МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Факультет: **ННІ Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **122 Комп'ютерні науки**
Освітня програма: **Комп'ютерні науки та інформаційні технології в бізнесі**

Група: АК–41б **денна форма навчання**

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

«БІОМЕДИЧНА ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ В АВТОМАТИЗОВАНИХ СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ»

ЗА НАКАЗОМ № 4601–5/335 ВІД 07 ЛЮТОГО 2025 РОКУ

здобувача вищої освіти **Миргородського Дмитра Олексійовича**

Робота допущена до захисту в ЕК
протокол кафедри ІТММ № 13 від 31.05.2025р.

Завідувач кафедри ІТММ
к.п.н., доцент
_____ Н.І. Стяглик

Науковий керівник
Ph.D з «Комп'ютерних наук»
_____ Д.М. Ковальчук

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально–науковий інститут "Каразінський банківський інститут"
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти перший (бакалаврський)
Спеціальність 122 Комп'ютерні науки
Освітня програма Комп'ютерні науки та інформаційні технології в бізнесі

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ **Н. І. Стяглик**
Підпис ініціали, прізвище

"08" лютого 2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Миргородського Дмитра Олексійовича
(прізвище, ім'я, по батькові студента)

1. Тема роботи Біомедична ідентифікація та аутентифікація в автоматизованих системах контролю доступу

керівник роботи Ph.D з «Комп'ютерних наук» Ковальчук Д.М.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від "08" лютого 2025 року № 4601–5/335

2. Строк подання студентом роботи 15 травня 2025 року

3. Перелік питань, які потрібно розробити:
У розділі 1: розлянури теоретичні засади біометричної ідентифікації та автентифікації. Провести порівняльний аналіз сучасних технологій і рішень з біометричної ідентифікації та автентифікації, що застосовуються в практиці контролю доступу..

У розділі 2: визначити технічні, функціональні та експлуатаційні вимоги до біометричних систем у складі автоматизованих систем контролю доступу. Провести порівняльний аналіз сучасних технологій і рішень з біометричної ідентифікації та автентифікації, що застосовуються в системах контролю доступу.

У розділі 3: спроєктувати архітектуру системи біометричної ідентифікації та аутентифікації з урахуванням вимог до інформаційної безпеки. Реалізувати програмне забезпечення системи, провести тестування його основних функцій та проаналізувати результати.

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір здобувачем теми кваліфікаційної бакалаврської роботи
2	Затвердження плану і завдання кваліфікаційної бакалаврської роботи
3	Здача кваліфікаційної бакалаврської роботи керівнику
4	Підпис кваліфікаційної бакалаврської роботи керівника
5	Підпис кваліфікаційної бакалаврської роботи у нормоконтролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної бакалаврської роботи
7	Захист кваліфікаційної бакалаврської роботи

5. Дата видачі завдання 08 лютого 2025 року

Студент _____ Д.О. Миргородський
підпис ініціали, прізвище

Керівник роботи _____ Д.М. Ковальчук
підпис ініціали, прізвище

РЕФЕРАТ
НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ
«БІОМЕДИЧНА ІДЕНТИФІКАЦІЯ ТА АУТЕНТИФІКАЦІЯ В АВТОМАТИЗОВАНИХ СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ»
Миргородського Дмитра Олексійовича

Кваліфікаційна бакалаврська робота містить 57 сторінок, 5 таблиць, 17 рисунків, список літератури з 14 найменувань.

Об'єктом дослідження є процеси ідентифікації та автентифікації користувачів у системах контролю доступу.

Предметом дослідження є біометричні методи і технології, що забезпечують ідентифікацію та автентифікацію особи на основі фізіологічних або поведінкових характеристик.

Мета кваліфікаційної бакалаврської роботи полягає у дослідженні теоретичних засад, аналізі існуючих рішень та розробці прототипу системи біометричної ідентифікації та автентифікації для автоматизованого контролю доступу.

Завданнями кваліфікаційної бакалаврської роботи є:

– дослідити поняття, принципи та класифікацію біометричних технологій;

– визначити переваги та недоліки біометричних методів;

– проаналізувати сучасні системи біометричної автентифікації та вимоги до них;

– обґрунтувати вибір біометричної ознаки для побудови власної системи;

– спроєктувати та реалізувати прототип системи біометричної ідентифікації та автентифікації;

– провести тестування та оцінку ефективності реалізованої системи.

Актуальність дослідження. У сучасних умовах швидкого розвитку інформаційних технологій та зростання загроз інформаційній безпеці, впровадження біометричних систем автентифікації є актуальним напрямом підвищення рівня захищеності систем контролю доступу.

За результатами дослідження: було створено функціональний прототип системи біометричної автентифікації на основі відбитків пальців, що забезпечує ефективне управління доступом користувачів та підвищує загальний рівень безпеки.

Практична новизна роботи полягає у реалізації авторського програмного рішення з використанням біометричних ознак для автентифікації користувачів у системі контролю доступу.

Одержані результати можуть бути використані у системах охорони, автоматизованих офісних та промислових об'єктах.

КЛЮЧОВІ СЛОВА: БІОМЕТРІЯ, ІДЕНТИФІКАЦІЯ, АВТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ, КІБЕРБЕЗПЕКА, АВТОМАТИЗОВАНА СИСТЕМА, ВІДБИТКИ ПАЛЬЦІВ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, PYTHON.

ABSTRACT

AT QUALIFICATION BACHELOR WORK

«BIOMETRIC IDENTIFICATION AND AUTHENTICATION IN AUTOMATED ACCESS CONTROL SYSTEMS»

Dmytro Myrhorodskyi

The bachelor's thesis contains 57 pages, 5 tables, 17 figures, and a reference list of 14 sources.

The object of the research is the processes of user identification and authentication in access control systems.

The subject of the research is biometric methods and technologies that ensure the identification and authentication of individuals based on physiological or behavioral characteristics.

The purpose of the bachelor's qualification work is to study theoretical foundations, analyze existing solutions, and develop a prototype of a biometric identification and authentication system for automated access control.

The tasks of the bachelor's thesis are as follows:

– to examine the concepts, principles, and classification of biometric technologies;

– to determine the advantages and disadvantages of biometric methods;

– to analyze modern biometric authentication systems and the requirements for their implementation;

– to justify the selection of biometric characteristics for system development;

– to design and implement a prototype of a biometric identification and authentication system;

– to test and evaluate the effectiveness of the developed system.

Relevance of the research: In the current context of rapid development in information technologies and increasing threats to information security, the implementation of biometric authentication systems is a highly relevant approach to enhancing the security of access control systems.

According to the results of the research, a functional prototype of a fingerprint-based biometric authentication system was developed, providing effective user access management and improving overall system security.

The practical novelty of the work lies in the implementation of an original software solution using biometric features for user authentication in an access control system.

The obtained results can be used in security systems, automated office environments, and industrial facilities.

KEYWORDS: BIOMETRICS, IDENTIFICATION, AUTHENTICATION, ACCESS CONTROL, CYBERSECURITY, AUTOMATED SYSTEM, FINGERPRINTS, SOFTWARE, PYTHON.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ І ТЕРМІНІВ

АСК – автоматизована система контролю

ІС – інформаційна система

ПЗ – програмне забезпечення

СКУД – система контролю та управління доступом

БД – база даних

API – програмний інтерфейс прикладного програмування

GUI – графічний інтерфейс користувача

ML – машинне навчання

ВСТУП

У сучасному світі, де інформаційна безпека набуває все більшого значення, надійна ідентифікація та аутентифікація користувачів стають критично важливими елементами будь-якої автоматизованої системи контролю доступу. Традиційні методи захисту, такі як паролі або магнітні картки, часто виявляються вразливими до крадіжок, підробок або соціальної інженерії. У цьому контексті біометричні технології, які базуються на унікальних фізіологічних або поведінкових характеристиках людини, забезпечують вищий рівень безпеки, точності та зручності використання. Актуальність дослідження зумовлена необхідністю впровадження ефективних біометричних систем у широке коло прикладних сфер – від офісів і підприємств до стратегічних об’єктів інфраструктури.

Об’єктом дослідження є процеси і методи ідентифікації та аутентифікації особистості в автоматизованих системах контролю доступу.

Предметом дослідження виступають біометричні технології і програмні засоби, що забезпечують ідентифікацію та аутентифікацію користувачів на основі фізіологічних ознак.

Мета кваліфікаційної бакалаврської роботи полягає у дослідженні, проєктуванні та реалізації програмної системи біометричної ідентифікації та аутентифікації на основі відбитків пальців для застосування в автоматизованих системах контролю доступу.

Завданнями кваліфікаційної бакалаврської роботи є:

– аналіз теоретичних основ біометрії та класифікація біометричних ознак;

– визначення переваг і обмежень біометричних технологій в порівнянні з традиційними методами;

– дослідження існуючих рішень біометричної ідентифікації та аутентифікації;

– обґрунтування вибору біометричної ознаки для розробки системи;

– проєктування архітектури програмного забезпечення;

– реалізація функціональної системи для розпізнавання відбитків пальців;

– тестування системи та оцінка її ефективності.

Практична новизна роботи полягає у створенні працездатного прототипу системи біометричної ідентифікації користувачів на основі аналізу відбитків пальців із використанням алгоритмів виявлення та зіставлення ознак. Реалізована система демонструє практичну придатність для використання в реальних умовах контролю доступу.

За результатами дослідження: було проаналізовано актуальні підходи до побудови біометричних систем, обґрунтовано вибір технічних рішень, створено програмне забезпечення, протестовано його працездатність і здійснено оцінку точності зіставлення біометричних зображень.

Одержані результати можуть бути використані:

– у розробці систем безпеки для підприємств та установ;

– в освітньому процесі при вивченні дисциплін з інформаційної безпеки;

– як основа для подальших досліджень та розширення функціоналу систем біометричної ідентифікації.

Перший розділ присвячено теоретичним основам біометрії: розглянуто поняття, принципи роботи, види біометричних ознак, переваги та недоліки технологій.

Другий розділ містить аналіз існуючих систем біометричної ідентифікації та аутентифікації, сформульовано вимоги до таких систем, наведено приклади реалізації у сучасних рішеннях.

У третьому розділі описано процес розробки власної програмної системи: обґрунтовано вибір біометричних ознак, представлено архітектуру ПЗ, реалізовано алгоритми аналізу відбитків пальців, виконано тестування та аналіз результатів. Висновок підсумовує результати дослідження, його значущість і перспективи розвитку.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

1.1. Поняття біометрії та біометричних технологій

Біометрія – це міждисциплінарна галузь, яка досліджує унікальні фізіологічні та поведінкові характеристики людини з метою її ідентифікації або автентифікації. До таких характеристик належать як зовнішні фізичні ознаки (відбитки пальців, форма вух, геометрія обличчя тощо), так і динамічні поведінкові патерни (голос, хода, стиль письма). Біометрія поєднує методи з біології, математики, інформатики, інженерії та соціальних наук, забезпечуючи надійні механізми безпечного доступу та персоніфікованої взаємодії з технологіями [1–3].

Біометричні технології – це прикладні інструменти й системи, що реалізують механізми збору, обробки та аналізу біометричних даних для автентифікації (верифікації) або ідентифікації особи. У сучасному світі такі технології широко використовуються в системах безпеки, банківській справі, охороні здоров’я, телекомунікаціях, а також при контролі доступу до інформаційних та фізичних ресурсів [1, 2].

Біометричні характеристики умовно поділяються на дві основні категорії [1–3, 5]:

– фізіологічні ознаки: відбитки пальців, геометрія руки та обличчя, райдужна оболонка та сітківка ока, ДНК, форма вуха;

– поведінкові ознаки: тембр і ритм голосу, динаміка підпису, хода, натиск клавіш тощо [1–2].

Кожна біометрична система функціонує за схожим принципом: на першому етапі відбувається реєстрація користувача, що передбачає збір кількох зразків за допомогою спеціалізованих сенсорів. Отримані дані обробляються, виділяються значущі ознаки, з яких формується еталонний

шаблон (реєстраційний профіль), який зберігається в системі для подальшого використання. Алгоритми створення шаблонів можуть бути як відкритими, так і запатентованими [1–3].

У процесі автентифікації система отримує «живий» біометричний зразок, порівнює його із збереженим шаблоном і приймає рішення про відповідність. Такий процес називають верифікацією (підтвердженням особи). Якщо ж система виконує ідентифікацію, то порівняння відбувається з усією базою шаблонів (схема «один–до–багатьох») для встановлення особи без попереднього її оголошення [1–3, 5].

