МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **СИСТЕМА КОНТРОЛЮ ДОСТУПОМ НА ОСНОВІ БІОМЕТРИЧНИХ ВЛАСТИВОСТЕЙ СУБ`ЄКТА**

Студент групи СЗЗ-51 Бабій Сергій Володимирович _____
(підпис)

Науковий керівник: д.т.н., проф., Ахрамович Володимир Миколайович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Бабію Сергію Володимировичу

1.Тема роботи: Система контролю доступом на основі біометричних властивостей суб`єкта, затверджено наказом від « 24 » лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси забезпечення контролю доступом на об`єктах інформаційної діяльності.

4. Предметом дослідження: технології захисту, які забезпечують безпеку об`єктів інформаційної діяльності при контролі доступом.

5. Мета роботи: удосконалення та рекомендації щодо застосування біометричних методів контролю доступом на об`єктах інформаційної діяльності.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій біометричної ідентифікації та сфери їх використання;
- аналіз та дослідження існуючих методів захисту технологій біометричної ідентифікації;
- створення рекомендацій щодо застосування технологій біометричної ідентифікації на об'єктах інформаційної діяльності.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Ахрамович В.М.
(підпис)

Завдання прийняв до виконання _____Бабій С.В.
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «24» лютого 2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 26.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студент: СЗЗ -51 Бабій С.В. _____

(підпис)

Науковий керівник: д.т.н., проф. Ахрамович В.М. _____

(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____

(підпис)

ЗМІСТ

РЕФЕРАТ

Дипломна робота містить 47 сторінок, 12 рисунків, 5 таблиць.

Наприкінці XX на початок XXI століть застосування біометрії до забезпечення контролю доступу до різних об`єктів значно зріс. Основною перевагою біометричних систем є те, що такі системи спроможні ідентифікувати людину за допомогою її фізіологічних та анатомічних даних. На теперішній час існує велика потреба точної ідентифікації в місцях масового скупчення людей, контролю перепусток і звірки документів на об`єктах інформаційної діяльності (ОІД). В першу чергу ця задача віднеслась до безпеки транспортних, а також державних і міждержавних систем - паспортних, візових, митних, міграційних служб. Усі надійні системи контролю доступом на теперішній час повністю залежать від біометричних технологій, що дають змогу перевіряти особистості величезної кількості людей, які проходять через точку контролю доступом.

Об’єктом дослідження: є процеси забезпечення контролю доступом на об`єктах інформаційної діяльності.

Предметом дослідження: є технології захисту, які забезпечують безпеку об`єктів інформаційної діяльності при контролі доступом.

Мета роботи удосконалення та рекомендації щодо застосування біометричних методів контролю доступом на об`єктах інформаційної діяльності.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій біометричної ідентифікації та сфери їх використання;

- аналіз та дослідження існуючих методів захисту технологій біометричної ідентифікації;
- створення рекомендацій щодо застосування технологій біометричної ідентифікації на об’єктах інформаційної діяльності.

ABSTRACT

Thesis contains 47 pages, 12 figures, 5 tables

In the late XX and early XXI centuries, the use of biometrics to control access to various objects increased significantly. The main advantage of biometric systems is that such systems are able to identify a person using his or her physiological and anatomical data. Nowadays there is a great need for accurate identification in crowded places, control of passes and verification of documents at information activity objects (IAO). First of all, this task is related to the security of transport, as well as state and interstate systems - passport, visa, customs, migration services. All reliable access control systems are currently fully dependent on biometric technologies, which allow verifying the identity of a huge number of people passing through an access control point.

Object of research: are the processes of ensuring access control at the objects of information activity.

The subject of the research is protection technologies that ensure the security of information objects during access control.

The purpose improvement and recommendations for the use of biometric methods of access control at information facilities.

To achieve this goal, the following main tasks are performed:

- analysis of implemented biometric identification technologies and their use;

- analysis and research of existing methods of protection of biometric identification technologies;

- development of recommendations for the use of biometric identification technologies at information facilities.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ОІД	Об`єкт інформаційної діяльності	Object of information activity
БСКД	Біометричні системи контроля доступом	Biometric access control systems
СКД	Системи контроля доступом	Access control systems
АДІС	Автоматизовані дактилоскопічні інформаційні системи	Automated fingerprint information systems
FRR	Помилка першого роду	False rejection rate
FAR	Помилка другого роду	False access rate
БД	Бази даних	Databases
СОРЧ	Системи обліку робочого часу	Working time tracking systems
СУКД	Система управління контролю доступом	Access control management system
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	
ЗЗІ	Засоби захисту інформації	
ІС	Інформаційна система	
ІТС	Інформаційно-телекомунікаційна система	

ОЗП	Оперативний запам’ятовувальний пристрій
УВЧ	Ультра високі частоти

ВСТУП

В завданнях захисту інформації під терміном «контроль доступу» розуміють комбінацію засобів від проникнення на ОІД, який уявляє собою зону, яка охороняється. Санкціонований доступ на ОІД, що захищається, доступний тільки для авторизованих користувачів, які отримали на це право (дозвіл). Найпростішим захистом ОІД є фізичний контроль, який реалізовується завдяки найму персоналу для здійснення захисту, а також механічними засобами, такими як ключі та замки на дверях, або через технічні засоби. У зв'язку з розвиненням технологій біометричні системи контролю доступу (БСКД), останні стають дедалі доступними та сучасними рішеннями. БСКД вважаються безпечнішими по відношенню до звичайних систем контролю доступом (СКД). Це пов`язано з тим, що БСКД порівнюють унікальні для кожної людини параметри такі, як відбитки пальців, райдужна оболонка ока, геометрія обличчя, голос.

