Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіті другий (магістерський)

Дослідження методів біометричної аутентифікації
(тема)

Виконав:
студент 2 курсу, групи ІМІм-22-2
Копиця А.А.
(прізвище, ініціали)

Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник: доц. Скорик Ю.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Безрук В.М.
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ / А.А. Копиця /
(підпис) (прізвище та ініціали)

Керівник _____ / Ю.В. Скорик /
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Телекомунікації та радіотехніка

(код і повна назва)

Тип програми освітньо-наукова

Освітня програма Інформаційно-мережна інженерія

(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«18» березня 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Копиці Аллі Анатоліївні
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів біометричної аутентифікації

затверджена наказом по університету «18» березня 2024 р. № 232 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 26 червня 2024 р.

3. Вхідні дані до роботи *Методи біометричної автентифікації; характеристики показників якості методів біометричної автентифікації; види пристроїв біометричної автентифікації; метод аналізу ієрархії*

4. Перелік питань, що потрібно опрацювати у *Вступ*
1 Біометрична автентифікація
2 Типи біометричних пристроїв та їх аналіз
3 Порівняння методів біометричної автентифікації
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Слайди у форматі Power Point (назва та мета роботи, біометрична автентифікація, методи біометричної автентифікації, біометричні пристрої та їх типи, контактні біометричні пристрої, безконтактні біометричні пристрої, гібридні або біометричні пристрої, аналіз типів біометричних пристроїв, середні значення показників FAR та FRR для різних біометричних систем контролю та управління доступом, порівняння біометричної аутентифікації, метод аналізу ієрархій, Результати вибору переважного методу біометричної аутентифікації, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	18.03. – 25.03.2024	вик.
2	Підбір літератури за темою роботи	26.03. – 15.04.2024	вик.
3	Біометрична автентифікація	16.04. – 30.04.2024	вик.
4	Типи біометричних пристроїв та їх аналіз	01.05. – 24.05.2024	вик.
5	Порівняння методів біометричної	25.05. – 14.06.2024	вик.
	автентифікації		
7	Оформлення презентаційного матеріалу,	15.06. – 20.06.2024	вик.
	підготовка до захисту у ЕК		

Дата видачі завдання 18 березня 2024 р.

Студент _____ Копиця А.А.
(підпис)

Керівник роботи _____ доц. Скорик Ю.В.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 63 с., 15 рис., 26 джерел, 2 додатка.

Об’єкт роботи – методи та пристрої біометричної автентифікації.

Мета роботи – дослідження та вибір переважного методу біометричної автентифікації.

Проведено огляд методів біометричної автентифікації, виявлено переваги та недоліки. Зроблено огляд та аналіз типів біометричних пристроїв. Із застосуванням методу аналізу ієрархій обрано переважний метод біометричної автентифікації.

БІОМЕТРІЯ, РАЙДУЖНА ОБОЛОНКА ОКА, АУТЕНТИФІКАЦІЯ, ВЕРИФІКАЦІЯ, АВТОРИЗАЦІЯ, СИСТЕМА, БЕЗПЕКА, НАДІЙНІСТЬ, БІОМЕТРИЧНИЙ ПРИСТРІЙ, СКАНЕР

THE ABSTRACT

Explanatory note: 63 p., 15 figures, 26 sources, 2 appendices.

Object of work – methods and devices of biometric authentication.

Purpose – to study and select the preferred method of biometric authentication.

A review of biometric authentication methods is conducted, advantages and disadvantages are identified. The types of biometric devices are reviewed and analyzed. Using the method of hierarchy analysis, the preferred method of biometric authentication is selected.

BIOMETRICS, IRIS, AUTHENTICATION, VERIFICATION, AUTHORIZATION, SYSTEM, SECURITY, RELIABILITY, BIOMETRIC DEVICE, SCANNER

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AePS – Aadhaar-Enabled Payment System – Платіжна система з підтримкою Aadhaar;

AFIS – Integrated Automated Fingerprint Identification System – Автоматизована система ідентифікації за відбитками пальців;

BAT – Biometric Automated Toolset – автоматизований набір біометричних інструментів;

CAGR – compound annual growth rate – сукупний середньорічний темп зростання;

FAR – False Acceptance Rate – ймовірність помилкового допуску;

FRR – False Rejection Rate – ймовірність помилкового затримання;

HDR – High Dynamic Range Imaging – загальна назва технологій роботи із зображеннями і відео;

HIIDE – Handheld Interagency Identity Detection Equipment – портативне міжвідомче обладнання для розпізнавання осіб;

ISO – International Organization for Standardization – Міжнародна організація зі стандартизації;

RFID – Radio Frequency IDentification – радіочастотна ідентифікація;

СКУД – системи контролю та управління доступом.

ВСТУП

В останні роки біометрія привертає увагу як одна з інформаційних технологій, що почала стрімко розвиватися в 21 столітті, визначаючи розвиток систем персональної ідентифікації та співставлення, дозволяючи використовувати результати біометричної науки в різноманітних сучасних системах контролю доступу та безпеки з надзвичайно високою надійністю.

Основна перевага біометричних технологій (біометрії) полягає в тому, що вони дозволяють швидко і легко ідентифікувати або верифікувати особу, в більшості випадків без незручностей для неї [1].

За останнє десятиліття біометричні технології зробили великий крок вперед у своєму розвитку, ставши, по суті, самостійною галуззю з перспективами зростання. На початку 21 століття практичне застосування методів біометричної ідентифікації та верифікації є досить важливою складовою інформаційних технологій, якщо не одним з найважливіших шляхів їх розвитку.

Сьогодні біометричні системи вважаються другим поколінням систем безпеки, а біометрія – це наука про використання специфічних для людини параметрів вимірювання для ідентифікації та верифікації людини.

Заходи з ідентифікації та верифікації необхідні для вирішення проблем, таких як [1]:

– злочинність та тероризм;

– нелегальна імміграція;

– шахрайство у сфері електронної та мобільної комерції.

Законослухняні громадяни також гостро потребують ефективних і надійних засобів і систем масової ідентифікації.

Громадяни потребують зручних, надійних, швидко зчитуваних та захищених від підробок документів у таких ситуаціях [1]:

– паспорти та проходження прикордонного контролю;

– підтвердження спеціального статусу та/або повноважень на здійснення спеціальної діяльності;

– доступ до систем медичного та соціального забезпечення, страхування, бібліотек, музеїв та інших культурних і наукових установ тощо;

– взаємодія з органами державної влади;

– використання фінансових систем, програм лояльності та додаткових транспортних послуг [1].

Важливість біометричних технологій у забезпеченні комплексної безпеки постійно зростає, про що свідчить неухильне збільшення використання технології в аеропортах та інших об'єктах критичної інфраструктури.

Одним з найбільш перспективних напрямків є розробка і виробництво різних біометричних інтелектуальних систем безпеки.

До систем біометричної ідентифікації відносяться системи доступу на основі відбитків пальців, долонь, райдужної оболонки ока, геометрії обличчя, малюнка вен на руках і пальцях, ДНК, форми вух, температури шкіри, підпису і голосу. І це не вичерпний список, який постійно розширюється [1].

Розширення сфери застосування біометрії зумовлене, головним чином, зростаючою потребою державних установ та бізнесу в безпеці, вразливістю персональних комп'ютерів та існуючих інформаційних мереж, а також постійним зростанням комп'ютерних злочинів.

Сучасна біометрія ще не розкрила всіх своїх можливостей, і в майбутньому будуть запропоновані нові апаратні та програмні рішення, засновані на останніх досягненнях біометричних технологій.

1 БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ

Біометрична автентифікація, рішення для цифрової ідентифікації, яке використовує унікальні фізіологічні та поведінкові біометричні характеристики людини, переосмислює способи автентифікації в Інтернеті, забезпечуючи безпечний і безперешкодний доступ до конфіденційної інформації, пристроїв і послуг [2].

У цьому розділі буде розглянуто основні принципи біометричної автентифікації та її реальні приклади, пропонуючи всебічний погляд на технологію, яка безперешкодно інтегрується в повсякденне життя.

1.1 Що таке біометрична автентифікація

Біометрична автентифікація – це форма перевірки особи та процесу безпеки, яка використовує унікальні фізіологічні та поведінкові особливості особи – такі як відбитки пальців, зображення обличчя, голосові патерни або навіть ритм друку – для підтвердження особи при доступі до цифрових сервісів або пристроїв. На відміну від традиційних методів автентифікації, які покладаються на те, що людина знає (наприклад, пароль), або на те, що вона має (наприклад, токен чи картку), біометричні методи автентифікації ґрунтуються на людині та її індивідуальних особливостях [3].

Механізм біометричної автентифікації має дві складові: біометричну реєстрацію та біометричну автентифікацію.

На етапі реєстрації біометрична система безпеки збирає і надійно зберігає дані, отримані на основі унікальної характеристики користувача, наприклад, сканування відбитків пальців. Ці зібрані біометричні дані слугують точкою відліку для всіх майбутніх порівнянь [3].