Архітектурна структура типової біометричної системи зображена на рис. 1.1, де подано основні компоненти процесу – від збору зразка до остаточного рішення системи. Ключову роль виконує постачальник біометричної служби – програмний компонент, що забезпечує реалізацію біометричних операцій відповідно до певного протоколу чи інтерфейсу [4, 5].

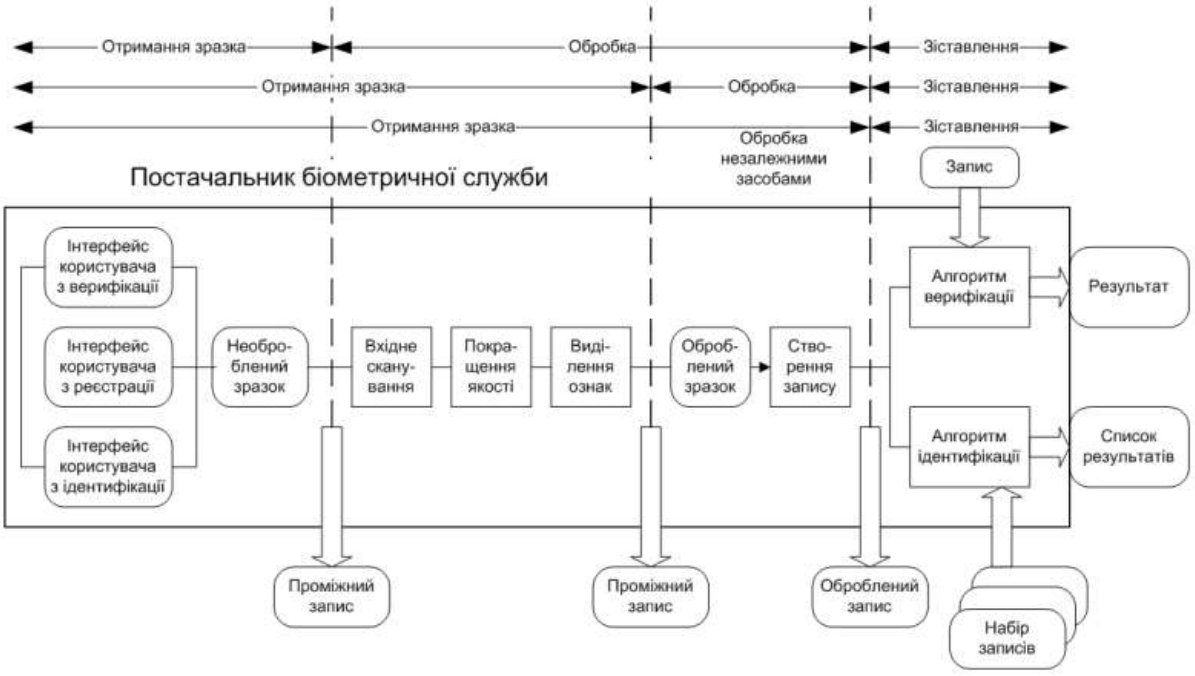

Рис. 1.1. Архітектура базової моделі біометричної системи

Варто зазначити, що процеси стандартизації у сфері біометрії активно розвиваються на міжнародному рівні. Підкомітет SC 37 технічного комітету

ISO/IEC JTC 1 вже розробив понад 30 міжнародних стандартів у цій галузі. В Україні впровадження біометричних технологій розпочалося з 2010 року зі створення національного технічного комітету, який адаптує ці стандарти до вітчизняних потреб. Сьогодні біометрія використовується в нашій країні здебільшого у сфері контролю кордонів, видачі документів та захисту доступу до конфіденційної інформації [4-6].

1.2. Класифікація біометричних ознак

Біометричні ознаки являють собою сукупність фізіологічних, поведінкових або психологічних характеристик людини, що є унікальними для кожної особи і можуть використовуватись для цілей ідентифікації та автентифікації. На відміну від традиційних методів, таких як паролі або ідентифікаційні картки, біометричні дані не потребують запам’ятовування, важко підробляються і є набагато зручнішими для користувача, що робить їх надзвичайно ефективними в сучасних системах безпеки. Основною перевагою біометричних ознак є їхній високий рівень індивідуальності: ймовірність того, що дві особи матимуть однакові відбитки пальців або однакову форму райдужної оболонки, надзвичайно мала – наприклад, для відбитків пальців ця ймовірність становить приблизно 1 до 24 мільйонів. Крім того, біометричні параметри значно складніше підробити, що підвищує рівень захисту інформаційних систем. Порівняльна характеристика методів біометричної ідентифікації наведена в таблиці 1.1 [4, 5].

Залежно від способу взаємодії користувача із системою, біометричні ознаки поділяють на активні та пасивні. Активні ознаки вимагають свідомих дій з боку людини, таких як прикладання пальця до сканера, вимова фрази або підпис. Пасивні ж можуть бути зафіксовані без участі користувача – наприклад, автоматичне зчитування обличчя або малюнка райдужної оболонки ока за допомогою камери. Такий розподіл важливий при

проєктуванні зручних і ефективних систем ідентифікації, особливо у місцях з високою прохідністю, де мінімізація дій користувача має критичне значення.

Таблиця 1.1.

Порівняльна характеристика методів біометричної ідентифікації

Біометричний метод	Ймовірність відмови в доступі, %	Імовірність хибного допуску сторонньої особи (без муляжу), %	Імовірність хибного допуску сторонньої особи (з муляжем), %	Можливість збереження конфіденційності біометричного шаблону	Орієнтовна вартість реалізації, у.о.
Аналіз форми кисті	0,2–4	0,2–1	10–75	Неможливо забезпечити повну конфіденційність	600–3000
Сканування відбитків пальців	2–6	0,0001	10–70	Захист повної таємниці не гарантується	60–600
Вивчення сітківки ока	0,4	6–10	–	Приховування шаблону неможливе	Близько 4000
Ідентифікація за райдужкою	0,2–2	0,0001	–	Приховати біометричний образ неможливо	500–6000
Розпізнавання обличчя	1–9	–	–	Неможливо уникнути відкритого доступу до образу	55000
Аналіз почерку	0,5–5	0,5–5	0,5–5	Часткова можливість збереження образу (від 8 до 40%)	–
Оцінка манери набору тексту	3–9	3–9	–	Обмежена конфіденційність (6–12%)	–
Голосова біометрія	0,5–5	0,5–5	25–90 (при використанні запису)	Частково можливе приховування (10–30%)	1–60

Серед розглянутих біометричних методів кожен має свої переваги та обмеження, що слід враховувати при виборі технології для конкретного застосування. Метод ідентифікації за геометрією руки базується на аналізі

форми та розмірів кисті. Він є технічно простішим у реалізації порівняно з іншими підходами, однак має нижчу точність та більшу ймовірність помилкової ідентифікації при використанні підроблених зразків. Попри це, він може бути ефективним у середовищах із невисокими вимогами до безпеки, наприклад, у навчальних закладах чи офісах із внутрішнім контролем доступу [4-6].

Відбитки пальців є найбільш поширеним методом біометричної аутентифікації завдяки високій унікальності папілярних візерунків. Метод характеризується відносно низькою ймовірністю відмови у доступі та широким розповсюдженням, зокрема, у смартфонах, банківських системах і системах доступу. Водночас технологія має один з найвищих ризиків підробки – за допомогою муляжів або копій, що потребує додаткових механізмів захисту, наприклад, перевірки живої тканини [5–7].

Сканування сітківки ока забезпечує надзвичайно високу точність і низький рівень помилок, оскільки малюнок судин очного дна є унікальним і складним для фальсифікації. Однак цей метод є менш зручним для користувача через необхідність точної фіксації погляду та використання спеціального обладнання, що обмежує його масове впровадження. Райдужна оболонка ока також вважається одним із найнадійніших біометричних параметрів. Вона дозволяє досягти точності ідентифікації на рівні 0,0001%, є стійкою до змін з віком, проте потребує якісної камери та стабільних умов сканування, що іноді ускладнює її застосування у динамічному середовищі.

Метод ідентифікації за портретом обличчя вирізняється зручністю, адже може здійснюватися без фізичного контакту та у фоновому режимі, наприклад, при проходженні крізь контрольну зону. Разом з тим, на точність розпізнавання впливають зовнішні чинники: рівень освітлення, зміни міміки, наявність аксесуарів чи косметики. У більшості випадків такі системи вимагають високоякісного обладнання та алгоритмів з урахуванням багатьох змінних, що впливає на загальну вартість впровадження [5–7].

Варто також зазначити особливості автоматичного розпізнавання обличчя, яке сьогодні активно використовується у громадських місцях і прикордонному контролі. Технології face–контролю забезпечують точність до 86–93%, що суттєво перевищує здатність людини ідентифікувати знайомі обличчя за старими фотографіями. Проте надійність таких систем залежить від якості обладнання, рівня освітлення, кута огляду та роздільної здатності зображення. Наприклад, для ефективного аналізу зображення необхідно, щоб відстань між зіницями на зображенні становила не менше 200 пікселів [5, 6].

У світлі розвитку біометричних технологій з'являються і нові напрямки. Серед них – використання електрофізіологічних ознак, таких як сигнали мозкової активності або електрокардіограми (ЕКГ), що відкривають перспективи побудови ще більш захищених та персоналізованих систем. Також інтенсивно розвивається цифрова поведінкова біометрія, яка враховує моделі взаємодії користувача з пристроями, що дозволяє проводити ідентифікацію у фоновому режимі без перешкод для звичного користування пристроєм [6].

Класифікація біометричних ознак також базується на їх природі: розрізняють фізіологічні (статичні) та поведінкові (динамічні) ознаки. До фізіологічних належать такі стабільні параметри, як відбитки пальців, геометрія кисті, сітківка та райдужка ока, структура вен, форма вуха, ДНК. Порівняльна характеристика фізіологічних методів ідентифікації наведена в таблиці 1.2. Ці характеристики є сталими протягом життя і не змінюються під впливом зовнішніх або емоційних факторів. Поведінкові ознаки, навпаки, залежать від особистих звичок і моторики людини – зокрема, це голос, динаміка підпису, хода, стиль натискання клавіш або руху курсора. Незважаючи на більшу мінливість, поведінкові параметри також дозволяють досягти високого рівня точності при відповідній побудові алгоритмів [6, 7].

Таблиця 1.2.

Порівняльна таблиця фізіологічних методів ідентифікації

Біометрична характеристика	Тип пристрою для реєстрації	Тип зразка	Ключові досліджувані риси
Геометрія кисті	Спеціалізований настінний апарат	Об'ємне (3D) зображення зверху та збоку долоні	Розміри та форма суглобів і пальців, висота та ширина кісток
Відбитки пальців	Настільні сканери, ПК-периферія, зчитувачі у клавіатурах, мишах, картки типу PC Card, мікросхеми	Зображення відбитка (оптичне, ультразвукове, кремнієве або безконтактне)	Лінії, розгалуження та мікроструктура папілярного візерунку
Сітківка ока	Спеціалізовані настільні або настінні сканери	Зображення сітківки	Малюнок судинної сітки – положення кровоносних судин
Райдужна оболонка ока	Відеокамери з інфрачервоним підсвічуванням, комп'ютерні камери	Чорно-біле зображення райдужної оболонки	Візерунок смуг, борозенок і текстура райдужки
Обличчя	Цифрові фото- та відеокамери, у тому числі вбудовані в комп'ютери	Фото особи (у видимому або інфрачервоному спектрі)	Геометричні пропорції та просторове розміщення носа, очей, скул

Серед динамічних методів біометричної ідентифікації кожен має свої особливості, переваги та певні обмеження, які слід враховувати під час вибору технології для практичного використання (див. таблицю 1.3). Голосова ідентифікація базується на аналізі акустичних характеристик мовлення, таких як частота, тембр, інтонація, тощо. Цей метод є досить зручним, не потребує складного обладнання та може бути реалізований навіть через звичайні мобільні телефони. Проте на якість розпізнавання можуть впливати фоновий шум, мікрофонні перешкоди або фізичний стан користувача, наприклад, застуда.

Рукописний підпис, що використовується як динамічна біометрична ознака, включає аналіз не лише зовнішнього вигляду підпису, але й його поведінкових характеристик – швидкості руху, натиску пера, напрямку ліній, прискорення та ритму. Такі параметри дозволяють виявити спроби підробки

або неавтентичного виконання підпису. Разом з тим, для повноцінного застосування цього методу необхідне спеціальне обладнання, зокрема графічні планшети або стилуси з функцією тиску [7, 8].

Таблиця 1.3.

