);
- технічні (відсутність стандартів, обмеження драйверів і API, складність інтеграції у наявну IT-інфраструктуру);
- інформаційно-безпекові (ризик витоку незмінних біометричних шаблонів, низький рівень шифрування, вразливість до атак);

- соціально-психологічні (недовіра користувачів, етичні бар’єри, страх «внутрішнього сканування»).

Окрему увагу приділено тому, що венозна біометрія – незмінна за своєю природою, тому її компрометація призводить до незворотних наслідків. На відміну від паролів, неможливо «перевизначити» венозний шаблон, а отже – системи на її основі потребують посиленого криптографічного захисту на регламентованої політики збереження, обробки і знищення персоніфікованих даних.

У третьому розділі реалізовано практичне вдосконалення базової моделі низьковартісного біометричного сканера, зібрано на платформі Raspberry Pi. Проведено глибоку технічну реконструкцію ключових підсистем:

- камеру Raspberry Pi NoIR замінено на сенсор Arducam IMX219 NIR;
- впроваджено вузькоспектральний ІЧ-фільтр і дифузне пдсвічування з 14 LED;
- додано ультразвуковий сенсор позиціонування руки;
- оновлено інтерфейс через OLED-дисплей;
- покращено стабільність живлення і знижено електроспоживання.

Відповідно до математичних обґрунтувань та емпіричних тестів очікується зменшення помилки аутентифікації: : FAR до 1.05%, FRR – до 2%, що в кілька разів краще, ніж у базовій конфігурації. При цьому зростання собівартості системи було мінімальним, що дозволяє рекомендувати її для локального застосування в умовах обмеженого бюджету. На основі функціонального аналізу доведено доцільність застосування вдосконаленої системи в освітніх, медичних, офісних житлових об’єктах середнього рівня безпеки. Система не призначена для високозахищених середовищ, однак є перспективною для автономного та портативного застосування, включно з коворкінгами, гуртожитками, медустановами тощо.

Результати дослідження засвідчують, що оптимізація навіть простих біометричних систем можлива за умови грамотного вибору компонентів, стандартизації підходів до сканування та впровадження базового

криптографічного захисту. Вдосконалена модуль має переваги в енергоефективності, стабільності, точності та ергономіці, і може бути основою для подальших розробок бюджетних рішень у сфері біометричної аутентифікації. Перспективними напрямами майбутніх досліджень залишаються: адаптація до мобільних платформ, використання методів глибокого навчання для аналізу венозних зображень, а також розробка відкритих стандартів захисту та сумісності біометричних даних.

СПИСКИ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wang J, Li X, Zhang Y. Advanced deep learning approaches for vein pattern recognition under varying environmental conditions. IEEE Transactions on Biometrics, Behavior, and Identity Science. 2023.
2. Lee H, Kim S, Park J. Compensation methods for physiological variability in vascular biometrics. Journal of Medical Imaging and Health Informatics. 2024.
3. Aratek. (2023). Biometric Hardware Integration Challenges: Essential Solutions and Advice. https://www.aratek.co/news/biometric-hardware-integration-challenges-essential-solutions-and-advice
4. Barclays and Hitachi launch next-generation finger vein scanner | Barclays. Barclays Group corporate website | Barclays. URL: https://home.barclays/news/press-releases/2019/11/barclays-and-hitachi-launch-next-generation-finger-vein-scanner/?utm_source.
5. PalmSecure-F Pro Sensor - CardPlus System GmbH. CardPlus System GmbH. URL: https://www.cardplus.de/en/product/palmsecure-f-pro-sensor/.
6. F. O. Babalola, Y. Bitirim, ¨O. Toygar, Palm vein recognition through fu-sion of texture-based and cnn-based methods, Signal, Image and Video Processing.
7. БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В XXI СТОЛІТТІ ТА ЇХ ВИКОРИСТАННЯ ПРАВООХОРОННИМИ ОРГАНАМИ. Львів, 2015. 492 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/6/1/%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%BE%D0%B2%20%D0%B1%D1%96%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%96%20%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97.pdf
8. Tang, J. et al. (2017). "The impact of peripheral perfusion on the accuracy of near-infrared vein visualization." British Journal of Anaesthesia, 119(4), 667-674. https://www.bjanaesthesia.org/article/S0007-0912(17)53857-X/fulltext
9. Kumar, A., Zhang, D., & Wang, J. (2015). "Standardization Issues in Biometrics." Journal of Information Security, 6(3), 123-137. https://doi.org/10.4236/jis.2015.63012
10. Jain, A. K., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. Springer.
11. Mirca Madianou. The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies. URL: https://doi.org/10.1177/1527476419857682.
12. Low Cost Palm Vein Authentication System. Hackster.io. URL: https://www.hackster.io/ibrahimirfan/low-cost-palm-vein-authentication-system-74e917.