На етапі автентифікації, коли особа шукає доступ до пристрою або послуги, система порівнює збережені дані з новопридбаною біометричною характеристикою, наприклад, порівнюючи щойно отримані скани відбитків пальців. Якщо виявлено збіг, користувач проходить автентифікацію, після чого йому надається доступ.

Системи біометричної автентифікації пропонують бездоганне поєднання безпеки та зручності для користувачів у доступі до фізичних і цифрових

ресурсів, гарантуючи, що особа, яка бажає отримати доступ, дійсно є тією, за кого себе видає.

Незалежно від того, чи надається доступ до захищених фізичних об'єктів, таких як корпоративні офіси, серверні кімнати IT або зони безпеки в аеропортах, чи до цифрових активів, таких як бази даних, портали державних послуг або персональні пристрої, біометрична автентифікація виступає в ролі воротаря, гарантуючи, що доступ отримають лише авторизовані особи [3].

1.2 Поширені види біометричної автентифікації

Системи біометричної автентифікації не є універсальними – кожна система пристосована до конкретних потреб та середовища. Для цього сучасні рішення біометричної автентифікації бувають різних типів, залежно від типу біометричних ознак, що використовуються для автентифікації особи.

Найпоширеніші типи методів біометричної автентифікації включають фізіологічну, поведінкову та мультимодальну біометричну автентифікацію.

Фізіологічна біометрія зосереджується на вроджених фізичних характеристиках людини. Вона включає в себе розпізнавання відбитків пальців, обличчя, райдужної оболонки ока [3].

Розпізнавання відбитків пальців є однією з найпопулярніших і усталених форм біометрії, яка покладається на унікальні патерни, знайдені у відбитках пальців, для підтвердження особи користувача. Відбитки пальців збираються за допомогою сканерів відбитків пальців, які фіксують відскановані зображення пальців, які потім конвертуються в цифрові формати.

Системи розпізнавання облич використовують камери і передові алгоритми для точної ідентифікації людей на основі їхніх рис обличчя. Ці системи можуть працювати як в пасивному, так і в активному режимах, причому пасивний режим фіксує зображення обличчя на відстані, а активний режим вимагає, щоб люди дивилися безпосередньо в камеру з метою автентифікації.

Системи розпізнавання райдужної оболонки покладаються на унікальні візерунки райдужної оболонки очей людини для підтвердження її особи. На відміну від розпізнавання обличчя, ці системи вимагають доступу з близької відстані і використовують найсучаснішу технологію інфрачервоної візуалізації для ідентифікації користувачів з неперевершеною точністю.

Поведінкова біометрія використовує унікальні поведінкові риси людини, такі як голос або манера друку, для підтвердження особи. Вона включає в себе розпізнавання голосу та підпису, динаміку натискання клавіш [3].

Біометричні системи розпізнавання голосу підходять як для фізичного, так і для онлайн-середовища, використовуючи шаблони унікального голосу людини для автентифікації її особи. Біометрія з розпізнаванням голосу особливо популярна в колл-центрах, де її можна використовувати як для перевірки особи клієнта, так і для підтвердження автентичності фінансових транзакцій.

Системи розпізнавання підписів здатні ідентифікувати унікальний стиль письма людини, забезпечуючи безпечну автентифікацію та доступ до фізичних і цифрових ресурсів.

Динаміка натискання клавіш – це дослідження того, як люди друкують, покладаючись на ритми і шаблони набору тексту для підтвердження особи користувача. Ця форма біометричної автентифікації особливо корисна в цифровому середовищі, забезпечуючи безпечну і зручну систему автентифікації для онлайн-сервісів.

Мультимодальна біометрія – це форма багатофакторної автентифікації, яка поєднує кілька типів біометричних ознак для більш надійної автентифікації користувача [3]. Поєднуючи різні фізіологічні та поведінкові форми, ідентичність особи можна перевірити з більшою точністю та безпекою.

Наприклад, мультимодальна біометрія може поєднувати розпізнавання обличчя з розпізнаванням голосу або відбитків пальців для автентифікації особи для доступу до фізичних або цифрових активів.

Розуміння різноманітних типів методів біометричної автентифікації має вирішальне значення, оскільки дозволяє організаціям і приватним особам вибрати найбільш підходящий і безпечний метод, виходячи з їхніх конкретних потреб. Незалежно від того, чи це додатки з високим рівнем безпеки, чи повсякденні споживчі пристрої, існує біометричне рішення, пристосоване для кожного сценарію [3].

1.3 Зростання біометричної автентифікації

Розвиток технологій призвів до зміни парадигми в тому, як люди сприймають безпеку. Традиційні методи, такі як паролі та PIN-коди, які колись

вважалися золотим стандартом, зараз відходять на другий план завдяки більш досконалим і безпечним системам біометричної автентифікації [3].

В останні роки біометрична автентифікація стала свідком стрімкого зростання впровадження в різних секторах, що зумовлено зростаючою потребою в посиленні безпеки та швидким розвитком біометричних технологій. Поширення біометричної автентифікації – це не просто тренд, а свідчення зростаючої уваги до безпеки, зручності та персоналізації у всьому світі.

Згідно з останніми маркетинговими дослідженнями, світовий ринок біометричної автентифікації та ідентифікації у 2021 році оцінювався в 4 135 мільйонів доларів США [4]. Але це лише початок. Прогнози свідчать, що до 2030 року ця цифра злетить до вражаючих 14 225 мільйонів доларів США. Таке вражаюче зростання, позначене середньорічним темпом приросту (CAGR) на рівні 16,7%, підкреслює зростаючу довіру до рішень біометричної автентифікації як з боку бізнесу, так і з боку споживачів.

Існує кілька факторів, які сприяють бурхливому розвитку ринку біометричної автентифікації, на які треба звернути увагу [3].

Інтеграція в побутову електроніку. Інтеграція біометричних функцій в побутову електроніку, особливо в смартфони і ноутбуки, відіграє ключову роль. Оскільки користувачі вимагають швидшого та безпечнішого доступу до своїх пристроїв, виробники вбудовують у свої продукти сканери відбитків пальців, системи розпізнавання обличчя та інші біометричні функції.

Революція банківських та фінансових послуг. Фінансовий сектор переживає трансформацію. З розвитком онлайн-банкінгу та цифрових транзакцій виникла нагальна потреба в надійних заходах безпеки. Біометрична автентифікація пропонує рішення, яке гарантує, що лише власник рахунку може отримати доступ до транзакцій та авторизувати їх.

Урядові ініціативи. Від електронних паспортів до національних програм ідентифікації особи, уряди в усьому світі інтегрують біометрію, стимулюючи ринок і підкреслюючи важливість цієї технології.

Занепокоєння з приводу безпеки. В епоху, коли витоки даних і кібератаки набувають загрозливих масштабів, біометрична автентифікація пропонує більш безпечну альтернативу традиційним методам, зменшуючи ризик несанкціонованого доступу.

Технологічний прогрес. Постійні дослідження і розробки в галузі біометрії призвели до створення більш точних, ефективних і доступних систем, що ще більше стимулює їх впровадження.

Поєднання біометричних даних з системами безпеки пропонує більш безпечний, зручний та ефективний метод перевірки особи та автентифікації [3]. Незалежно від того, чи це розблокування смартфона за допомогою зчитувача відбитків пальців, чи доступ до об'єкту з високим рівнем безпеки за допомогою технології розпізнавання обличчя, біометрична автентифікація змінює спосіб, у який людина взаємодіє зі світом. В міру того, як людина рухається вперед, залежність від біометричної автентифікації тільки зростатиме. Йдеться вже не лише про безпеку, а й про створення безперебійного, персоналізованого користувацького досвіду. І як свідчить ринкова статистика, біометрична автентифікація вже на шляху до того, щоб стати нормою, а не винятком.

1.4 Біометрична автентифікація в дії

Біометрична автентифікація вийшла за рамки простого заходу безпеки. Її застосування охоплює різні сектори, революціонізуючи те, як людина взаємодіє, здійснює транзакції і навіть живе. В цьому підрозділі буде розглянуто, як біометрична автентифікація змінює індустрію та повсякденне життя [2].

Біометрична автентифікація у фінансах та банківській справі [3]. Банківський сектор завжди був в авангарді впровадження передових заходів безпеки. З біометричною автентифікацією минули ті часи, коли потрібно було запам'ятовувати складні паролі або носити з собою токени. Тепер простий відбиток пальця або сканування обличчя може надати доступ до банківського рахунку, роблячи транзакції більш безпечними та безпроблемними. Це не тільки підвищує безпеку, але й забезпечує безперебійний банківський досвід для клієнтів, знижуючи ризик шахрайства та крадіжки особистих даних.

Крім того, біометрична автентифікація революціонізує управління касовими операціями в банках. Вона дозволяє наглядачам швидко і безпечно санкціонувати транзакції, ініційовані касирами. Така інтеграція біометрії не лише посилює заходи безпеки, але й оптимізує операційні процеси, забезпечуючи більш плавний і надійний банківський досвід як для клієнтів, так і для персоналу.