Порівняльна таблиця динамічних біометричних методів ідентифікації

Біометрична характеристика	Реєструючий пристрій	Тип зразка	Досліджувані риси
Голос	Мікрофон, телефон, аудіоінтерфейс	Запис голосу	Частотні характеристики, мел–кепстральні коефіцієнти, інтонація, ритм, тембр, тривалість звуків
Рукописний підпис	Графічний планшет, цифрове перо	Динамічний підпис	Швидкість руху, тиск пера, порядок ліній, кут нахилу, прискорення, ритм написання
Клавіатурний почерк	Комп’ютерна клавіатура	Ритм набору тексту	Час натискання та відпускання клавіш, інтервали між натисканнями, послідовність введення символів
Динаміка руху миші	Комп’ютерна миша, сенсорна панель	Траєкторія руху курсора	Швидкість переміщення, прискорення, кути повороту, ритм руху, характерні точки траєкторії

Клавіатурний почерк – ще один перспективний метод, що аналізує ритміку та часові характеристики введення тексту користувачем. Це включає фіксацію часу натискання й відпускання клавіш, а також інтервалів між окремими символами. Цей метод має перевагу непомітної інтеграції у фоновому режимі, не потребує додаткового обладнання і може бути використаний у процесі звичайної роботи з комп’ютером. Однак точність такого розпізнавання може варіюватися в залежності від настрою, втоми або фізичного стану користувача.

Динаміка руху миші базується на аналізі траєкторії переміщення курсора, включаючи швидкість, напрямок, прискорення, кути повороту та характерні точки траєкторій. Кожен користувач має індивідуальні патерни взаємодії з маніпулятором, що дозволяє сформувати унікальний цифровий профіль. Цей метод є особливо привабливим для впровадження в системи онлайн–ідентифікації, оскільки не потребує зміни інтерфейсу чи втручання в процес роботи користувача. Водночас, точність може знижуватись у разі використання різних пристроїв (наприклад, миші та сенсорної панелі) або при зміні налаштувань системи [7, 8].

Усі ці динамічні методи мають великий потенціал для подальшого розвитку, зокрема, у контексті багатофакторної автентифікації та систем поведінкової безпеки, де важлива не лише унікальність, але й здатність до постійного фонової перевірки особи без порушення її звичайної взаємодії з пристроєм.

Однією з ключових переваг динамічних методів біометричної ідентифікації, зокрема технологій, що базуються на аналізі інформаційного (клавіатурного) почерку, є їхня економічність та простота впровадження. Відсутність необхідності у спеціалізованому дорогому обладнанні, як–от сканери сітківки ока або системи високої точності, робить ці технології особливо привабливими для масового застосування. Реалізація таких рішень дозволяє здійснювати неперервний моніторинг доступу до конфіденційних даних, забезпечуючи захист від несанкціонованого проникнення, витоків інформації та кібершпигунства [4–7].

Варто підкреслити, що найвищий рівень безпеки досягається при використанні комбінованих систем автентифікації, які поєднують кілька біометричних підходів або інтегрують біометрію з іншими апаратними засобами ідентифікації. Такий мультифакторний підхід дозволяє створити багаторівневу архітектуру захисту, яка значно ускладнює спроби обходу системи. Надійність та ефективність подібних рішень підтверджується зростаючим інтересом з боку провідних розробників програмного

забезпечення та кібербезпеки, які активно впроваджують ці технології у свої продукти [4–6, 8].

1.3. Принципи біометричної ідентифікації та автентифікації

Біометрична ідентифікація та автентифікація ґрунтуються на використанні унікальних фізіологічних і поведінкових характеристик особи для її достовірного розпізнавання в інформаційних та фізичних системах. Основні принципи цих процесів можна умовно поділити на кілька ключових категорій. До першої відносяться традиційні методи на кшталт парольного захисту, які, хоча й не є біометричними за своєю суттю, часто поєднуються з біометричними засобами у рамках мультифакторної автентифікації. Друга категорія охоплює методи перевірки фізичних параметрів – це відбитки пальців, структура обличчя, геометрія руки, райдужна оболонка, сітківка та венозний малюнок. Третя група базується на психофізіологічних особливостях, зокрема аналізі голосу, стилю підпису, клавіатурного почерку. Четвертий напрям – новітній і перспективний – включає інтелектуальні системи, що враховують інформаційну поведінку користувача: коло інтересів, стиль взаємодії з системою, траєкторії миші, час активності тощо.

Узагальнено принцип дії біометричних систем складається з двох основних етапів – реєстрації та ідентифікації. На першому етапі відбувається зчитування унікального біометричного зразка за допомогою відповідного пристрою. Цей зразок обробляється програмними алгоритмами з метою виділення значущих ознак, які кодуються в цифровий шаблон. Важливо підкреслити, що система не зберігає оригінальне зображення (наприклад, фото обличчя чи сітківки), а лише математично оброблений шаблон, що дозволяє зменшити ризик витоку персональних даних. Кількість і тип алгоритмів обробки залежать від виду біометричної ознаки: для відбитків пальців і райдужки вони будуть суттєво відрізнятися від методів для аналізу голосу чи підпису [4, 6, 8].

Після завершення реєстрації система готова до виконання своєї основної функції – автентифікації користувача. Тут виділяють два базових підходи: ідентифікацію та верифікацію. Ідентифікація є процесом типу «один–до–багатьох», коли наданий зразок порівнюється з усіма шаблонами в базі даних з метою визначення найбільш імовірного збігу. Це поширений підхід у криміналістиці або в системах відеоспостереження у громадських місцях. Верифікація, натомість, передбачає порівняння «один–до–одного» – тобто система перевіряє, чи відповідає наданий біометричний зразок конкретному шаблону, попередньо визначеному користувачем, наприклад, при вході в обліковий запис чи доступі до банківських операцій. Для цього необхідно додатково вказати свій ідентифікатор (логін, номер картки, ID), щоб система знала, з яким шаблоном здійснювати порівняння.

Типова архітектура біометричної системи, включаючи обидва процеси – реєстрації та автентифікації – представлена на рис. 1.2. Ця схема демонструє поетапну обробку біометричних даних – від зчитування до прийняття рішення про дозвіл або заборону доступу [7-9].

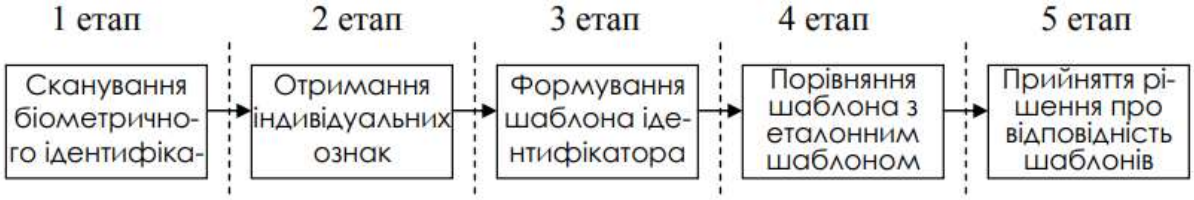

Рис. 1.2. Загальний алгоритм функціонування систем біометричної ідентифікації

Після завершення етапу реєстрації система переходить у режим постійного функціонування, де її завданням є визначення особи та надання відповідних прав доступу до системи або її ресурсів. Залежно від цілей і контексту використання, система може працювати у режимі ідентифікації (пошук у базі) або верифікації (підтвердження заявленої особи). Наприклад, у сферах безпеки на транспортних вузлах (вокзали, аеропорти) частіше використовуються ідентифікаційні режими, тоді як у банківській справі,

електронному урядуванні чи корпоративному середовищі – верифікаційні механізми (рис. 1.3) [8, 9].

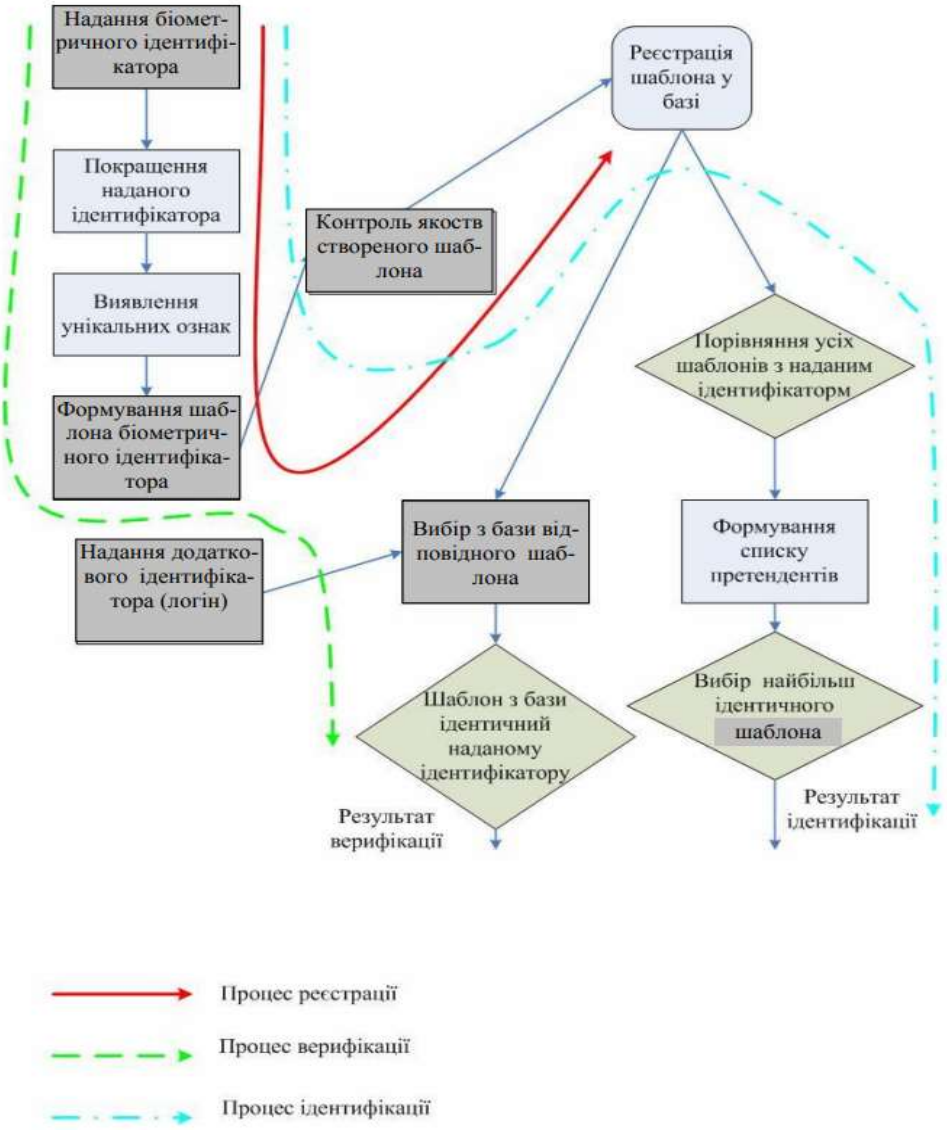

Рис. 1.3. Загальна схема функціонування системи біометричної ідентифікації

Таким чином, принципи біометричної ідентифікації та автентифікації ґрунтуються на поєднанні унікальності біометричних ознак, безпечного способу їх збереження (через шаблони), та ефективних алгоритмів зіставлення, що забезпечують як точність, так і швидкість розпізнавання користувача в реальному часі. Удосконалення таких систем передбачає впровадження адаптивних моделей, здатних враховувати змінність параметрів користувача без втрати точності.

1.4. Переваги та недоліки біометричних технологій

Сучасні біометричні технології ідентифікації та автентифікації відіграють ключову роль у системах інформаційної безпеки, пропонуючи більш надійні, зручні та персоналізовані методи підтвердження особистості порівняно з традиційними механізмами, такими як паролі, PIN–коди чи смарт–картки. Незважаючи на численні переваги, впровадження біометрії супроводжується певними технологічними, етичними та правовими викликами [8, 9].

Сформулюємо переваги біометричних систем [7–9].

1) Унікальність та складність підробки. Біометричні характеристики є винятковими для кожної людини, що робить їх значно складнішими для копіювання чи несанкціонованого дублювання у порівнянні з паролями або фізичними ключами.

2) Швидкість розпізнавання. Сучасні біометричні системи здатні здійснити процес ідентифікації протягом декількох секунд. Наприклад, аналіз відбитка пальця або райдужної оболонки ока зазвичай триває 1–2 секунди, що забезпечує ефективність у режимі реального часу.