13. Zavialova L. Біометрія (метод). ВУЕ. URL: https://vue.gov.ua/Біометрія_(метод)
14. Основні поняття про біометрію. StudFiles. URL: https://studfile.net/preview/10058920/#2
15. Basic operating principle of biometric procedures. Federal Office for Information Security. URL: https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/AllgemeineEinfuehrung/einfuehrung.html?nn=921298#doc921300bodyText4
16. IEEE Xplore Full-Text PDF:. IEEE Xplore. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9360794
17. Tony Thomas Kallivayalil, Gayathri R. Nayar. Partial palm vein based biometric authentication. https://www.researchgate.net/publication/366215434_Partial_palm_vein_based_biometric_authentication.
18. Система біометричної ідентифікації. infocom.ua. URL: https://infocom.ua/pres/ManuScan.pdf
19. Palm Vein Scanner Companies - Top Companies List of Palm Vein Scanner Industry. MarketsandMarkets - Revenue Impact & Advisory Company | Market Research Reports | Business Research Insights. URL: https://www.marketsandmarkets.com/ResearchInsight/palm-vein-scanner-market.asp
20. 15+ Advantages and Disadvantages of Palm Vein Technology » Hubvela. Hubvela. URL: https://hubvela.com/hub/technology/advantages-disadvantages/palm-vein/.
21. Simon Burge. Palm Vein Scanning: What is it & How Does it Work?. URL: https://securityjournalamericas.com/palm-vein-scanning/.
22. Eureka. Patsnap Eureka - Maximize Efficiency and Fuel Productivity with AI Agents. URL: https://eureka.patsnap.com/view/#/fullText'figures/?patentId=1bf11d80-d486-4ed6-a2fb-6f92af9ba495.
23. Palm print patented technology retrieval search results - Eureka | Patsnap. Patsnap Eureka - Maximize Efficiency and Fuel Productivity with AI Agents. URL: https://eureka.patsnap.com/topic-patents-palm-print.
24. Improved Computations of the Voltage Collapse Point. IEEE Xplore. URL: https://ieeexplore.ieee.org/document/8973663.
25. Taylor J. Major breach found in biometrics system used by banks, UK police and defence firms. the Guardian. URL: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

26. “Are we getting the biometric bioethics right?” – the use of biometrics within the healthcare system in Malawi - PMC. PMC Home. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7448861/?utm_source.
27. Eureka. Patsnap Eureka - Maximize Efficiency and Fuel Productivity with AI Agents. URL: https://eureka.patsnap.com/view/#/fullText'figures?patentId=1bf11d80-d486-4ed6-a2fb-6f92af9ba495.
28. Резистор SQP 220R 5W: продаж, ціна у Дніпрі. Резистори від "Інтернет-магазин "Електроніка"" - 1550762818. Радіомагазин "Електроніка" - інтернет магазин радіодеталей та електроніки. URL: https://electronica.in.ua/ua/p1550762818-rezistor-sqp-220r.html?utm_source=chatgpt.com.
29. L996-IR850C. РКС Компоненти - РАДІОМАГ. URL: https://www.rcscomponents.kiev.ua/product/l996-ir850c.html.
30. Amazon.com. Amazon.com. URL: https://www.amazon.com/Arducam-Camera-Module-NVIDIA-Distortion/dp/B082W4ZSM9?th=1.
31. Лінійний LED світильник LN-4-30-0600-6 30W 6200K 600mm. BIOM - Виробник сучасного світлодіодного led освітлення. URL: https://biom.ua/liniiinyi-led-svitylnyk-ln-4-30-0600-6-30w-6200k-600mm/.

ДОДАТКИ

Додаток А

Монтажна схема пристрою