Як приклад, можна представити – аутентифікацію за відбитками пальців в індонезійському банку [5]. Завдяки впровадженню сканера відбитків пальців A400 від Aratek, керівники можуть швидко та безпечно авторизувати транзакції, що значно підвищує безпеку та ефективність банківських операцій.

Біометрична автентифікація в освіті, як захист навчальних закладів [3]. Навчальні заклади використовують біометричну автентифікацію для підвищення безпеки студентів і персоналу. Від контролю доступу до управління відвідуванням, біометричні системи гарантують, що тільки авторизовані особи можуть увійти в певні зони і точно відстежувати відвідуваність, тим самим сприяючи безпечному навчальному середовищу.

Реальний приклад цього – розпізнавання облич для контролю доступу до школи в Китаї [6].

Свідченням ефективності біометричної автентифікації в навчальних закладах є Пекінська академія танцю. Академія успішно впровадила біометричну систему контролю доступу TruFace від Aratek, щоб обмежити доступ і забезпечити вхід на територію тільки авторизованим особам. Це впровадження значно підвищило загальний рівень безпеки закладу, захистивши як студентів, так і персонал.

Ще одне варте уваги впровадження в університеті l'ISSEG в Гвінеї, де мобільні біометричні рішення Aratek були використані для ефективного управління відвідуваністю [7]. Це значно зменшило розбіжності в записах відвідуваності та заощадило час для підвищення ефективності щоденних операцій.

Біометрична автентифікація в державних послугах для впорядкування доступу до них [3]. Уряди в усьому світі впроваджують біометричну автентифікацію для спрощення доступу до різних державних послуг. Це підвищує ефективність і безпеку надання послуг, гарантуючи громадянам безперешкодний доступ до пільг і послуг, на які вони мають право, тим самим зменшуючи кількість крадіжок особистих даних і шахрайських заяв.

Як реальний приклад впорядкування державних послуг – Індійська платіжна система з підтримкою Aadhaar (AePS) [8]. Помітне впровадження біометричної автентифікації в державних службах можна побачити в індійській платіжній системі Aadhaar-Enabled Payment System (AePS). За допомогою сканерів відбитків пальців Aratek, сертифікованих STQC, AePS забезпечує платформу для фінансових і нефінансових транзакцій через номер Aadhaar

особи. Ця система не тільки спрощує процес доступу до різних державних послуг, але й гарантує, що пільги надійно та ефективно надходять до тих, кому вони призначені.

Біометрична автентифікація в гуманітарній допомозі, як ефективний розподіл ресурсів [3]. У регіонах, що стикаються з гуманітарними кризами, біометрична автентифікація має вирішальне значення для управління розподілом допомоги. Точно ідентифікуючи людей, біометричні системи гарантують, що допомога потрапляє саме до тих людей, зменшуючи розбіжності та підвищуючи ефективність гуманітарних зусиль.

Реальний приклад в гуманітарній допомозі – це розпізнавання відбитків пальців для управління біженцями в Туреччині [9]. Впровадження біометричних технологій допомогло точно ідентифікувати і зареєструвати біженців, тим самим забезпечивши ефективний і безпечний розподіл гуманітарної допомоги серед тих, хто її потребує.

Біометрична автентифікація в телекомі, як захист даних користувачів та покращення клієнтського досвіду [3]. У телекомунікаційному секторі оператори інтегрують біометричні системи для автентифікації користувачів для таких послуг, як мобільний банкінг, цифрові платежі і навіть портали обслуговування клієнтів, забезпечуючи безпечний і персоналізований досвід. Крім того, з розвитком технології eSIM і переходом телекомунікаційних операторів на цифрові технології, біометрична автентифікація пропонує додатковий рівень безпеки під час процесу приєднання до мережі, забезпечуючи безперебійний і безпечний досвід для користувачів. Нарешті, телекомунікаційні оператори використовують біометричну автентифікацію для доступу співробітників до захищених об'єктів і систем, тим самим підвищуючи загальну безпеку в організації.

Біометрична автентифікація в подорожах та імміграції, як впорядкування прикордонного контролю [3]. Аеропорти та служби прикордонного контролю використовують біометричну автентифікацію для спрощення імміграційного процесу. Розпізнавання обличчя, відбитків пальців і райдужної оболонки ока використовуються для перевірки особи мандрівників, скорочуючи час очікування, покращуючи загальний досвід подорожей і підвищуючи безпеку на міжнародних кордонах.

Біометрична автентифікація в охороні здоров'я, як захист інформації про пацієнтів [3]. Сектор охорони здоров'я обробляє деякі з найбільш чутливих

даних. Біометрична автентифікація використовується для захисту інформації про пацієнтів і забезпечення доступу до медичних записів лише уповноваженому персоналу. Це не тільки захищає конфіденційність пацієнтів, але й підвищує ефективність надання медичних послуг, зменшуючи ризик помилок.

Біометрична автентифікація в побутовій електроніці, як персоналізація користувацького досвіду [3]. Інтеграція біометричних функцій у смартфони, ноутбуки та інші споживчі пристрої змінила досвід користувачів. Біометрична автентифікація пропонує користувачам швидкий і безпечний доступ до своїх пристроїв і мобільних додатків, додаючи персоналізованого дотику до взаємодії з технологіями.

Біометрична автентифікація в правоохоронних органах, як забезпечення санкціонованого доступу до конфіденційних даних [3]. У сфері правоохоронної діяльності біометрична автентифікація має першорядне значення для захисту доступу до конфіденційних і засекречених баз даних, таких як Автоматизована система ідентифікації за відбитками пальців (AFIS). Використовуючи біометричні методи, такі як розпізнавання відбитків пальців або обличчя, установи можуть гарантувати, що лише уповноважений персонал матиме доступ до важливих записів, даних розслідувань та іншої конфіденційної інформації. Цей суворий захід безпеки має важливе значення для збереження цілісності правоохоронних операцій і запобігання потенційному витоку даних.

Біометрична автентифікація в корпоративній безпеці, такі як доступ співробітників та захист даних [3]. У корпоративному світі біометрична автентифікація є наріжним каменем для забезпечення безпечного доступу співробітників до об'єктів, захисту конфіденційних корпоративних даних і точного управління часом і відвідуванням. Компанії розгортають біометричні системи, такі як сканери відбитків пальців і розпізнавання облич, для контролю доступу до офісних будівель, центрів обробки даних і зон з обмеженим доступом на робочому місці. Крім того, ці системи використовуються для моніторингу робочого часу співробітників, зменшення крадіжок робочого часу та забезпечення точної обробки заробітної плати. Таке багатогранне застосування біометричної автентифікації підвищує загальну операційну ефективність, безпеку та управління робочою силою в корпоративному середовищі.

Біометрична автентифікація проникає в тканину нашого суспільства, пропонуючи підвищену безпеку, зручність та ефективність у різних секторах. Реальне застосування біометричної автентифікації свідчить про її універсальність і трансформаційний вплив на майбутнє.

1.5 Переваги та недоліки використання біометричної автентифікації

Дедалі ширше впровадження біометричної автентифікації в різних галузях свідчить про її численні переваги. Розглянемо переваги, які роблять біометричну автентифікацію кращим вибором [3].

Підвищена безпека – біометричні дані є унікальними для кожної людини, що робить їх надзвичайно складними для підробки або маніпуляцій. Ця унікальність забезпечує вищий рівень безпеки порівняно з традиційними методами, такими як паролі або PIN-коди, які можуть бути легко скомпрометовані.

Зручність та ефективність – зручність і швидкість біометричних систем сприяють підвищенню задоволеності користувачів. Безперешкодний досвід використання біометрії для автентифікації призводить до позитивного залучення користувачів і зміцнює довіру до системи.

Широке застосування – універсальність і доступність біометричних ознак означає, що методи біометричної автентифікації можуть застосовуватися в широкому спектрі секторів, включаючи охорону здоров'я, фінанси, освіту, державні служби тощо. Адаптивність біометрії робить її підходящим рішенням для різних потреб безпеки [3].

Економічна ефективність – з часом системи біометричної автентифікації можуть довести свою економічну ефективність за рахунок зниження витрат, пов'язаних з управлінням і відновленням втрачених паролів, токенів або карток доступу.

Інтеграція з існуючими системами – багато сучасних рішень для біометричної автентифікації розроблені для безперешкодної інтеграції з існуючими інфраструктурами безпеки, що робить перехід плавним і безпроблемним.

Підзвітність користувачів – біометрична автентифікація забезпечує остаточний аудиторський слід дій користувача. Це забезпечує більшу підзвітність, оскільки кожна транзакція або доступ можуть бути відстежені до

конкретної особи, що сприяє підвищенню відповідальності та стримує зловмисну діяльність [3].

Інновації та захист на майбутнє – постійний розвиток біометричних технологій та їх інтеграція з новими технологіями, такими як штучний інтелект, гарантують, що біометрична автентифікація залишається передовим і перспективним рішенням для перевірки особистих даних і забезпечення безпеки.