3) Неможливість втрати або забуття. Оскільки біометричні ознаки є невід’ємною частиною людського тіла, користувачеві не потрібно нічого запам’ятовувати або носити із собою.

4) Зручність для користувачів. Біометричні технології не вимагають від користувача додаткових дій, окрім звичної поведінки (дотик, погляд, розмова), що робить процес автентифікації інтуїтивно зрозумілим і комфортним.

5) Масова доступність. Завдяки мініатюризації технологій та їхній інтеграції у смартфони, банкомати, системи доступу, біометричні засоби стали доступними як для корпоративного, так і для побутового застосування.

6) Підвищена точність і стабільність. Біометричні системи здатні забезпечувати високу точність розпізнавання навіть у складних умовах, якщо застосовуються комбіновані алгоритми верифікації.

До недоліків та ризиків біометричних технологій можна віднести наступне [6, 7].

1) Незворотність біометричних даних. На відміну від паролів, біометричні ознаки неможливо змінити у разі їх компрометації. Це створює серйозні ризики у випадку витоку даних, оскільки "новий відбиток пальця" створити неможливо.

2) Залежність від фізичного стану користувача. Травми, ампутації, вікові зміни або хвороби можуть змінити або деформувати біометричні ознаки, що призводить до хибних відмов у доступі або потреби в оновленні еталонних шаблонів.

3) Вартість впровадження. Хоча кінцеве використання біометричних пристроїв може бути економним, первинна розробка, закупівля високоточного обладнання та інтеграція в існуючі системи потребують значних фінансових ресурсів.

4) Загроза конфіденційності. Біометричні дані є особливо чутливими і, у разі витоку, можуть надати зловмисникам доступ не лише до цифрових, а й до медичних або юридичних ресурсів користувача. Захист таких даних вимагає суворого дотримання стандартів шифрування та зберігання.

5) Юридичні та етичні питання. Залишається відкритим питання використання біометричних даних без згоди особи, наприклад, у системах відеоспостереження, що може призвести до зловживань з боку державних або комерційних структур.

6) Потреба в нормативному регулюванні. З огляду на зростання масштабів використання біометрії, постає потреба у створенні відповідної законодавчої бази, яка регламентуватиме порядок збору, обробки, зберігання та знищення біометричних даних.

7) Технологічні обмеження. У разі використання некаліброваних або низькоякісних зчитувальних пристроїв (наприклад, дешевих сканерів), точність системи значно знижується, що може створити ризики як безпеки, так і зручності.

Таким чином, біометричні технології мають значний потенціал у контексті підвищення рівня безпеки та автоматизації процесів автентифікації. Водночас їх успішне впровадження вимагає збалансованого підходу, врахування технічних, етичних і правових аспектів, а також належного захисту персональних біометричних даних користувачів.

РОЗДІЛ 2
АНАЛІЗ ІСНУЮЧИХ СИСТЕМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПОМ

2.1. Основні вимоги до систем біометричної ідентифікації та аутентифікації в автоматизованих системах керування доступом

Біометричні технології ідентифікації та аутентифікації особи передбачають використання унікальних фізіологічних або поведінкових ознак людини для підтвердження її особистості. До таких ознак належать: відбитки пальців, структура обличчя, голос, форма кисті, візерунок райдужної оболонки ока, термографічні зображення та інші характеристики [6–8].

Сучасні системи біометричного контролю доступу застосовуються з метою забезпечення безпечної та точної перевірки особи. Вони аналізують і зіставляють біометричні дані користувача з еталонною інформацією, що дозволяє приймати рішення про надання чи обмеження доступу до певних об’єктів, приміщень або інформаційних систем залежно від прав користувача. Такі рішення значно підвищують ефективність процедур ідентифікації та рівень захисту від несанкціонованого доступу.

Щоб такі системи були ефективними та надійними, до них висувається низка технічних та експлуатаційних вимог:

– висока точність розпізнавання. Система має точно визначати особу, зводячи до мінімуму ймовірність помилкової ідентифікації або пропуску користувача;

– швидкодія. Процес ідентифікації та надання доступу повинен відбуватись миттєво, без затримок, щоб не створювати перешкод у проході чи роботі персоналу;

– надійність захисту. Необхідно гарантувати стійкість системи до несанкціонованого доступу, підробки біометричних ознак та зовнішніх атак;

– мінімізація хибних спрацьовувань. Надійна система повинна забезпечувати мінімальний рівень помилок першого роду (відмова у доступі легальним користувачам) і другого роду (допуск неавторизованих осіб);

– зручність у користуванні. Інтерфейс має бути простим і доступним для користувачів без спеціальної технічної підготовки;

– інтеграція з іншими системами. Система має безперешкодно взаємодіяти з іншими елементами інфраструктури безпеки, такими як відеоспостереження, сигналізація, системи обліку робочого часу тощо;

– стійкість до впливу навколишнього середовища. Умови експлуатації можуть бути несприятливими – пил, вологість, низькі або високі температури. Біометричні пристрої повинні стабільно працювати в таких умовах;

– захист персональних даних. Обробка біометричної інформації має здійснюватися з дотриманням вимог конфіденційності згідно із законодавством у сфері захисту персональних даних;

– економічна доцільність. Рішення має бути вартісно ефективним – як з точки зору впровадження, так і технічного обслуговування [8].

Використання систем біометричної ідентифікації та аутентифікації в автоматизованих системах контролю доступу є надзвичайно актуальним напрямом, що має великий потенціал для подальшого розвитку. Такі технології здатні суттєво підвищити рівень безпеки, оптимізувати доступ до ресурсів та об'єктів, а також підтримувати надійний контроль за переміщенням персоналу. Разом із перевагами, впровадження таких систем потребує врахування ряду критичних аспектів: точність розпізнавання, швидкість обробки, зручність користування, стійкість до зовнішніх впливів, інтеграція з іншими системами безпеки та відповідність нормам захисту персональних даних. Крім того, важливим є правильний вибір біометричної технології відповідно до специфіки об'єкта та поставлених задач [6–9].

2.2. Аналіз існуючих систем біометричної ідентифікації та аутентифікації в автоматизованих системах

Біометричні системи ідентифікації та аутентифікації використовуються для визначення або підтвердження особи на основі унікальних фізіологічних або поведінкових характеристик. До основних методів належать:

– відбитки пальців – аналізують унікальні візерунки на поверхні пальців;

– розпізнавання обличчя – використовує геометричні та текстурні ознаки обличчя;

– сканування радужки – базується на аналізі неповторного малюнка райдужної оболонки ока;

– голосова ідентифікація – ідентифікує особу за характеристиками її голосу [8, 9].

Залежно від рівня захисту, можуть застосовуватись такі типи аутентифікації:

– однофакторна аутентифікація – верифікація здійснюється за одним біометричним параметром;

– двофакторна аутентифікація – комбінує біометричний параметр з додатковим фактором (наприклад, PIN-кодом або карткою доступу).

У системах контролю доступу ці технології дозволяють:

– підвищити рівень безпеки завдяки унеможливленню використання чужих даних;

– забезпечити швидкий та зручний вхід уповноважених осіб;

– здійснювати облік переміщення та присутності користувачів у захищених зонах [8, 9].

На рис. 2.1 представлено розподіл використання біометричних систем у різних сферах діяльності. Зображення ілюструє, в яких галузях біометричні технології впроваджуються найактивніше, включаючи державний сектор, банківську справу, охорону здоров’я, транспорт, освіту та інші. Такий аналіз

дозволяє оцінити актуальність і потенціал застосування біометричних методів для ідентифікації та аутентифікації в системах контролю доступу [9].

Рис. 2.1. Структура застосування біометричних систем у різних галузях

Згідно з аналізом предметної області, було визначено ключові напрямки застосування біометричних систем в системах контролю доступом, що представлено в таблиці 2.1. З таблиці можна зробити кілька ключових висновків щодо застосування біометричних систем для контролю доступу. По-перше, ці системи мають значні переваги у підвищенні безпеки, зручності та дисципліни. Вони забезпечують точний облік доступу та присутності, що знижує ймовірність людських помилок та шахрайства. Біометрія також дозволяє зменшити ризики несанкціонованого доступу до важливих об'єктів або інформації, завдяки унікальним характеристикам кожної людини [9, 10].

По-друге, біометричні системи можуть бути ефективними для різних типів об'єктів, від контролю доступу на охоронювані території до індивідуальних сейфів і відеоспостереження, надаючи можливість забезпечити високий рівень захисту та зручність для користувачів. Водночас, використання таких систем зменшує необхідність зберігання паролів або інших персональних ідентифікаційних засобів, що може бути вразливим до втрати або крадіжки.

Таблиця 2.1.

Використання біометричних систем для контролю доступу

Тип біометричної системи	Переваги від впровадження біометрії	Необхідне обладнання
Системи контролю доступу на охоронювані об'єкти	Покращення безпеки та зручності для отримання доступу	Біометричні термінали, автономні замки з вбудованими сканерами відбитків пальців
Системи ідентифікації працівників служби охорони при обході периметра	Підвищення дисципліни при обходах та виконанні маршруту в певний час	Біометричні термінали
Системи обліку робочого часу для фіксації присутності працівників на робочому місці	Забезпечення точності обліку робочого часу, підвищення дисципліни	Біометричні термінали, біометричні сканери, автономні системи обліку часу
Індивідуальні сейфи з доступом через біометрію	Збільшення рівня безпеки та зручності використання сейфів в критичних умовах	Автономний біометричний замок для сейфа
Системи відеоспостереження з розпізнаванням осіб	Зниження ризиків терористичних актів та заворушень на об'єктах стратегічного значення	Програмні засоби розпізнавання осіб з відеопотоків
Інформаційні термінали для доступу до захищеної інформації	Покращення захисту інформації та зручності доступу	Вбудовані сканери для ідентифікації особи

Основні переваги біометричних систем контролю доступу полягають у їхній простоті використання, швидкодії та зручності для користувача. Вони ефективно вирішують низку проблем, пов'язаних з людським фактором, таких як втрата доступу, необхідність зберігання паролів або кодів ідентифікації. Оскільки біометричні характеристики людини є унікальними,

їх неможливо підробити або використати зловмисниками, що забезпечує високий рівень безпеки.

Проте, до недоліків таких систем можна віднести ймовірність помилок розпізнавання, потребу у спеціалізованому обладнанні, а також складність в обслуговуванні та супроводі, що може спричиняти високі витрати на їх впровадження та підтримку.

Але, незважаючи на це, загальні тенденції розвитку вказують на зростання попиту на біометричні технології як у корпоративному, так і в особистому користуванні. Отримані результати є підґрунтям для переходу до наступного етапу дослідження – розробки власної системи біометричної ідентифікації та аутентифікації для автоматизованої системи контролю доступу, яка враховуватиме переваги існуючих рішень і мінімізуватиме їх недоліки.

РОЗДІЛ 3
РОЗРОБКА СИСТЕМИ БІОМЕДИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ ДЛЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ

3.1 Вибір біометричних ознак

Розробка систем біометричної ідентифікації та аутентифікації для автоматизованих систем керування доступом передбачає врахування низки технічних та експлуатаційних факторів. До таких факторів належать: пропускна здатність системи, її надійність, вартість впровадження, ергономічність, рівень захисту персональних даних, точність розпізнавання та продуктивність в умовах реального часу. Обґрунтований вибір біометричних ознак дозволяє забезпечити ефективне функціонування системи в умовах підвищених вимог до безпеки. Загалом, біометричні ознаки поділяють на дві основні категорії: фізіологічні (відбитки пальців, геометрія обличчя, сітківка та райдужна оболонка ока, форма вуха тощо) та поведінкові (голос, динаміка підпису, темп введення тексту тощо). Кожна з цих ознак має свої переваги й обмеження, тому їх вибір повинен базуватись на специфіці задачі, умовах функціонування та доступному технічному забезпеченні [8, 9].

Серед найпоширеніших ознак, що застосовуються у системах доступу, є:

– відбитки пальців – забезпечують високу точність, швидкість розпізнавання та широке поширення сенсорів. Системи на їх основі становлять значну частку ринку біометричної ідентифікації;

– геометрія обличчя – є безконтактним методом, що дозволяє проводити розпізнавання без фізичної взаємодії з пристроєм. Це знижує ризики поширення забруднень або інфекцій, а також забезпечує високий

рівень зручності. Найчастіше використовується у системах відеоспостереження та контролю на великих об’єктах;

– райдужна оболонка ока – одна з найнадійніших біометричних ознак, але вимагає наявності високоточних зчитувальних пристроїв і відповідних умов освітлення [8, 9].

Згідно з аналітичними даними [10, 11], понад 80% сучасних біометричних систем ґрунтуються саме на трьох згаданих ознаках. Зокрема, технології розпізнавання обличчя активно використовуються у випадках, коли фізичний контакт із пристроєм небажаний або неможливий, наприклад, при дистанційній ідентифікації через відеокамери спостереження. Однак ефективність таких рішень істотно знижується при великій кількості користувачів у базі даних та в умовах високого потоку людей.

У таблиці 3.1 наведено порівняльні характеристики біометричних ознак за основними критеріями, зокрема рівнем помилок FAR (False Acceptance Rate) та FRR (False Rejection Rate), що дозволяє обґрунтовано підійти до вибору ознаки з урахуванням вимог до точності та надійності системи [11, 12].

Як видно з таблиці, найнижчий рівень хибного допуску (FAR) спостерігається у систем, що базуються на скануванні райдужної оболонки (0,00001%). Цей метод також демонструє найвищу точність ідентифікації – понад 99,94%, а стабільність біометричного шаблону залишається незмінною протягом усього життя користувача.

Водночас технології 2D–розпізнавання обличчя, хоч і є зручними у впровадженні, показують вищий рівень помилок – зокрема, показник FRR сягає 7%, що свідчить про ризик частих відмов у доступі. Більш точним, але і дорожчим є 3D–аналіз обличчя, який, окрім високої точності (99,95%), вирізняється кращими характеристиками захищеності та стійкості до зовнішніх чинників [12].

Найбільш збалансованим за параметрами «ціна–якість–зручність» залишаються системи, побудовані на основі відбитків пальців. Вони

демонструють високу точність, швидкодію та простоту експлуатації, а також не потребують надто дорогого обладнання, що є важливим чинником при впровадженні в автоматизовані системи контролю доступу [12].

Таблиця 3.1.

Порівняльна характеристика біометричних методів ідентифікації

Критерій оцінювання	Відбитки пальців	2D–аналітика обличчя	3D–моделювання обличчя	Аналіз райдужної оболонки
Ймовірність хибного дозволу (FAR), %	0,001	0,1	0,005	0,00001
Ймовірність хибного відхилення (FRR), %	0,6	7	0,1	0,1
Успішність автентифікації (ATV), %	99,39	92,91	99,895	99,899
Рівень точності розпізнавання, %	99,69	96,45	99,948	99,949
Максимальна рекомендована кількість користувачів	316	35	141	3162
Оцінка захищеності (за шкалою 1–10)	6	4	9	10
Стійкість до навколишніх факторів (1–10)	10	6	8	9
Зручність експлуатації (1–10)	9	6	10	8
Витрати на впровадження (1–10)	10	10	5	7
Швидкість виконання (1–10)	10	10	7	10
Стабільність біометричної ознаки в часі (1–10)	9	8	10	10

Проведений аналіз дозволяє дійти висновку, що системи біометричного контролю доступу, які базуються на скануванні райдужної оболонки ока, доцільно впроваджувати на середніх та великих підприємствах, а також на об’єктах стратегічної важливості, де забезпечення максимальної безпеки є критичним. Водночас, у випадку об’єктів із чисельністю персоналу до декількох сотень осіб найбільш ефективним рішенням є впровадження

технологій ідентифікації за відбитками пальців, зважаючи на їхню надійність, зручність та відносну дешевизну впровадження [11, 12].

Серед усіх методів дактилоскопія є однією з найстаріших і найбільш досліджених технологій біометричної ідентифікації. Її розвиток отримав потужний імпульс завдяки широкому застосуванню у криміналістиці протягом XX століття. Основний принцип цієї технології полягає в аналізі унікального візерунка папілярних ліній на поверхні пальців людини. Алгоритми ідентифікації базуються на виявленні і порівнянні характерних точок візерунка – закінчень ліній, розгалужень та окремих точок – із шаблонами, збереженими в базі даних [11–13].

Окрім виявлення точкових особливостей, сучасні системи аналізують морфологічну структуру відбитка: взаємне розташування закритих ліній, спіралей, дуг тощо. В результаті формується цифровий шаблон біометричної характеристики особи, який забезпечує високу точність ідентифікації та не втрачає інформативності навіть у разі часткового пошкодження відбитка.

Існує два основні підходи до порівняння біометричних даних із шаблонами в базі: перший орієнтований на аналіз розташування характерних точок, другий – на загальний рельєф відбитка. Використання гібридного підходу, який поєднує обидва методи, забезпечує підвищену точність і стійкість до збоїв.

Процедура біометричної реєстрації включає сканування одного або кількох пальців, цифрову обробку зображення та виділення ключових ознак – типу точки, її положення та орієнтації. Ці дані формують індивідуальний шаблон, який зберігається для подальшого порівняння у процесі аутентифікації (рис. 3.1).

Рис. 3.1. Процес дактилоскопічного розпізнавання

Процес ідентифікації особи за допомогою відбитків пальців базується на зіставленні отриманого під час сканування біометричного шаблону з відповідними еталонними даними, що зберігаються у базі. У разі встановлення достатнього рівня збігу, система приймає рішення про успішну верифікацію або ідентифікацію особи. Завдяки своїй ефективності та простоті, даний метод отримав найширше розповсюдження як у професійному середовищі (наприклад, доступ до корпоративних мереж), так і в повсякденному житті (розумні замки, мобільні пристрої) [11, 12].

Проте, незважаючи на високі показники точності, постають питання щодо захисту від потенційного несанкціонованого доступу. Існує ризик фальсифікації відбитків за допомогою різних технологічних прийомів. Наприклад, можливе створення штучного відбитка шляхом виготовлення копії пальця або руки із нанесеним на нього візерунком папілярних ліній. Для протидії таким загрозам у сучасних пристроях передбачене використання інфрачервоних сенсорів, які здатні виявляти теплове випромінювання, притаманне лише живій тканині, тим самим забезпечуючи базову перевірку життєздатності об'єкта сканування [10, 12].

Ще одним потенційним способом обману є перенесення зображення відбитка зловмисником на власні пальці за допомогою спеціальних матеріалів або плівок. У такому випадку потрібно мати високоякісне

зображення відповідного пальця саме тієї особи, яка зареєстрована в системі, що значно ускладнює спробу злому [13].

Серед основних переваг ідентифікації за відбитками пальців можна виділити:

– високий рівень точності й надійності ідентифікації;

– доступність та відносно невисока вартість необхідного обладнання;

– простота та швидкість процедури сканування.

До основних обмежень методу належать:

– вразливість до механічних пошкоджень поверхні шкіри (подряпини, порізи);

– потенційна можливість копіювання відбитка і використання для несанкціонованого доступу;

– необхідність постійного контролю за станом сенсорів для забезпечення точності зчитування [14].

3.2. Проєктування системи біометричної ідентифікації та автентифікації

У зв’язку з тим, що на попередньому етапі було обрано відбитки пальців як основну біометричну характеристику, нижче розглянемо етапи створення системи біометричної ідентифікації та автентифікації, яка ґрунтується саме на цьому типі даних [11–13].

Розглянемо апаратне забезпечення системи біометричної ідентифікації та автентифікації:

– сканер відбитків пальців (рис. 3.2) – головний елемент системи, який виконує зчитування унікального малюнка папілярних ліній. Залежно від умов застосування та бюджету, використовуються оптичні, ємнісні або ультразвукові сканери;

– контролер – електронний блок, що відповідає за обробку сигналів з датчика та первинне зіставлення отриманих даних зі збереженими шаблонами;

– процесор – обчислювальний модуль, який виконує програмні алгоритми ідентифікації;

– сховище даних – забезпечує збереження біометричних шаблонів та супровідної інформації про користувачів.

Рис. 3.2. Типи сканерів відбитків пальців: ультразвуковий, оптичний, ємнісний

Для коректної роботи системи необхідне багаторівневе програмне забезпечення, що включає:

– модуль збору біометричних даних;

– програмні засоби для попередньої обробки зображень;

– механізм порівняння шаблонів;

– інструменти для управління правами доступу;

– додаткові функціональні блоки – реєстрація нових користувачів, логування подій тощо.

Тепер розглянемо організацію зберігання інформації. Біометрична база даних – містить зашифровані шаблони відбитків пальців, які необхідно захистити від стороннього доступу. Журнали активності – фіксують усі події в системі, включаючи час доступу, дії користувача та відповідні ресурси.

Для узагальнення принципів функціонування системи автентифікації за допомогою біометричних характеристик розроблено класифікаційну схему (рис. 3.3) [14].

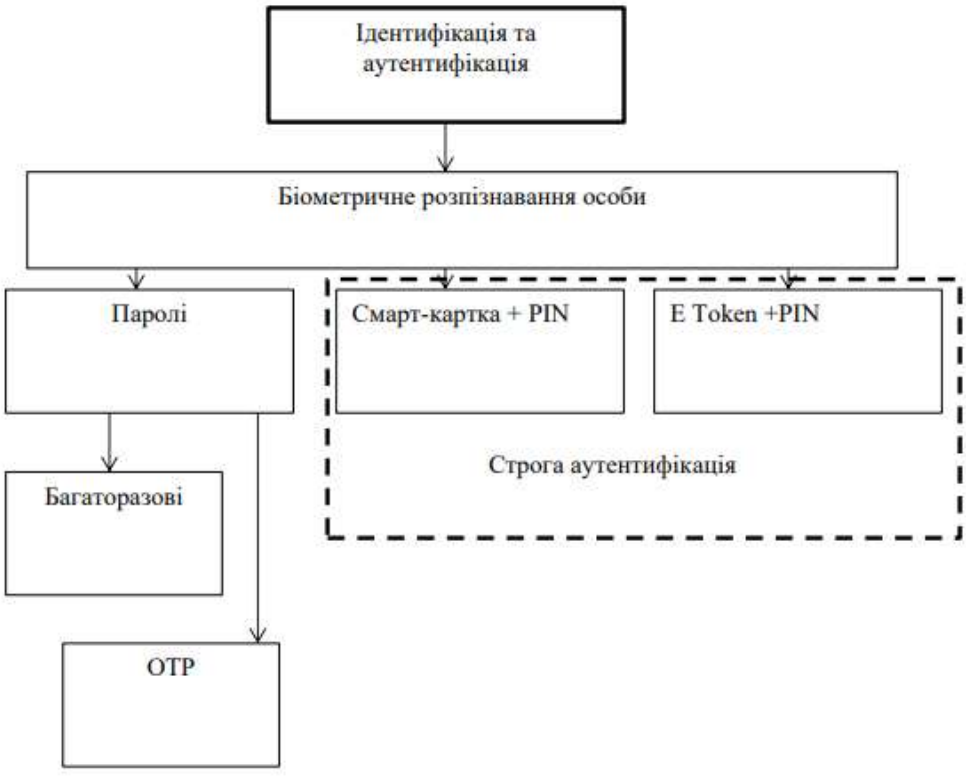

Рис. 3.3. Схема автентифікації з використанням біометричних параметрів

Розглянемо алгоритм функціонування системи (рис. 3.4).

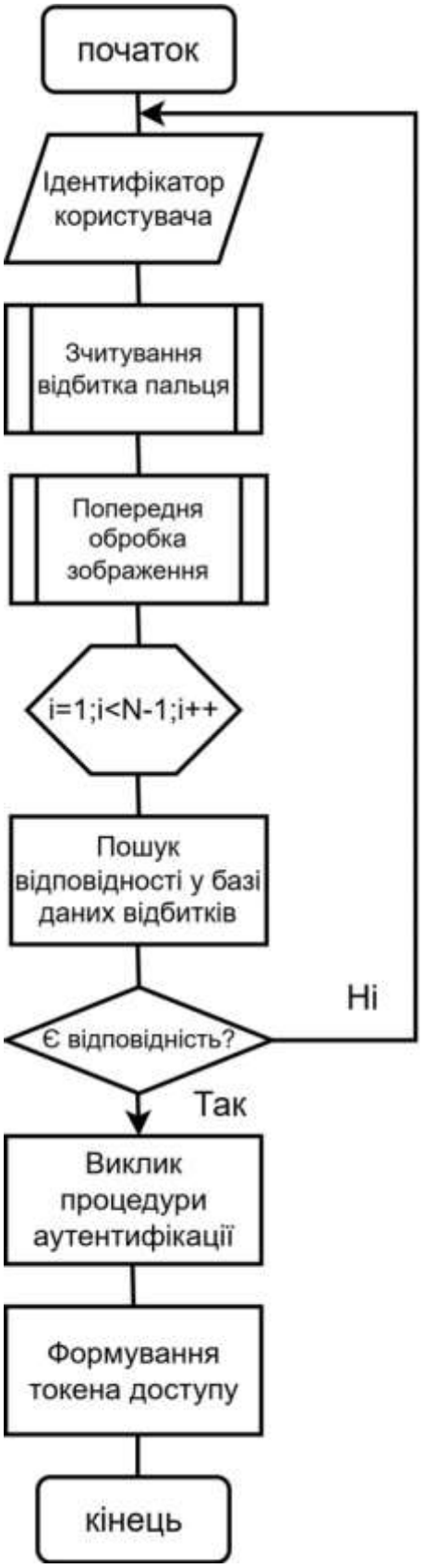

Рис. 3.4. Алгоритм ідентифікації з використанням відбитків пальців

Автентифікація у запропонованій системі здійснюється за наступною послідовністю дій:

1) оброблене зображення відбитка пальця потрапляє до модуля збору даних, де відбувається його оцифрування;

2) потім цифрове зображення обробляється для виділення вектору параметрів – контрольних точок папілярного візерунка;

3) отриманий вектор порівнюється із шаблонами, що зберігаються у базі даних;

4) після цього здійснюється перевірка введеного ідентифікатора (логіну);

5) для підтвердження особи вводиться пароль користувача.