Використовуючи біометричну автентифікацію, як приватні особи, так і організації переходять у сферу підвищеної безпеки та зручності, прокладаючи шлях до більш безпечного та ефективного майбутнього.

Для більшого розуміння такої технології, як біометрична автентифікація, також розглянемо і ряд недоліків, які спричиняють деякі труднощі у її використанні [10].

Можливі помилкові біометричні збіги – хоча це трапляється рідко, помилковий збіг біометричних даних може статися. Це трапляється, коли біометричні дані двох осіб потребують уточнення. Найчастіше це відбувається у випадку двох схожих на вигляд братів і сестер. Якщо біометричні дані, що використовуються, записані неправильно, то ймовірність таких помилок різко зростає.

Щоб зменшити кількість помилкових схвалень у системах біометричної автентифікації, система повинна мати можливість збирати високоякісні біометричні дані. Вона також повинна мати можливість регулярно оновлювати еталонні біометричні дані, щоб відповідати користувачам [10].

Здатність відкидати легальних користувачів – замість того, щоб видавати помилкові спрацьовування, біометрична автентифікація може відмовити легальному користувачеві. Це може статися, коли біометричні характеристики людини змінюються (з віком/внаслідок нещасного випадку/збільшення або зменшення ваги). Погане захоплення зображення також може призвести до помилкових відмов.

Щоб запобігти цьому, треба переконатися, що датчики системи фіксують високоякісні біометричні зразки та шаблони.

Упередженість біометрії – системи біометричної верифікації працюють на основі алгоритмів машинного навчання [11]. У минулих дослідженнях Національний інститут стандартів і технологій США показав, що афроамериканці та азіати мають у 10-100 разів вищий FAR.

Слід з особливою ретельністю навчати ці алгоритми на всеохоплюючих наборах даних, які не дискримінують раси та демографічні показники. Найкращі системи автентифікації повинні відповідати стандартам ISO, щоб не допускати дискримінації або несприятливого ставлення до жодної групи [10].

Безпечний та безперебійний цифровий досвід – бренди будуються на довірі та відмінних відносинах з клієнтами. Для бізнесу та клієнтів важливий якісний та безпечний цифровий досвід. Системи верифікації ідентичності повинні забезпечувати баланс між безпекою та зручністю відповідно до потреб організації.

Мультибіометричні системи можуть поєднувати перевірку автентичності за кількома біометричними характеристиками [10].

Має сенс багаторівнева перевірка ідентифікаційних даних, щоб забезпечити ідеальний рівень швидкості та безпеки біометричної автентифікації. Треба проводити перевірку імен, дат народження та адрес разом з біометричними даними, щоб встановити довіру до особистості людини.

Біометрична автентифікація є свідченням прогресу в технологіях безпеки, пропонуючи поєднання підвищеної безпеки, зручності та ефективності. Від захисту конфіденційної інформації в секторі охорони здоров'я до зміцнення транзакцій у фінансовому світі – застосування біометричної автентифікації є широким і різноманітним. Реальні приклади, такі як реалізовані компанією Aratek, демонструють відчутні переваги та трансформаційний вплив біометричних рішень у різних галузях.

Оскільки технології продовжують розвиватися, для приватних осіб і організацій вкрай важливо залишатися на крок попереду, використовуючи інноваційні рішення, які не тільки вирішують поточні проблеми, а й передбачають майбутні. Біометрична автентифікація з її безліччю переваг є одним з таких рішень, що обіцяє безпечніше та ефективніше цифрове майбутнє.

2 ТИПИ БІОМЕТРИЧНИХ ПРИСТРОЇВ ТА ЇХ АНАЛІЗ

Використання біометричних пристроїв настільки проникло в повсякденне життя, що навіть якщо людина не знає про їх існування, ймовірно, взаємодіяла з ними в різних сценаріях, наприклад, коли йшла на роботу і використовувала своє обличчя для доступу до воріт будівлі або коли платила за щось, використовуючи відбитки пальців, і це лише кілька прикладів [12].

Стає все більш очевидним, що біометричні технології та різноманітні пристрої відіграватимуть ключову роль у забезпеченні безпеки, роблячи життя простішим і зручнішим.

У цьому розділі буде розглянуто різні типи біометричних пристроїв, які сьогодні доступні на ринку, про те, як вони працюють, і наведено приклади.

Біометричний пристрій – це електронний пристрій, який використовує біометричні ідентифікатори для ідентифікації та верифікації осіб [13].

Рисунок 2.1 – Біометричні пристрої

Біометричні пристрої мають вбудовані біометричні датчики, які використовують різноманітні сенсорні технології для збору унікальних фізичних або поведінкових характеристик людини, таких як відбитки пальців, риси обличчя, відбитки долонь, сканування райдужної оболонки ока, геометрія руки, голосові патерни, хода людини та інші біометричні ідентифікатори.

Біометричні пристрої можна знайти будь-де, включаючи – аеропорти, банки, урядові будівлі, лікарні, офіси, школи та багато іншого.

Біометричні апаратні пристрої набувають все більшого поширення; за даними Meticulous Research®x, до 2029 року ринок біометричних систем (включаючи біометричні апаратні продукти та програмні продукти) становитиме 51,6 мільярда доларів США. З 2022 по 2029 рік середньорічний темп зростання складе 12,4% [14].

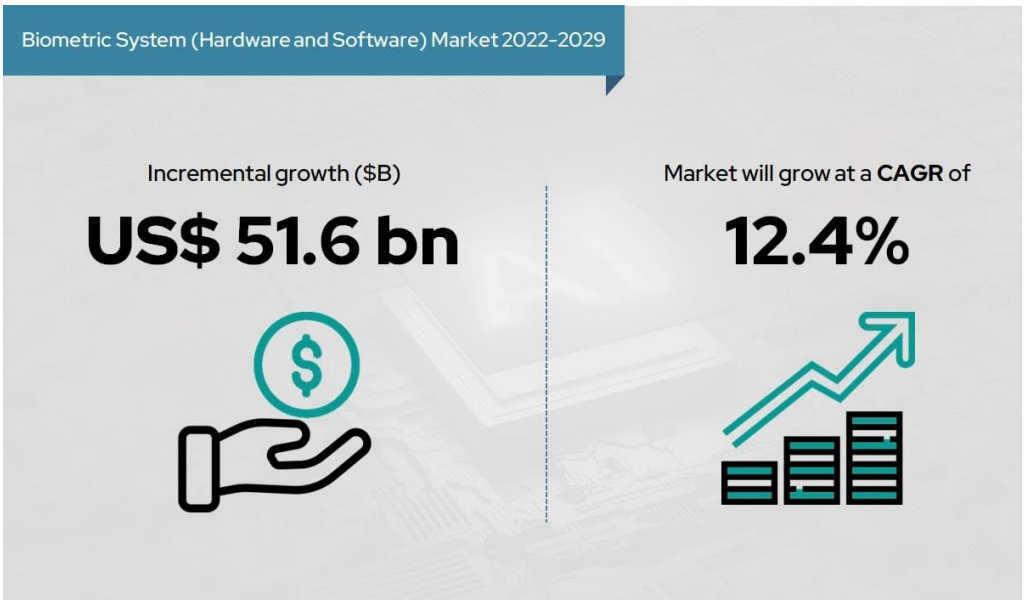

Рисунок 2.2 – Ринок біометричних систем (включаючи апаратне та програмне забезпечення) 2022-2029 рр. від Meticulous Research®

Очікується, що зростання ринку біометричних систем буде зумовлене зростанням ринку біометричних пристроїв. Цей сегмент розширюється у світовій біометричній індустрії завдяки зростаючому попиту на мобільні біометричні пристрої, більше уваги приділяється апаратно-орієнтованим засобам безпеки, а біометричні технології все частіше використовуються в побутовій електроніці для біометричної автентифікації та біометричної ідентифікації [12].

Біометричні пристрої стають все більш популярними для ідентифікації та автентифікації, використовуючи різні методи для ідентифікації особи, такі як розпізнавання відбитків пальців, розпізнавання обличчя, сканування вен долоні, розпізнавання райдужної оболонки ока і навіть розпізнавання голосу.

Список біометричних пристроїв [12]:

– контактні біометричні пристрої;

– безконтактні біометричні пристрої;

– гібридні або комбіновані біометричні пристрої.

2.1 Контактні біометричні пристрої

Контактні біометричні пристрої – це тип біометричних пристроїв, які вимагають фізичного контакту для збору біометричних даних. Цей тип пристроїв зазвичай використовується для збору відбитків пальців або долоні за допомогою електронного датчика [12].

Контактні біометричні пристрої можна розділити на три типи, які найчастіше зустрічаються на ринку:

– сканери відбитків пальців;

– сканери відбитків долонь;

– сканери геометрії рук.

Сканери відбитків пальців є найпоширенішим типом контактних біометричних пристроїв [15]. Існує два основних типи сканерів відбитків пальців – оптичні та ємнісні.