На рис. 3.5 подано узагальнену схему системи біометричної автентифікації, яка демонструє взаємозв’язок основних елементів системи.

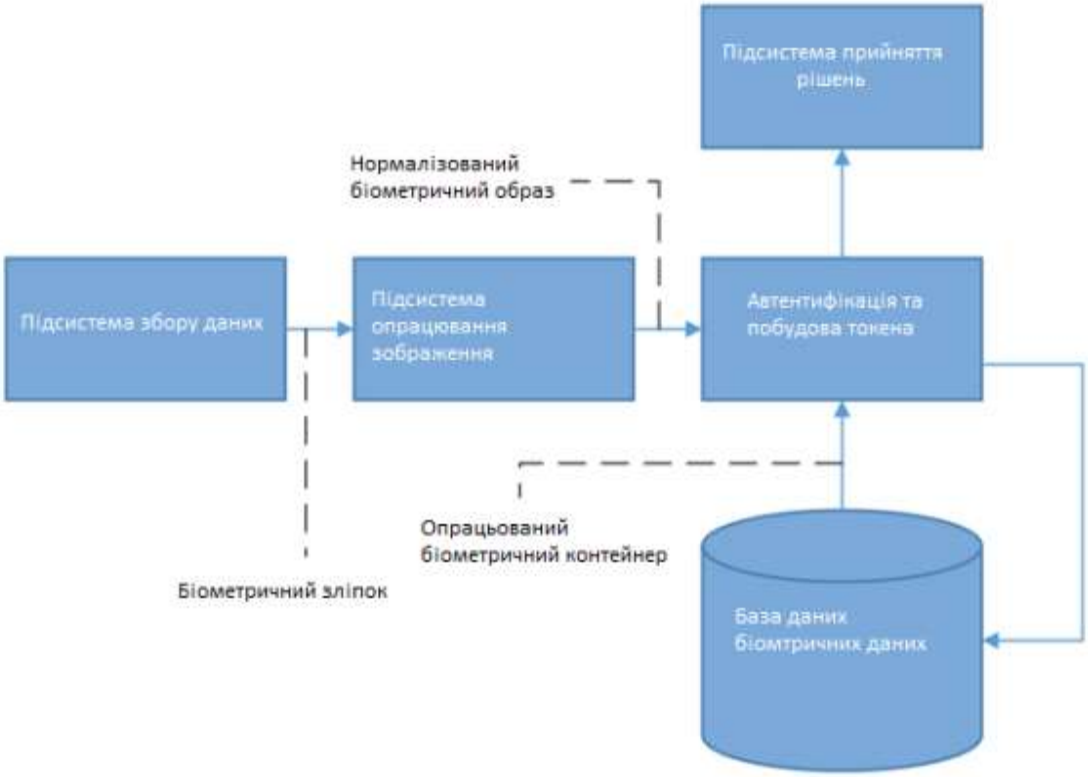

Рис. 3.5. Схема системи біометричної автентифікації

3.3. Інструментальні засоби розробки програмного забезпечення

Для створення програмного забезпечення системи біометричної ідентифікації та автентифікації було використано інтегроване середовище розробки PyCharm 2024.1.1. Це сучасне IDE, спеціалізоване на розробці з використанням мови програмування Python, яке забезпечує повноцінну підтримку всього циклу створення програмного забезпечення: від написання коду до тестування, налагодження та розгортання.

До основних переваг PyCharm належать:

- інтелектуальний редактор коду з функцією автодоповнення, підсвічуванням синтаксису та виявленням помилок у режимі реального часу;
- інтеграція з системами контролю версій (Git, Mercurial, SVN);
- вбудовані засоби тестування;
- зручна робота з базами даних через графічний інтерфейс;
- підтримка віртуального середовища та гнучка система розширення функціоналу за допомогою плагінів [12–14].

Як основну мову програмування обрано Python – потужну, гнучку та зручну мову високого рівня, яка користується великою популярністю в науковій і прикладній сфері. Її простий та лаконічний синтаксис дозволяє швидко опановувати програмування навіть початківцям, а також значно скорочує час розробки. Python ідеально підходить для реалізації різноманітних компонентів системи біометричної ідентифікації та автентифікації, зокрема для обробки біометричних зображень, виділення ознак, порівняння шаблонів, організації збереження та обробки даних у базах даних, а також для побудови графічного інтерфейсу користувача [12–14].

Широкий набір спеціалізованих бібліотек робить Python особливо ефективним у задачах біометрії:

- OpenCV використовується для обробки зображень і відео;
- NumPy і SciPy – для математичних розрахунків та чисельного аналізу;
- Scikit–learn – для реалізації алгоритмів машинного навчання;

- Matplotlib і Seaborn – для візуалізації результатів;

- TensorFlow або Keras – для побудови моделей глибокого навчання у разі потреби.

Крім того, Python забезпечує хорошу інтеграцію з іншими мовами програмування, такими як C або C++, що дозволяє ефективно працювати з драйверами пристроїв, наприклад, сканерів відбитків пальців. Активна спільнота користувачів Python є додатковою перевагою, адже забезпечує швидкий доступ до технічної підтримки, численних форумів і навчальних матеріалів.

3.4. Розробка програмного забезпечення системи біометричної ідентифікації та автентифікації

Переходимо до практичного етапу реалізації. На етапі практичної реалізації системи біометричної ідентифікації розглянемо процес побудови програмного модуля для зіставлення відбитків пальців з використанням бібліотеки OpenCV. Почнемо з огляду процесу підключення бібліотеки OpenCV, яка є одним із основних інструментів для обробки зображень у Python. Першим кроком є імпортування самої бібліотеки. Найпоширенішим способом цього є використання команди: import cv2

Далі проаналізуємо фрагмент коду, який реалізує алгоритм зіставлення відбитків пальців. У цьому рішенні використано метод масштабно–інваріантного перетворення ознак (SIFT), що входить до складу бібліотеки OpenCV. Програма приймає зображення еталонного відбитка пальця як вхідний параметр і виконує порівняння з великою кількістю інших зображень (кандидатів), щоб визначити найкращий збіг за ознаками.

Суть алгоритму полягає у виявленні ключових точок (характерних ознак) на кожному зображенні, а також у розрахунку дескрипторів – числових векторів, що описують локальні особливості кожної ключової точки. Далі ці дескриптори використовуються для пошуку можливих

відповідностей між еталонним та кандидатськими зображеннями за допомогою методу найближчого сусіда. Отримані відповідності додатково фільтруються за допомогою співвідношення відстаней, після чого обчислюється узагальнена оцінка на основі кількості якісних (good) збігів. Зображення–кандидат з найвищою оцінкою вважається найкращим збігом з еталоном.

Програмний модуль виконує наступні дії:

– завантажує еталонне зображення та кожне зображення–кандидат з файлової системи;

– витягує ключові точки та дескриптори за допомогою SIFT;

– здійснює пошук відповідностей між ознаками з використанням алгоритму k–NN;

– виконує фільтрацію відповідностей на основі співвідношення відстаней;

– обчислює відсоткову оцінку відповідності та зберігає найкращий результат;

– виводить зображення з візуалізацією співпадаючих ключових точок.

Метод розпізнавання відбитків пальців є широко застосовуваним у системах ідентифікації особистості, особливо в галузі безпеки. Висока точність і стійкість таких алгоритмів мають вирішальне значення для їх ефективного впровадження. У запропонованій реалізації використовується набір зображень відбитків пальців, що містить 6000 зразків, зібраних у реальних умовах, для тестування та оцінки алгоритму.

Цей набір даних включає зображення відбитків пальців людей різного віку, статі та етнічного походження. Така різноманітність дозволяє алгоритму зіставлення навчатися на широкому спектрі варіацій, що сприяє його узагальненості та покращує надійність при застосуванні у реальних системах.

Підключення бібліотек реалізується так:

```
import os
import cv2
```

Для завантаження зразкового відбитка пальця використовується рядок: sample = cv2.imread ("SOCOFing/150__M_Right_index_finger_Obl.BMP"). Цей файл вважається еталонним зразком для подальшого порівняння.

Ось перефразований варіант вашого тексту з збереженням обсягу та змісту.

Змінна best_score = 0 призначена для збереження найвищого значення відповідності, яке вдалося виявити під час процесу порівняння; вона ініціалізується нульовим значенням. Змінна filename = None служить для збереження назви файлу зображення, що забезпечує найкращий збіг, і на початку встановлюється як None. Аналогічно, змінна image = None використовується для зберігання самого зображення з найвищим рівнем відповідності, також ініціалізована як None. Змінні kp1, kp2 та mp, які на початку встановлюються в None, виконують роль контейнерів для відповідних даних: ключових точок на зразковому зображенні, ключових точок на зображенні–кандидаті, а також набору якісних відповідностей між ними. Ініціалізація цих змінних як None дозволяє запобігти виникненню помилок у випадку, якщо під час виконання не буде виявлено жодних релевантних збігів.

У циклі обробки кандидатських зображень використовується лічильник counter = 0, що веде підрахунок кількості оброблених зображень. Оператор for file in [file for file in os.listdir("SOCOFing/Real")][:5000] перебирає до 5000 файлів з каталогу "SOCOFing/Real". Для забезпечення зворотного зв’язку з користувачем щодо перебігу обробки, в кожній 10–й ітерації (if counter % 10 == 0) програма виводить поточне значення лічильника counter (тобто кількість уже опрацьованих зображень) і назву оброблюваного файлу. Рядок counter += 1 збільшує значення змінної counter на одиницю після кожного проходження циклу. Для зчитування чергового зображення кандидатського відбитка з відповідної директорії використовується функція imread з бібліотеки OpenCV, що реалізується через конструкцію fingerprint_image = cv2.imread("SOCOFing/Real/" + file).

Наступним етапом є виявлення та зіставлення характерних ознак на зображеннях. Для цього створюється об’єкт SIFT за допомогою команди sift = cv2.SIFT_create(). Далі, за допомогою методу sift.detectAndCompute, обчислюються ключові точки та дескриптори для еталонного зразка (keypoints_1, descriptors_1 = sift.detectAndCompute(sample, None)) і для зображення кандидатського відбитка пальця (keypoints_2, descriptors_2 = sift.detectAndCompute(fingerprint_image, None)). Отримані результати зберігаються відповідно у списках keypoints_1 (або keypoints_2) та descriptors_1 (або descriptors_2). Далі здійснюється пошук відповідностей між цими ключовими точками. Для цього використовується алгоритм k–ближчих сусідів (k–NN), який дозволяє знайти потенційні збіги між ознаками зображень. Метод knnMatch повертає список matches, у якому кожен елемент відповідає парі відповідних дескрипторів – одного з descriptors_1 і одного з descriptors_2. Значення параметра k=2 вказує на те, що для кожного дескриптора з першого набору шукають два найближчі сусіди з другого набору. Цикл пошуку наведено на рис. 3.6.

```
counter += 1
fingerprint_image = cv2.imread("SOCOFing/Real/" + file)
sift = cv2.SIFT_create()

keypoints_1, descriptors_1 = sift.detectAndCompute(sample, None)
keypoints_2, descriptors_2 = sift.detectAndCompute(fingerprint_image, None)

matches = cv2.FlannBasedMatcher({'algorithm': 1, 'trees': 10}, {}).knnMatch(descriptors_1, descriptors_2, k=2)

match_points = []
for p, q in matches:
    if p.distance < 0.1 * q.distance:
        match_points.append(p)
```

Рис. 3.6. Цикл пошуку

Для фільтрації знайдених відповідностей використовується цикл for p, q in matches, який перебирає всі пари, отримані на попередньому етапі. У цьому контексті p відповідає першому з двох найближчих дескрипторів (з descriptors_1), тоді як q – другому (з descriptors_2), що дозволяє порівняти їхню схожість та відсіяти менш надійні збіги.

Для виключення неточних або випадкових відповідностей використовується умовний блок if p.distance < 0.1 * q.distance. У цьому випадку виконується порівняння відстаней між ключовими точками: p.distance – це відстань до найближчої відповідності (перша відповідність), а q.distance – до другої найближчої. Якщо перша відстань значно менша (менше 10% другої), це вказує на те, що відповідність p є якісною та достовірною. У такому разі відповідність p вважається надійною та додається до списку match_points[] для подальшого аналізу.

Обчислюємо оцінку зіставлення (рис. 3.7).

```
keypoints = 0
if len(keypoints_1) < len(keypoints_2):
    keypoints = len(keypoints_1)
else:
    keypoints = len(keypoints_2)
if len(match_points) / keypoints * 100 > best_score:
    best_score = len(match_points) / keypoints * 100
    filename = file
    image = fingerprint_image
    kp1, kp2, mp = keypoints_1, keypoints_2, match_points
```

Рис. 3.7. Обчислення оцінки зіставлення

Змінна keypoints = 0 використовується для зберігання меншої кількості ключових точок між двома зображеннями. Якщо кількість ключових точок в еталонному зображенні (len(keypoints_1)) менша, ніж у кандидатському (len(keypoints_2)), змінній keypoints присвоюється значення len(keypoints_1). В іншому випадку вона отримує значення len(keypoints_2). Такий підхід дозволяє уникнути потенційного ділення на нуль під час подальших обчислень оцінки відповідності.

У рядку best_score = len(match_points) / keypoints * 100 обчислюється поточна оцінка зіставлення у відсотках. Якщо вона перевищує значення, яке зберігається у змінній best_score (тобто є найкращою на поточний момент), тоді:

змінна best_score оновлюється на нове, краще значення;

filename отримує ім’я поточного файлу зображення кандидатського відбитка;

image оновлюється відповідним зображенням;

kp1, kp2 та mp оновлюються відповідно до ключових точок і знайдених відповідностей.

Таким чином, ці змінні зберігають інформацію про найкраще зіставлення лише тоді, коли поточний результат перевищує попередній. На завершення виконується візуалізація знайденого найкращого результату.

Рядок print("BEST MATCH: " + filename) виводить на екран назву файлу зображення кандидатського відбитка пальця, яке показало найвищу схожість з еталонним. А print("SCORE: " + str(best_score)) демонструє відповідну оцінку зіставлення у відсотках.

Далі, за допомогою result = cv2.drawMatches(sample, kp1, image, kp2, mp, None), виконується візуалізація знайдених відповідностей між ключовими точками двох зображень – еталонного та кандидатського. Ця функція OpenCV з’єднує відповідні точки лініями на об'єднаному зображенні.

Завершальний рядок result = cv2.resize(result, None, fx=4, fy=4) масштабовує отриману візуалізацію, збільшуючи її в чотири рази по обох осях, щоб покращити наочність зіставлення.

Повний код реалізації подано на рис. 3.8.

Розглянемо безпосередній результат виконання програми. На рис. 3.9 зображено процес пошуку найбільш схожого відбитка пальця. Перше зображення ілюструє початок обробки, а друге демонструє, що вже перевірено понад 3000 зразків із колекції.

Після завершення пошуку програма автоматично виводить назву файлу з папки "SOCOFing/Real", у якому виявлено відбиток пальця з найвищим ступенем схожості із заданим зразком. Крім цього, виводиться кількість знайдених відповідностей між ключовими точками та відображається графічне представлення цих відповідностей – об'єднане зображення, на

якому еталонний відбиток і знайдений кандидат розташовані поруч, а відповідні ключові точки поєднані лініями.

```
import os
import cv2
sample = cv2.imread("SOCOFing/150__M_Right_index_finger_Obl.BMP")
best_score = 0
filename = None
image = None
kp1, kp2, mp = None, None, None
counter = 0
for file in [file for file in os.listdir("SOCOFing/Real")][:5000]:
    if counter % 10 == 0:
        print(counter)
        print(file)
    counter += 1
    fingerprint_image = cv2.imread("SOCOFing/Real/" + file)
    sift = cv2.SIFT_create()
    keypoints_1, descriptors_1 = sift.detectAndCompute(sample, None)
    keypoints_2, descriptors_2 = sift.detectAndCompute(fingerprint_image, None)
    matches = cv2.FlannBasedMatcher({'algorithm': 1, 'trees': 10}, {}).knnMatch(descriptors_1, descriptors_2, k=2)
    match_points = []
    for p, q in matches:
        if p.distance < 0.1 * q.distance:
            match_points.append(p)
    keypoints = 0
    if len(keypoints_1) < len(keypoints_2):
        keypoints = len(keypoints_1)
    else:
        keypoints = len(keypoints_2)
    if len(match_points) / keypoints * 100 > best_score:
        best_score = len(match_points) / keypoints * 100
        filename = file
        image = fingerprint_image
        kp1, kp2, mp = keypoints_1, keypoints_2, match_points
print("BEST MATCH: " + filename)
print("SCORE: " + str(best_score))
result = cv2.drawMatches(sample, kp1, image, kp2, mp, None)
result = cv2.resize(result, None, fx=4, fy=4)
cv2.imshow("Result", result)
cv2.waitKey(0)
cv2.destroyAllWindows()
```

Рис. 3.8. Лістинг коду додатку

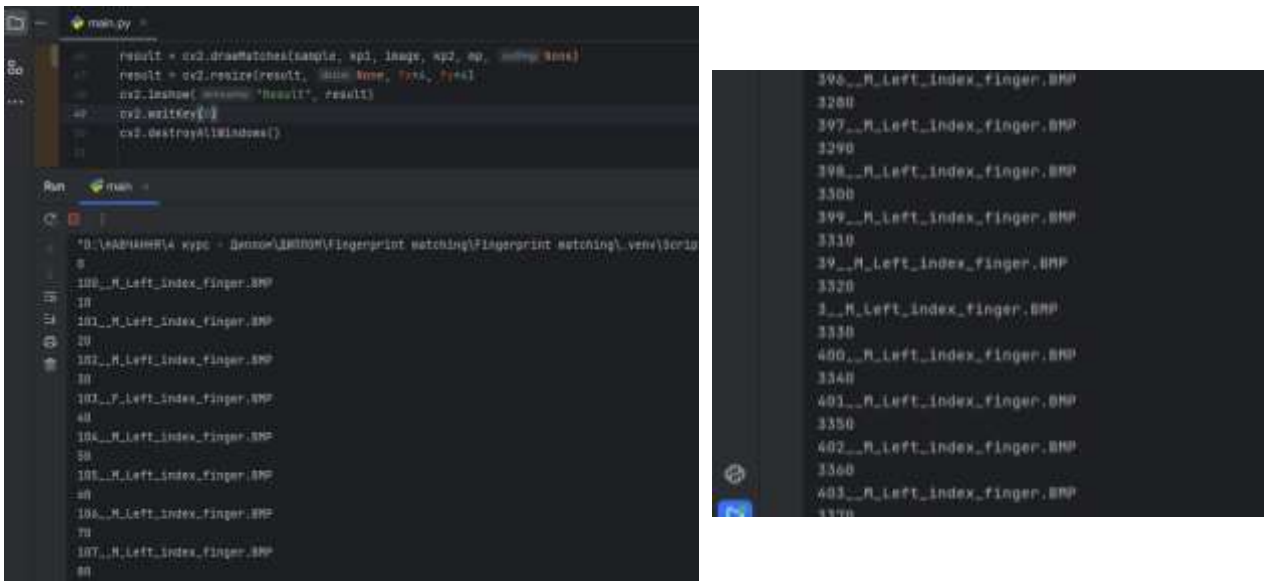

Рис. 3.9. Процес виконання коду для порівняння відбитків пальців

У проаналізованому прикладі найкращим збігом виявився файл 150__M_Right_index_finger.BMP, із результатом:

BEST MATCH: 150__M_Right_index_finger.BMP

SCORE: 57.14285714285714

Це свідчить про те, що в каталозі "SOCOFing/Real" було знайдено файл «150__M_Right_index_finger.BMP», відбиток пальця в якому збігається із зразком на 57,14%, що показано на рис. 3.10.

Рис. 3.10. Результат виконання алгоритму пошуку зображення відбитка пальця, що найбільше відповідає зразку

Зліва представлено зображення зразка відбитка пальця, з якого розпочинався пошук. Праворуч знаходиться зображення відбитка з каталогу "SOCOFing/Real", який алгоритм визначив як найбільш схожий на зразок. Кількість з'єднувальних ліній демонструє, скільки ключових точок із зразка було знайдено на відповідному відбитку. Товщина цих ліній може відрізнятися: товстіші лінії відображають більш надійні зіставлення, тоді як тонші – менш впевнені. Області без ліній можуть свідчити про відсутність відповідностей у цих частинах зображень. Візуальне представлення зіставлення ключових точок наведено на рис. 3.11.

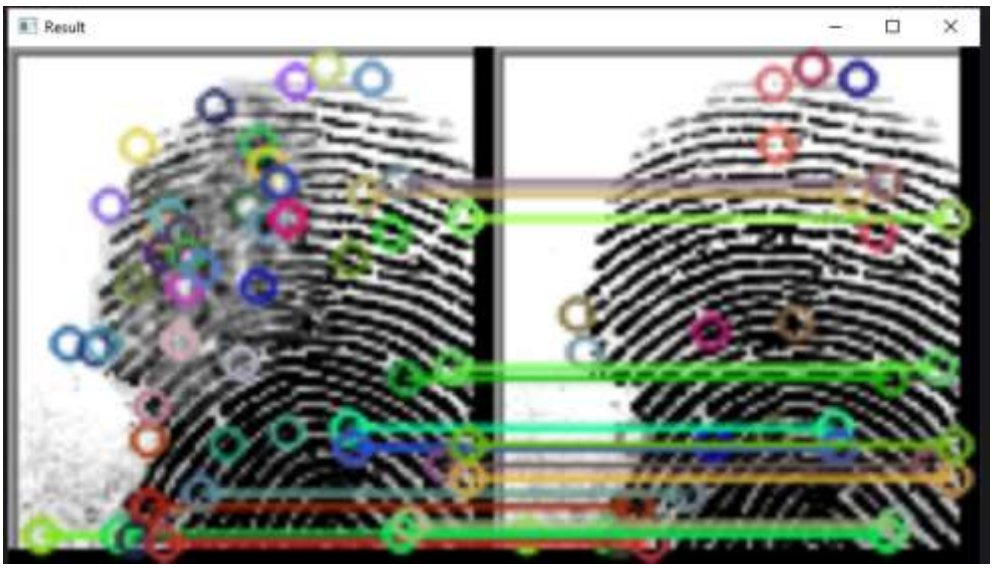

Рис. 3.11. Графічне відображення відповідностей ключових точок між двома зображеннями відбитків пальців

Тепер розглянемо випадок, коли зображення зразка відбитка пальця було повернуто. Результати наведено на рис. 3.12.