Оптичні сканери відбитків пальців використовують оптичну технологію для сканування зображень відбитків пальців. Він сканує пальці за допомогою світлодіодного світла, щоб знайти зміну в картині відбитого світла, що викликає електричний сигнал, який потім перетворюється на цифрові дані.

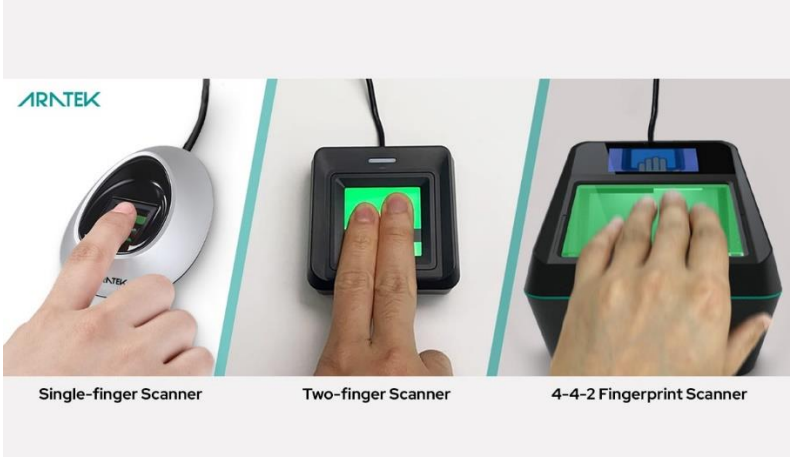

Рисунок 2.3 – Оптичні сканери відбитків пальців

В ємнісних сканерах відбитків пальців ємнісні датчики використовуються для вимірювання змін електричного струму, спричинених змінами в тому, наскільки добре шкіра проводить електрику [12].

Рисунок 2.4 – Ємнісні сканери відбитків пальців

Сканери відбитків пальців – це тип біометричного пристрою, який використовується вже досить давно. Це надзвичайно корисний інструмент для реєстрації та перевірки особи в різних ситуаціях, включаючи отримання національного посвідчення особи, реєстрацію для участі в голосуванні, банківські операції, реєстрацію SIM-карти, захист кібербезпеки і так далі. Крім того, біометрична система може забезпечити захист від використання фальшивих або підроблених відбитків пальців, що є основною проблемою в галузі біометрії, використовуючи біометричну техніку виявлення живої людини [12].

Нарешті, у зв'язку з пандемією Covid-19 на ринку з'явилося ще кілька безконтактних сканерів відбитків пальців, які забезпечують більш гігієнічний спосіб автентифікації особи за допомогою високоякісних зображень відбитків пальців.

Сканери відбитків долонь – це різновид контактних біометричних пристроїв, які роблять зображення долоні, а потім використовують це зображення для підтвердження ідентифікації. Ці сканери отримують зображення долоні за допомогою оптичного датчика зображення. Він працює подібно до сканера відбитків пальців, за винятком того, що він зчитує долоню.

Рисунок 2.5 – Сканер відбитків долонь

Сканери відбитків долонь можуть ідентифікувати особу, зчитуючи її унікальні біометричні дані з візерунків вен на долоні та порівнюючи їх з базою даних вже встановлених шаблонів. Ці сканери з'явилися на початку 2000-х років, і їх часто використовують у місцях, що вимагають високого рівня безпеки, таких як урядові будівлі та військові бази [12].

Сканери геометрії рук використовуються для ідентифікації людей шляхом вимірювання розміру та форми їхніх рук.

Ці пристрої мають пластину з вбудованими штифтами, які направляють положення людської руки для досягнення найкращих результатів. Після того, як розміщується рука, камери з зарядовим зв'язком роблять її зображення, яке потім порівнюється з шаблоном, що зберігається в пам'яті пристрою. Якщо біометричні дані геометрії руки збігаються з шаблоном, пристрій розблокується.

Рисунок 2.6 – Сканери геометрії рук

Пристрої геометрії руки використовуються в різноманітних системах біометричної автентифікації та додатках, включаючи, але не обмежуючись ними: перевірка ідентифікації, облік робочого часу та відвідування, а також контроль фізичного доступу [16].

2.2 Безконтактні біометричні пристрої

Безконтактні біометричні пристрої можуть знімати біометричні дані без необхідності фізичного контакту.

Безконтактні біометричні пристрої можна розділити на три типи, які широко доступні на ринку [12]:

– термінали розпізнавання обличчя;

– сканери райдужної оболонки ока;

– сканери вен на долоні;

На сьогоднішній день термінали розпізнавання обличчя можуть бути найбільш широко використовуваним безконтактним біометричним пристроєм [17].

Рисунок 2.7 – Термінали розпізнавання обличчя

Термінали розпізнавання обличчя фіксують зображення обличчя за допомогою спеціалізованих камер, таких як HDR або ІЧ-камери. Ці камери можуть розпізнавати риси обличчя, такі як очі, ніс, рот і навіть відтінок шкіри. Під час використання термінал розпізнавання обличчя може миттєво сканувати обличчя, коли людина проходить повз нього в режимі реального часу. Після

отримання зображення обличчя, програмні алгоритми розпізнавання обличчя використовуються для визначення особи на основі рис обличчя, які були зафіксовані камерою, і порівнюються з базою даних раніше бачених облич. Якщо знайдено збіг, особу можна підтвердити.

Деякі сучасні пристрої розпізнавання облич, такі як біометричний пристрій контролю доступу Aratek BA8300, також можуть зчитувати безконтактні RFID-картки, що додає ще один рівень безпеки і гарантує, що контроль доступу здійснюється правильно і надійно [18]. Завдяки двофакторній автентифікації, зчитувач RFID-карт контролю доступу додає ще один рівень безпеки, щоб гарантувати, що тільки авторизовані люди можуть потрапити в чутливі зони [19]. Це захищає власність людини від можливих загроз і небажаних відвідувачів.

Під час пандемії COVID-19 термінали розпізнавання облич швидко стали найпоширенішим типом пристроїв ідентифікації безпеки, що використовуються в системах біометричного контролю доступу. Це відбулося головним чином завдяки тому, що термінали розпізнавання облич не потребують фізичного контакту і мають широкий спектр можливостей. Наприклад, інфрачервоні датчики та алгоритми розпізнавання масок можуть бути легко інтегровані в ці термінали, щоб вимірювати температуру тіла і визначати, чи носить людина маску під час сканування обличчя. Це ефективне рішення для контролю входу в будівлю, оскільки воно може миттєво повідомити, якщо хтось заразився інфекційним захворюванням, роблячи громадські місця безпечнішими.

Рисунок 2.8 – Термінал розпізнавання облич Aratek з вимірюванням температури тіла та розпізнаванням масок для контролю доступу

Сьогодні термінали розпізнавання облич стають все більш поширеними в громадських місцях, таких як аеропорти і торгові центри, щоб підвищити безпеку контролю доступу. Ці безпечні пристрої дозволяють отримати доступ до будівель або контрольно-пропускних пунктів, не роблячи і не торкаючись нічого, окрім як показати своє обличчя і пройти повз, полегшуючи життя і водночас забезпечуючи безпеку [12].

Сканери райдужної оболонки ока також є поширеним типом безконтактних біометричних пристроїв. Ці пристрої фіксують райдужну оболонку ока за допомогою камери ближнього інфрачервоного світла для розпізнавання райдужної оболонки [20]. Райдужна оболонка містить інформацію, яка може бути ідентифікована тільки однією людиною, це дозволяє сканерам райдужної оболонки ідентифікувати людину на основі чітких пігментних візерунків (забарвлення райдужної оболонки), які присутні на райдужці.

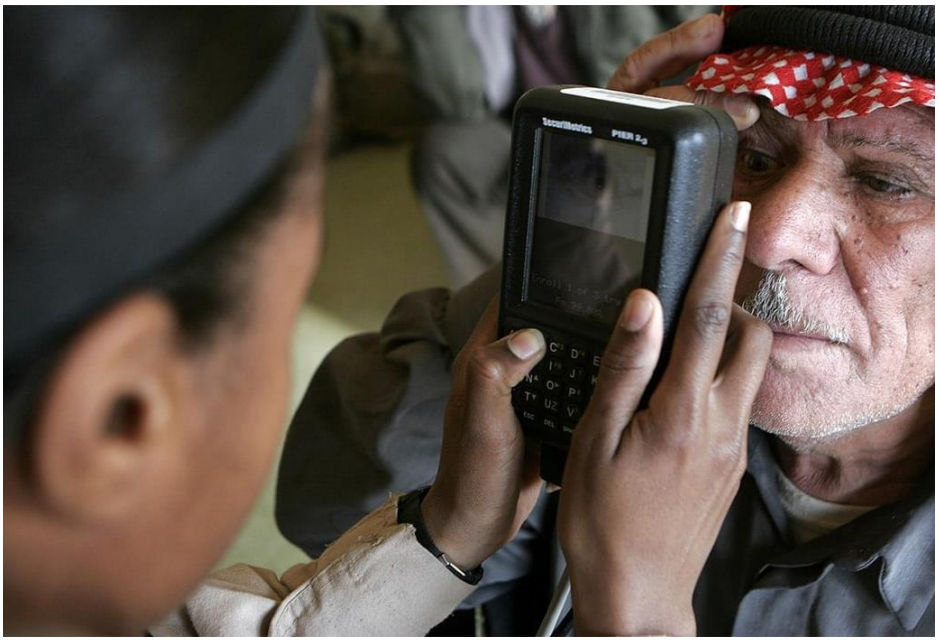

Рисунок 2.9 – Сканер райдужної оболонки ока, що виконує розпізнавання райдужної оболонки

Сканери райдужної оболонки ока і розпізнавання райдужної оболонки корисні для швидкої і точної ідентифікації людей. Ці біометричні пристрої використовуються як безконтактне рішення різними організаціями, включаючи правоохоронні органи, банки, лікарні, аеропорти, державні установи,

прикордонні служби та інші. Ці пристрої також використовуються з метою ідентифікації в різних країнах, включаючи Індію, Мексику, Сполучені Штати Америки та багато інших [12].

Сканери вен долоні – це тип безконтактного біометричного пристрою, який знімає зображення вен на долоні, використовуючи ближнє інфрачервоне світло для освітлення вен у руці (мережа кровоносних судин під шкірою долоні). Біометричні дані цього зображення вен руки можуть бути зіставлені з базою даних для підтвердження особи в процесі розпізнавання малюнка вен.

Рисунок 2.10 – Сканери вен на долоні

Оскільки сканери долонних вен точні і не вимагають фізичного контакту з користувачем, вони стають все більш популярними в останні роки. Це робить їх ідеальним вибором для використання в системах безпеки в найрізноманітніших умовах, особливо в таких місцях, як лікарні, аеропорти та офісні будівлі, які вимагають більш високого рівня гігієни та безпеки.

Сканер сітківки ока – це біометричний пристрій, який випромінює промінь низько-енергетичного інфрачервоного світла в око, щоб виконати сканування сітківки, поки людина дивиться через окуляр. Таким чином створюється зображення крихітних капілярів сітківки, які є кровоносними

судинами в задній частині ока. На основі цього зображення можна створити біометричну карту, за допомогою якої можна з'ясувати особу [12].

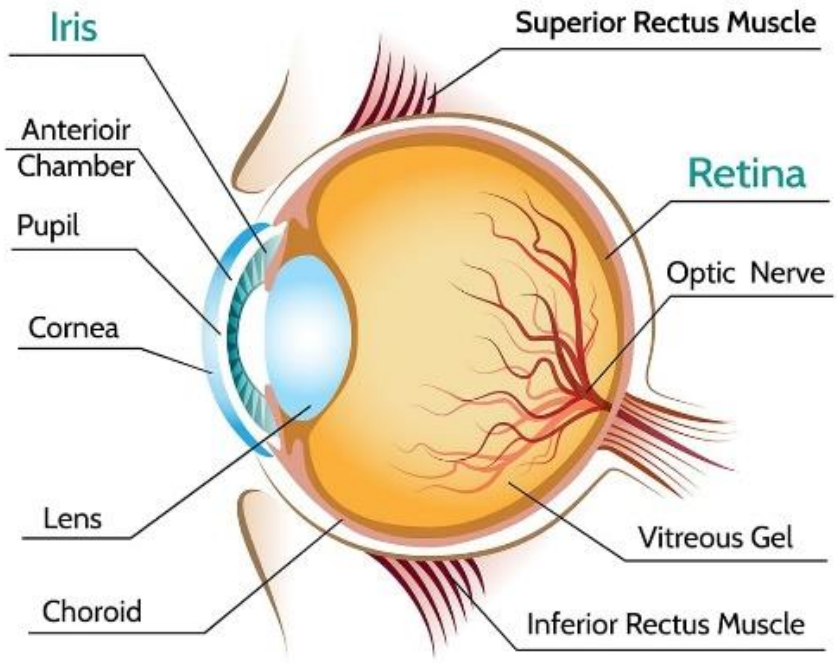

Рисунок 2.11 – Анатомія ока, що показує розташування райдужної оболонки та сітківки

На біометричному ринку немає сканерів сітківки ока, оскільки ця біометрична технологія все ще є новою, і їх створення є дорогим порівняно з іншими типами обладнання [12].

Хоча в різних засобах масової інформації та інтернет-джерелах є згадки та зображення сканерів сітківки ока, більш детальне вивчення виявляє розбіжності в їхньому представленні. Наприклад, такі системи, як BAT і HIIDE, які часто називають сканерами сітківки, насправді використовують технологію сканування райдужної оболонки ока [21, 22]. Аналогічно, такі пристрої, як LG Iris IrisAccess® 3000, які на деяких зображеннях помилково позначені як сканери сітківки, насправді є спеціальними сканерами райдужної оболонки ока [23]. Дуже важливо розрізняти ці два види очної біометрії.

Рисунок 2.12 – Деякі приклади того, як сканери райдужної оболонки помилково видають за сканери сітківки

Станом на 2024 рік технологія сканування сітківки в основному знаходить своє застосування в діагностиці сітківки, як, наприклад, сканер сітківки Eidon, а не в біометричній автентифікації [24]. Ця відмінність підкреслює той факт, що справжнім сканерам сітківки ока для біометричних цілей ще належить зайняти значну частку ринку.

2.3 Гібридні або комбіновані біометричні пристрої

Гібридний біометричний пристрій або мультибіометричний пристрій – це пристрій, який фіксує та перевіряє особу людини за допомогою двох або більше біометричних методів [12].

Багатофакторний портативний біометричний пристрій або біометричні портативні мобільні пристрої, такі як ті, що використовують правоохоронці в аеропортах або працівники відділів реєстрації виборців на виборчих дільницях, часто використовують гібридну біометричну або багатофакторну автентифікацію для ідентифікації та верифікації людей [17]. Це робить процес ідентифікації більш точним і безпечним. Люди можуть використовувати ці мобільні біометричні пристрої для сканування відбитків пальців та інших біометричних даних, щоб отримати точну інформацію про особу без необхідності брати її під варту.

Рисунок 2.13 – Гібридний біометричний пристрій поєднує в собі розпізнавання обличчя та відбитків пальців

Термінали багатофакторного розпізнавання обличчя. Наприклад, в системах контролю доступу розгортання багатофакторного терміналу розпізнавання обличчя з вбудованим модулем датчика відбитків пальців для розпізнавання відбитків пальців є відмінним підходом для забезпечення більшої безпеки. Він може спочатку виконати ідентифікацію "1:N", щоб визначити, "хто ви", а потім додати другий фактор і попросити відсканувати відбиток пальця, щоб виконати аутентифікацію "1:1" і відповісти на питання "Ви той, за кого себе видаєте?" Це ускладнює доступ несанкціонованих користувачів до захищених зон [12].

Рисунок 2.14 – Багатофункціональний термінал розпізнавання облич з вбудованим модулем датчика відбитків пальців

Відбитки пальців, райдужна оболонка ока та розпізнавання обличчя – найпоширеніші біометричні модальності, що використовуються в гібридних пристроях. У порівнянні з одномодальними пристроями, гібридні біометричні пристрої мають ряд переваг [12].

По-перше, вони можуть забезпечити вищий рівень безпеки, оскільки використовують мультибіометричні дані для автентифікації користувачів; додавання другого або третього біометричного атрибуту ускладнює підробку, ніж одного. Крім того, деякі пристрої використовують техніку виявлення біометричної активності, яка допомагає запобігти підробці біометричних даних і додає додатковий рівень безпеки.

По-друге, оскільки кожна модальність може надавати свій власний унікальний шаблон перевірки, вони можуть бути більш точними, ніж одномодальні пристрої.

По-третє, гібридні пристрої можуть бути довговічнішими, ніж одномодальні, оскільки вони можуть продовжувати працювати, навіть якщо одна з біометричних модальностей виходить з ладу.

Загалом, гібридні біометричні пристрої мають низку переваг над одномодальними пристроями, включаючи підвищену безпеку, точність і надійність.

2.4 Аналіз типів біометричних пристроїв

Біометричні пристрої – це електричні пристрої, що використовуються для біометричної верифікації, ідентифікації та автентифікації. Вони можуть бути використані для ідентифікації людей на основі їхніх унікальних людських особливостей, таких як відбитки пальців, сканування райдужної оболонки ока, риси обличчя тощо.

В таблиці 2.1 представлено аналіз та порівняння типів біометричних пристроїв [12].