Після обробки програма видала такий результат:

BEST MATCH: 150__M_Right_index_finger.BMP

SCORE: 22.86

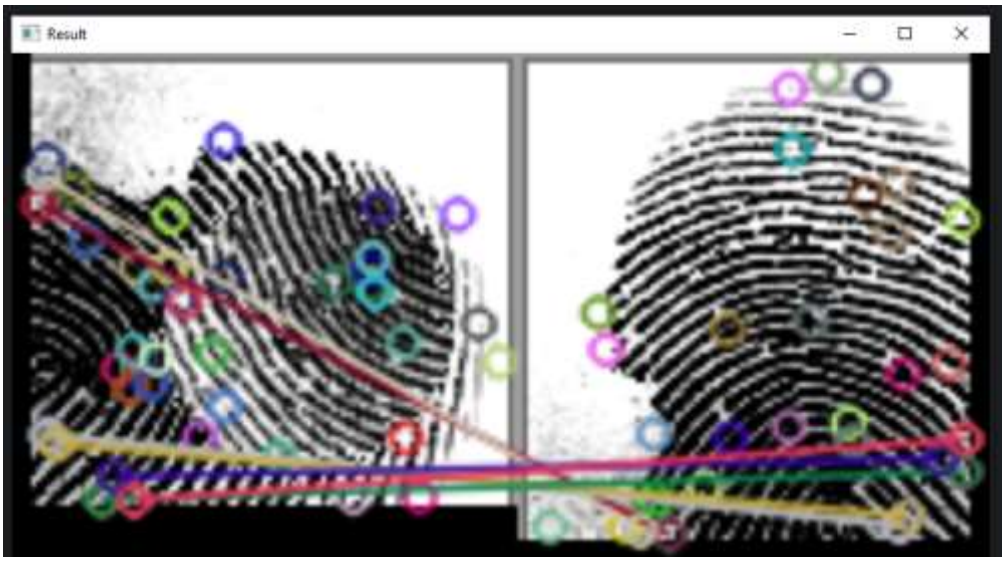

Рис. 3.12. Результат зіставлення після повороту зразка відбитка пальця на 90 градусів

Цей результат демонструє нижчий рівень схожості порівняно з попереднім випадком. Причина полягає в тому, що алгоритм SIFT не враховує орієнтацію ключових точок, тобто не розпізнає, чи розташована точка вгору, вниз або під іншим кутом. Після повороту зображення на 90 градусів частина ключових точок усе ще нагадує точки зі зразка, проте багато з них більше не збігаються. Як наслідок – менша кількість відповідностей і, відповідно, нижчий відсоток зіставлення.

На основі представленого зображення можна зробити кілька спостережень:

– кількість ліній, що з’єднують відповідні ключові точки, є значною. Це свідчить про наявність численних подібностей між зразком та знайденим відбитком пальця;

– лінії відповідностей переважно зосереджені в певних ділянках зображення, що може вказувати на наявність локалізованих характерних ознак, які сприяють схожості. Наприклад, видно, що багато ліній зосереджені на краях пальця;

– відсутність ліній у деяких регіонах може свідчити про відмінності у відповідних зонах двох відбитків. Зокрема, в центральній частині зображення долоні таких відповідностей майже не спостерігається.

Далі розглянемо випадок, коли зразок відбитка пальця повністю замінено іншим. Результат автоматичного зіставлення показує:

BEST MATCH: 1__M_Left_index_finger.BMP

SCORE: 18.75

Як видно на рисунку 3.13, ці два відбитки виявляють певний рівень подібності, однак не є ідентичними. Оцінка 18,75 означає, що лише 18,75% ключових точок збігаються. Виходячи з цього результату, можна впевнено стверджувати, що зображені відбитки пальців належать різним особам.

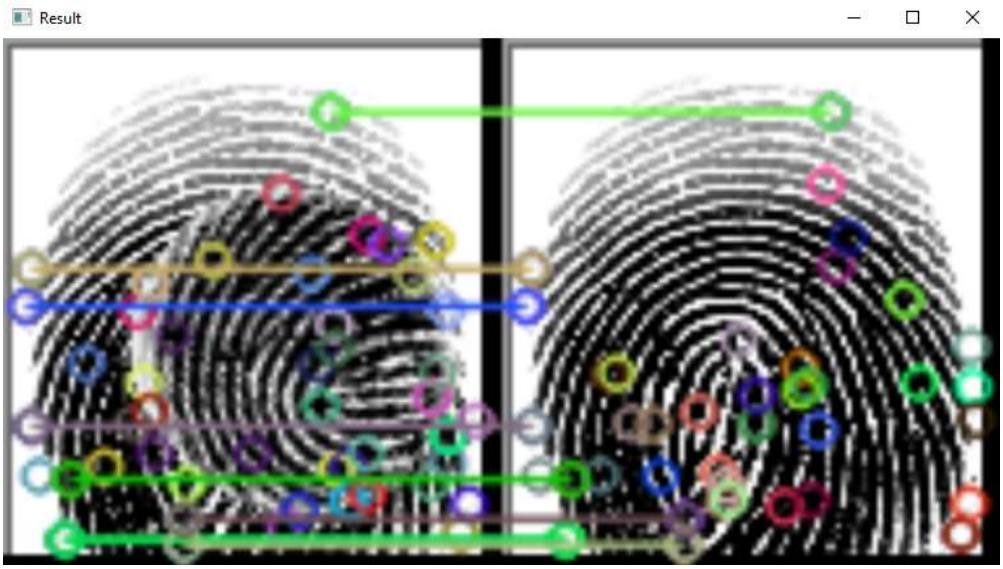

Рис. 3.13. Візуалізація порівняння ключових точок двох відбитків пальців, що належать різним людям

Наведена вище програмна реалізація алгоритму порівняння відбитків пальців представляє цікавий підхід до аутентифікації за відбитками пальців, використовуючи алгоритм SIFT. Хоча він може бути недостатньо надійним для високозахищених систем, він демонструє кілька ключових переваг, корисних для певних застосувань:

– повністю реалізований на програмному рівні за допомогою бібліотеки OpenCV, що робить його більш доступним та масштабованим у порівнянні з апаратними рішеннями для аутентифікації відбитків пальців;

– алгоритм SIFT орієнтований на виявлення та порівняння ключових точок відбитків пальців, а не на загальне зображення, що робить його стійким до незначних варіацій, таких як обертання пальця чи зміна тиску під час сканування;

– параметри SIFT, як–от кількість витягнутих точок або порогові значення для зіставлення, можна налаштувати для оптимізації роботи програми під конкретні потреби.

Однак, важливо зазначити обмеження цього підходу:

– запропонована програма, ймовірно, не досягне такої ж точності, як спеціалізовані апаратні сканери відбитків пальців, які використовують

складніші алгоритми та датчики високої роздільної здатності;

– для критичних систем безпеки може знадобитися додаткова перевірка або багатофакторна аутентифікація, оскільки оцінка зіставлення може бути недостатньою для точного ідентифікування.

ВИСНОВКИ

У межах кваліфікаційної бакалаврської роботи було здійснено комплексне дослідження теоретичних, методичних та прикладних аспектів біометричної ідентифікації та автентифікації у контексті їх використання в автоматизованих системах контролю доступу. Основні результати роботи можна узагальнити наступним чином:

1. У першому розділі розглянуто теоретичні основи біометрії. Надано визначення біометричних технологій, описано види біометричних ознак, серед яких виділено фізіологічні (відбитки пальців, геометрія обличчя, райдужна оболонка ока) та поведінкові (голос, підпис, динаміка натискань клавіш). Окрему увагу приділено принципам функціонування систем біометричної ідентифікації та автентифікації, а також порівняльному аналізу їх переваг та недоліків у контексті практичного застосування.

2. У другому розділі здійснено аналіз існуючих систем біометричної ідентифікації та автентифікації, що застосовуються в системах контролю доступу. Визначено основні вимоги до таких систем: точність, швидкість, безпека, зручність використання, стійкість до зовнішніх умов, сумісність та захист персональних даних. Розглянуто сучасні рішення на ринку, їх технічні характеристики та сфери застосування. Встановлено, що найбільш поширеними біометричними технологіями є розпізнавання відбитків пальців, обличчя та сканування райдужної оболонки.

3. У третьому розділі було спроєктовано та реалізовано систему біометричної ідентифікації та аутентифікації на основі відбитків пальців. Обґрунтовано вибір біометричної ознаки, здійснено вибір інструментальних засобів розробки, створено архітектуру програмного забезпечення та розроблено функціональну реалізацію. Особливу увагу приділено алгоритмам обробки та зіставлення відбитків (зокрема використанню методу SIFT), а також візуалізації результатів ідентифікації. Продемонстровано

ефективність системи в умовах тестового середовища, зокрема її здатність виявляти найбільш схожі відбитки з бази зображень.

Таким чином, у результаті виконаної кваліфікаційної роботи було досягнуто поставленої мети – розроблено програмну реалізацію системи біометричної ідентифікації та аутентифікації користувачів, що відповідає сучасним вимогам до засобів контролю доступу. Запропоноване рішення може бути використано як основа для побудови безпечних інформаційних систем у різних сферах – від офісних будівель до об’єктів критичної інфраструктури.

Практична новизна роботи полягає у створенні прототипу автоматизованої системи контролю доступу з біометричною автентифікацією, яка демонструє можливість інтеграції сучасних технологій обробки зображень для розпізнавання відбитків пальців у прикладних задачах безпеки.

Одержані результати можуть бути використані у навчальному процесі для підготовки фахівців із кібербезпеки, інформаційних технологій, а також у прикладних проєктах з розробки систем доступу до захищених об'єктів і приміщень.

Перспективи подальшого розвитку дослідження пов’язані з удосконаленням алгоритмів ідентифікації, впровадженням багатофакторної автентифікації, розширенням використання інших біометричних модальностей (наприклад, розпізнавання обличчя чи райдужки ока), а також із дослідженням можливостей адаптації систем до змін умов навколишнього середовища та мобільних платформ.

ПЕРЕЛІК ПОСИЛАНЬ

1. Євсеєв С. П., Шматко О. В., Ахієзер О. Б., Горбач Т. В. Основи кібербезпеки: навчально-практичний посібник. – Харків: НТУ «ХПІ»; Львів: Новий Світ-2000, 2025. – 95 с.

2. Богуш В. М., Богуш В. В., Бровко В. Д., Настрадін В. П. Основи кіберпростору, кібербезпеки та кіберзахисту. – К.: Ліра-К, 2020. – 554 с.

3. Кулініч, О.В. Біометрична ідентифікація та автентифікація особи за геометрією обличчя / О.В. Кулініч, О.О. Лисенко // Вісник Національного технічного університету України "Київський політехнічний інститут". Серія: Радіотехніка. Радіоапаратобудування. - 2017. - № 71. - С. 68-75.

4. Бурячок В. Л., Киричок Р. В., Складанний П. М. Основи інформаційної та кібернетичної безпеки. – К.: 2018. – 320 с.

5. Полшакова О., Мальченко Ю. Представлення системи біометричного контролю доступу до «розумного» авто методом сканування відбитків пальців // Адаптивні системи автоматичного управління. – 2019. – № 35. – С. 123–130. – DOI: 10.20535/1560-8956.35.2019.197426.

6. Кубик В. О. Мультимодальна біометрична автентифікація користувачів в системах контролю доступу підприємства : пояснюв. записка диплом. роботи магістра / В. О. Кубик. – Київ : КНУ, 2022. – 63 с. – URL: https://ir.library.knu.ua/handle/123456789/1513.

7. Левченко А. В. Система контролю доступу та ідентифікації осіб на режимних об’єктах : магістерська дис. / А. В. Левченко. – Київ : КПІ ім. Ігоря Сікорського, 2024. – 112 с. – URL: https://ela.kpi.ua/handle/123456789/63978.

8. Маланчук А. О. Система керування доступом на основі технології SSO, з використанням біометричної автентифікації : дипломна робота / А. О. Маланчук. – Київ : НАУ, 2021. – 75 с. – URL: https://er.nau.edu.ua/handle/NAU/55924.

9. Іллюшко Б. О., Дьогтяр Р. С. Кібербезпекові аспекти побудови

системи контролю доступу за допомогою сканування відбитків пальців // Новітні технології у науковій діяльності і навчальному процесі : тези доп. Всеукр. наук.-практ. конф. – Чернігів : НУ «Чернігівська політехніка», 2020. – С. 173–175. – URL: http://ir.stu.cn.ua/123456789/22542.

10. Rane S., Wang Y., Draper S. C., Ishwar P. Secure Biometrics: Concepts, Authentication Architectures and Challenges // arXiv preprint arXiv:1305.4832. – 2013. – 15 с. – URL: https://arxiv.org/abs/1305.4832.

11. Karimian N., Guo Z., Tehranipoor F., Woodard D., Tehranipoor M., Forte D. Secure and Reliable Biometric Access Control for Resource-Constrained Systems and IoT // arXiv preprint arXiv:1803.09710. – 2018. – 12 с. – URL: https://arxiv.org/abs/1803.09710.

12. Joshi M., Mazumdar B., Dey S. Security Vulnerabilities Against Fingerprint Biometric System // arXiv preprint arXiv:1805.07116. – 2018. – 9 с. – URL: https://arxiv.org/abs/1805.07116.

13. Serratosa F. Security in Biometric Systems // arXiv preprint arXiv:2011.05679. – 2020. – 18 с. – URL: https://arxiv.org/abs/2011.05679.

14. Н. В. Сачанюк-Кавецька і І. О. Бондаренко, «Ідентифікація суб’єктів в системах контролю доступу за допомогою ідентифікаційної логіко-часової функції, як ефективний метод комплексного захисту інформації», Опт-ел. інф-енерг. техн., вип. 35, вип. 1, с. 14–23, Чер 2019.