Таблиця 2.1 – Аналіз та порівняння типів біометричних пристроїв

Хар-ки / Пристрої	Фіз. контакт	Поши-реність	Швид-кість	Безпека	Точність	Застосування організаціями	Ринок	Вартість
Сканери відбитків пальців	Так	Висока	Середня	Середня	Низька	Іноді	Є	Середня
Сканери відбитків долонь	Так	Середня	Середня	Середня	Низька	Іноді	Є	Середня
Сканери геометрії рук	Так	Середня	Середня	Середня	Низька	Іноді	Є	Середня
Термінали розпізнавання обличчя	Ні	Висока	Середня	Середня	Середня	Часто	Є	Висока
Сканери райдужної оболонки ока	Ні	Висока	Висока	Висока	Висока	Часто	Є	Висока
Сканери вен на долоні	Ні	Середня	Середня	Середня	Середня	Часто	Є	Висока
Сканери сітківки ока	Ні	Низька	Середня	Висока	Висока	Не використовується	Немає	Дуже висока
Термінали багатофакторного розпізнавання обличчя	Так/ні	Висока	Висока	Висока	Висока	Часто	Є	Висока

Оскільки існує багато різних категорій біометричних пристроїв, кожна з яких має свою нішу застосування і коло користувачів, простого рішення цієї проблеми не існує. Однак, уряд та правоохоронні органи, фінансові установи, бізнес та медичні заклади є одними з найчастіших користувачів біометричних пристроїв.

З огляду таблиці та проведення аналізу біометричних пристроїв, можна зробити висновок, що найкращим серед пристроїв є сканер райдужної оболонки ока, тому що він має найвищу швидкість обробки даних людини, високу точність, при визначенні особи, так як пігметні візерунки, які пристуні на райдужці, можуть належати тільки одній людині, не потребує фізичного контакту, що в наш час є дуже важливою перевагою. Сканери райдужної

оболонки ока часто використовують організації, для більш точного та швидкого розпізнавання особи.

Є кілька причин, чому слід використовувати біометричні пристрої. По-перше, біометрія може забезпечити більш безпечний метод автентифікації користувачів. По-друге, біометричні пристрої стають все більш доступними і простими у використанні, що робить їх ідеальним вибором для широкого спектру застосувань. Нарешті, біометрія може забезпечити зручний спосіб доступу користувачів до додатків.

3 ПОРІВНЯННЯ МЕТОДІВ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

3.1 Метод Аналізу Ієрархій

У даному розділі проводиться порівняння методів біометричної автентифікації при застосуванні метода аналіза ієрархій. В основі цього методу відбувається декомпозиція завдання за вибором переважного варіанта певної системи та поділення завдання на більш прості частини з урахуванням отриманих оцінок від експертів по парним порівнянням простих частин завдання, як показано на рисунку 3.1 [25, 26].

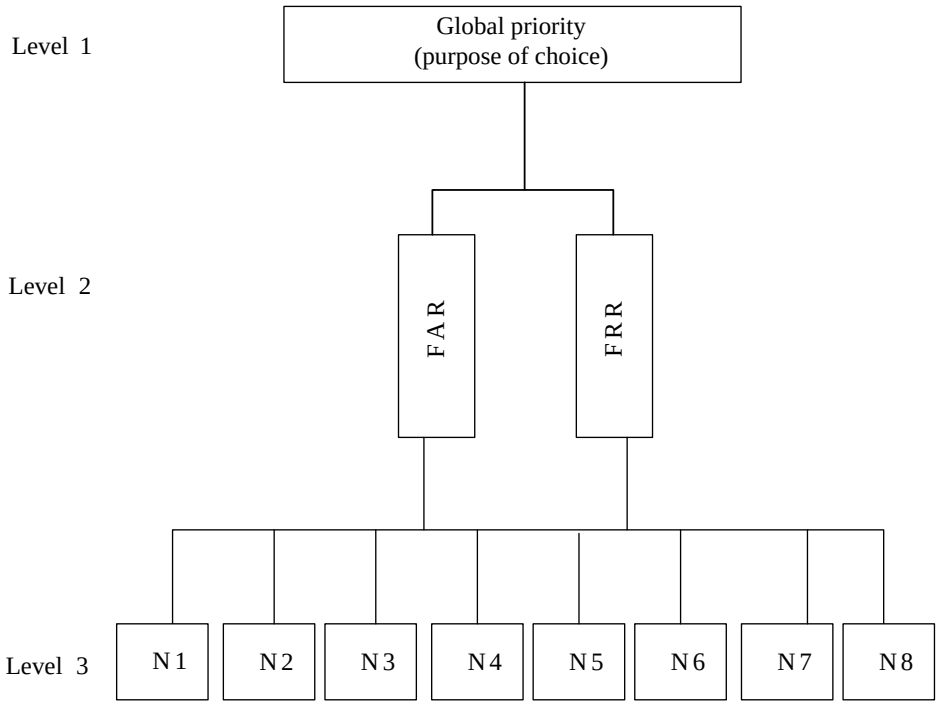

Рисунок 3.1 – Декомпозиція завдання вибору

Згідно методу формуються матриці на основі результатів від експертів. Далі проводиться обробка всіх матриць попарних порівнянь на всіх рівнях ієрархії рис. 3.1.

Після обробки матриць обчислюються власні вектори V_i та вектори пріоритетів P_i .

$$P_i = \frac{V_i}{S}\ ,\ V_i = \sqrt[n]{\prod_{j=1}^{n} a_{ij}}\ ,\quad \mathrm{S} = \sum_{i=1}^{n} V_i\ ,\ i = \overline{1,n}\ . \qquad 3.1$$

де n – кількість показчиків якості, N – кількість порівнювальних систем.

Для того, щоб обрати переважний варіант системи необхідно обчислити вектор глобального пріоритету $\vec{C}$, який знаходиться за виразом:

$$C_j = \sum_{i=1}^{n} P_i Q_{ij}\ ,\ j = \overline{1,N}\ . \qquad 3.2$$

Переважний варіант системи обирається за максимальним значенням компонент вектора $\vec{C}$.

3.2 Порівняння методів біометричної автентифікації

Для того, щоб була можливість якісно і точно порівняти системи були обрані наступні показники якості [25, 26]:

– FAR – коефіцієнт помилкового підтвердження. Відбувається при обставинах, коли система дозволяє доступ користувачам, які не зареєстровані в системі;

– FRR – коефіцієнт помилкової відмови. Відбувається при обставинах, коли система відмовляє у доступі зареєстрованому користувачеві.

Обидва параметри обчислюються за допомогою методів математичної статистики. Чим нижче значення цих показників, тим вище якість аутентифікації користувача.

Зокрема, у дослідженнях було проведено багаторазові порівняння з використанням ієрархічних методів аналізу для вибору переважних варіантів аналізу відбитків пальців, 2D-розпізнавання обличчя та біометричних методів аутентифікації на основі райдужної оболонки, сітківки, малюнка вен, почерку та голосу.

У таблиці 3.1 наведено середні значення показників FAR та FRR для різних біометричних систем контролю та управління доступом (СКУД) [25, 26].

Таблиця 3.1 – Середні значення показників FAR та FRR

№	Тип біометричної системи	FAR, %	FRR, %
N1	аналіз відбитку пальця	0,001	0,6
N2	розпізнавання людини 2D	0,1	2,5
N3	розпізнавання людини 3D	0,0005	0,1
N4	райдужна оболонка ока	0,00001	0,016
N5	сітківка ока	0,0001	0,4
N6	малюнок вен	0,0008	0,01
N7	клавіатурний почерк	0,01	3,0
N8	голос	1	3

Для зручності були перетворені вихідні значення показників якості FAR і FRR, які наведені в таблиці 3.2. Також, була виконана нормалізація показників якості.

Таблиця 3.2 – Нормування початкових значень показників якості FAR та FRR до максимального значення

№	Тип біометричної системи	FAR	FRR
N1	аналіз відбитку пальця	0,01	0,016
N2	розпізнавання людини 2D	0,0001	0,004
N3	розпізнавання людини 3D	0,02	0,1
N4	райдужна оболонка ока	1	0,625
N5	сітківка ока	0, 1	0,025
N6	малюнок вен	0,0125	1
N7	клавіатурний почерк	0,001	0,003
N8	голос	0,0001	0,003

У таблиці 3.3 представлена матриця парних порівнянь показників якості FAR та FRR.

Таблиця 3.3 – Матриця парних порівнянь показників якості FAR та FRR

Показники якості	FAR	FRR	V_i	P_i
FAR	1	2	1.41	0,66
FRR	0.5	1	0.7	0,33

У таблиці 3.4 представлена матриця парних порівнянь по відношенню до показника якості FAR.

Таблиця 3.4 – Матриця парних порівнянь по відношенню до показника якості FAR

FAR	N1	N2	N3	N4	N5	N6	N7	N8	V_i	P_i
N1	1	7	0.2	0.142	0.166	4	6	7	1.238737	0.088093
N2	0.142	1	0.125	0.111	0.125	0.142	0.2	0.5	0.207953	0.014789
N3	5	8	1	0.166	0.2	6	7	8	2.143839	0.152459
N4	7	9	6	1	5	7	8	9	5.589353	0.397486
N5	6	8	5	0.2	1	6	7	8	3.356971	0.23873
N6	0.25	7	0.166	0.142	0.166	1	3	7	0.78473	0.055806
N7	0.166	5	0.142	0.125	0.142	0.333	1	5	0.492887	0.035052
N8	0.142	2	0.125	0.111	0.125	0.142	0.2	1	0.247299	0.017587

У таблиці 3.5 представлена матриця парних порівнянь по відношенню до показника якості FRR.

Таблиця 3.5 – Матриця парних порівнянь по відношенню до показника якості FRR

FRR	N1	N2	N3	N4	N5	N6	N7	N8	V_i	P_i
N1	1	4	0.2	0.142	0.333	0.142	5	5	0.778048	0.056669
N2	0.25	1	0.166	0.125	0.2	0.125	3	3	0.429925	0.031314
N3	5	6	1	0.2	4	0.2	7	7	1.978927	0.144135
N4	7	8	5	1	6	0.333	9	9	3.819705	0.278208
N5	3	5	0.25	0.166	1	0.166	6	6	1.178471	0.085834
N6	7	8	5	3	6	1	9	9	5.027643	0.366187
N7	0.2	0.333	0.142	0.111	0.166	0.111	1	2	0.28083	0.020454
N8	0.2	0.333	0.142	0.111	0.166	0.111	0.5	1	0.236149	0.0172

У таблиці 3.6 наведені розраховані значення компонентів вектора пріоритету технічного варіанту для кожного показника якості, а також компонентів глобального вектора пріоритету, таких як:

– компоненти вектора пріоритету показника якості;

– компоненти вектора пріоритету показника якості FAR;
– компоненти вектора пріоритету показника якості FRR;
– компоненти пріоритету показника якості FRR.

Таблиця 3.6 – Розраховані значення компонент вектора

Тип біометричної системи	Q_{ij}		$\vec{C}$
	FAR	FRR	
аналіз відбитку пальця	0.088	0.056	0.07656
розпізнавання людини 2D	0.014	0.031	0.01947
розпізнавання людини 3D	0.152	0.144	0.14784
райдужна оболонка ока	0.397	0.278	0.35376
сітківка ока	0.238	0.085	0.18513
малюнок вен	0.055	0.366	0.15708
клавіатурний почерк	0.035	0.02	0.0297
голос	0.017	0.017	0.01683
P_i	0,66	0,33	

Після розрахунків на основі максимального значення $\vec{C}$ та проведення аналізу характеристик біометричних пристроїв у попередньому розділі обрано переважний метод біометричної автентифікації – райдужна оболонка ока, з характеристиками FAR 0,00001% та FRR 0,016% .

ВИСНОВКИ

У кваліфікаційній роботі було розглянуто біометричну автентифікацію, поширені види біометричної автентифікації, її зростання, переваги та недоліки, також були розглянуті приклади використання біометричної автентифікації в різних країнах світу та різних установах.

Розглянуто типи біометричних пристроїв, які на даний час існують та використовуються усюди, також були розглянуті типи пристроїв, які ще не ввійшли до ринку у зв’язку з причинами недостатньої обізнаності в системі. Проведено аналіз типів біометричних пристроїв та обрано переважний пристрій – сканер райдужної оболонки ока.

Також було проведено порівняння біометричних методів автентифікації при застосуванні метода аналіза ієрархії. Після розрахунків на основі максимального значення $\vec{c}$ обрано переважний метод біометричної автентифікації – райдужна оболонка ока, з характеристиками FAR 0,00001% та FRR 0,016% .

Використання біометрії може вирішити проблеми надійності і підвищити достовірність аутентифікації та ідентифікації об'єктів при організації доступу до систем з великою кількістю користувачів, а також при організації доступу до критично важливих систем у складі систем контролю і управління фізичним доступом або в якості додаткових елементів аутентифікації.

Було проведено порівняльний аналіз декількох біометричних систем контролю доступу на основі набору показників якості. Переважні біометричні методи були знайдені за допомогою методу ієрархічного аналізу. Це метод райдужної оболонки ока.

Апробація результатів дослідження кваліфікаційної роботи опублікована у двох тезах доповіді на конференції III INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «THEORETICAL AND PRACTICAL ASPECTS OF MODERN SCIENTIFIC RESEARCH» Seoul і на 28-Й МОЛОДІЖНИЙ МІЖНАРОДНИЙ ФОРУМ «РАДІОЕЛЕКТРОНІКА І МОЛОДЬ В XXI СТОЛІТТІ» Харків, а також підготовлено статтю і направлено до редакції до міжнародного журналу International Science Journal of Engineering & Agriculture, Poland.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. – 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2015. – 492 с.

2. What is Biometrics? Definition, Data Types, Trends (2024) [Електронний ресурс]. – Режим доступу: https://www.aratek.co/news/what-is-biometrics-definition-data-types-trends.

3. Exploring Biometric Authentication: From Basics to Case Studies [Електронний ресурс]. – Режим доступу: https://www.aratek.co/news/exploring-biometric-authentication-from-basics-to-case-studies.

4. Biometric Authentication and Identification Market [Електронний ресурс]. – Режим доступу: https://straitsresearch.com/report/biometric-authentication-and-identification-market.

5. Biometric Authentication for Bank Teller Management in Indonesia [Електронний ресурс]. – Режим доступу: https://www.aratek.co/case-studies/biometric-authentication-for-bank-teller-management-in-indonesia.

6. School Access Control for Beijing Dance Academy [Електронний ресурс]. – Режим доступу: https://www.aratek.co/case-studies/school-access-control-for-beijing-dance-academy.

7. University (ISSEG) Biometric Attendance Management in Guinea [Електронний ресурс]. – Режим доступу: https://www.aratek.co/case-studies/university-lisseg-attendance-management-in-guinea.

8. India Aadhaar Enabled Payment System (AePS) [Електронний ресурс]. – Режим доступу: https://www.aratek.co/case-studies/india-aadhaar-enabled-payment-system-aeps.

9. Biometric Refugee Registration in Turkey [Електронний ресурс]. – Режим доступу: https://aratek.co/case-studies/biometric-refugee-registration-in-turkey.

10. Biometric Verification [Електронний ресурс]. – Режим доступу: https://diro.io/biometric-verification/.

11. Machine Learning Technology for Detecting Fraud: How to Leverage Technologies? [Електронний ресурс]. – Режим доступу: https://diro.io/machine-learning-for-detecting-fraud/.

12. Biometric Devices 101: Definition and Examples [Електронний ресурс]. - Режим доступу: https://www.aratek.co/news/biometric-devices-definition-and-examples.

13. What is Biometrics? Definition, Data Types, Trends [Електронний ресурс]. - Режим доступу: https://www.aratek.co/news/what-is-biometrics-definition-data-types-trends.

14. Meticulous Research® [Електронний ресурс]. - Режим доступу: https://www.meticulousresearch.com/product/biometric-system-market-5309.

15. Fingerprint Scanner [Електронний ресурс]. - Режим доступу: https://www.aratek.co/product-category/fingerprint-scanner.

16. How a Biometric Attendance System Can Benefit Your Business [Електронний ресурс]. - Режим доступу: https://www.aratek.co/news/how-a-biometric-attendance-system-can-benefit-your-business.

17. Biometric Terminal [Електронний ресурс]. - Режим доступу: https://www.aratek.co/product-category/biometric-terminal#truface-terminal.

18. BA8300 [Електронний ресурс]. - Режим доступу: https://www.aratek.co/product/face-recognition-terminal-ba8300.

19. 10 Benefits of RFID Access Control Systems [Електронний ресурс]. - Режим доступу: https://www.aratek.co/news/10-benefits-of-rfid-access-control-systems.

20. Unlocking the Mystery of Iris Recognition [Електронний ресурс]. - Режим доступу: https://www.aratek.co/news/what-is-iris-recognition.

21. Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE) [Електронний ресурс]. - Режим доступу: https://nist.gov/system/files/documents/2021/03/23/ansi-nist_archived_vermury-bat-hiide.pdf.

22. This retina scanner tracks terrorists anywhere in the world [Електронний ресурс]. - Режим доступу: https://www.wearethemighty.com/mighty-tactical/this-retina-scanner-tracks-terrorists-anywhere-in-the-world/.

23. LG IrisAccess® 3000 Iris Recognition System [Електронний ресурс]. - Режим доступу: https://www.sourcesecurity.com/lg-iris-irisaccess-3000-technical-details.html.

24. Eidon Retinal scanner [Електронний ресурс]. - Режим доступу: https://www.crystalvisioneyes.com/eidonscanner.html.

25. Скорик Юлія, Безрук Валерій. Вибір переважного методу біометричної автентифікації. International Science Journal of Engineering & Agriculture Vol. 2, No. 4, 2023, pp. 1 – 7.

26. Valeriy, B., Yulia, S., Victotia, V. , Yuriy, K. Multicriterial Analysis and Selection of Mobile Communication Technologies of the Fourth and Fifth Generation // 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings, 2019, стр. 400–403.