Актуальність теми В еру розвитку цифрових технологій проблема безперервного забезпечення захисту інформації є однією з актуальних задач сьогодення. Сучасні класичні програмно-апаратні системи ідентифікації та автентифікації функціонують виключно протягом авторизації користувача в системі. Однак такі підходи не забезпечують достовірність того, що після авторизації в системі продовжує працювати користувач, який має допуск. З погляду оцінки безпеки та механізмів інформаційного захисту (ІЗ) користувачів, велике значення відіграє надійний захист інформації мобільних платформ, локальної критичної інформації, тощо. У тому випадку, коли доступ до пристрою отримує зловмисник, на весь період взаємодії залишається загроза витоку важливої інформації.

Для розв`язання задачі неможливості витоку конфіденційної інформації важливим є використання клавіатурного моніторингу користувачів. На теперішній час одним із перспективних підходів є розпізнавання клавіатурного почерку на основі аналізу динамічних біометричних характеристик людини. Даний метод заснований на аналізі таких характеристик користувача, як швидкість введення тексту, час утримання клавіш,

часовий інтервал між натисканнями на клавіші, частота утворення помилок під час введення даних; частота використання функціональних клавіш та комбінацій, стосовно одного й того самого класу пристроїв введення; рівень аритмічності під час набору тощо. Крім того, такі характеристики як відбиття пальців, око, голос є виключно особистим, тому дані параметри більш надійно захищають ОІД для легітимних користувачів. Тому створення надійних біометричних систем контролю доступом є актуальними на теперішній ч

Об’єктом дослідження: є процеси забезпечення контролю доступом на об`єктах інформаційної діяльності.

Предметом дослідження є технології захисту, які забезпечують безпеку об`єктів інформаційної діяльності при контролі доступом.

Мета роботи удосконалення та рекомендації щодо застосування біометричних методів контролю доступом на об`єктах інформаційної діяльності.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій біометричної ідентифікації та сфери їх використання;
- аналіз та дослідження існуючих методів захисту технологій біометричної ідентифікації;
- створення рекомендацій щодо застосування технологій біометричної ідентифікації на об’єктах інформаційної діяльності.

РОЗДІЛ 1 ОБЛАСТЬ ЗАСТОСУВАННЯ ТА ПРИНЦИПИ СТВОРЕННЯ БІОМЕТРИЧНИХ СИСТЕМ ІДЕНТИФІКАЦІЇ ОСОБИ

Технології БСКД уявляють собою автоматичні або автоматизовані методи розпізнавання особистості людини за її анатомічними та фізіологічними характеристиками або біологічними проявами. Основним інструментом біометричного методу є сканер для вимірювання біометричної характеристики та алгоритм, що дає змогу порівняти її з попередньо зареєстрованою тією самою характеристикою, який називають біометричним шаблоном (БШ). Існують два режими роботи системи:

- верифікація, тобто порівняння характеристик особи з нею самою;
- ідентифікація, тобто порівняння характеристик особи з характеристикою багатьох осіб.

На теперішній час існує не велика кількість можливих біометричних методів, а саме: відбиток пальця, геометрія кисті руки, форма обличчя, райдужна оболонка ока, сітківка ока. Саме ці характеристики використовують для створення відповідних сканерів в практичній реалізації БСКД. Сьогодні існує три основних підходи, а саме: розпізнавання за відбитком пальця, за двовимірним або тривимірним зображенням обличчя та за райдужною оболонкою ока.

1.1. Особливості створення біометричних систем в інформаційній безпеці та захисту інформації

В завданнях інформаційної безпеки та захисту інформації БСКД застосовуються для заміни процедури входу в автоматизовані системи через пароль, смарт-карти тощо на вхід через біометричні характеристики особистості. Широка спроможність використання засобів БСКД є ідентифікація або верифікація за біометричними параметрами в корпоративній мережі або під час входу на робочу станцію автоматизованої системи. Для захисту робочої станції

автоматизованої системи створюються шаблони біометричних даних найчастіше ними є відбитки пальців, які зареєстровані користувачами, які перебувають на ОІД. Після успішної реалізації процедури ідентифікації користувач отримує доступ.

Протягом реалізації технології в корпоративній мережі шаблони БШ активних користувачів, які працюють в мережі, зберігаються централізовано на спеціально створеному сервері аутентифікації. В період входу в мережу, користувач, піддається процедурі біометричної ідентифікації, яка взаємодіє безпосередньо зі спеціалізованим сервером, на якому і перевіряються сформовані ідентифікатори. Створення в структурі корпоративної мережі окремого сервера біометричної автентифікації дає можливість зберігати на такому сервері конфіденційну інформацію, доступ до якої надається виключно на основі біометричної ідентифікаційної ознаки власника інформації. В даній сфері отримало широкого застосування такі технології розпізнавання, як відбиток пальця, райдужна оболонка ока, голос, почерк, набір інформації клавіатурою.

1.2. Застосування біометричних систем в торгівлі

На теперішній час застосування біометричних систем в торгівлі поки що не розвинена, але на за межами України застосування БСКД набуло досить широкого розповсюдження. В першу чергу це відноситься до розпізнавання відбитка пальця і форми руки. Впровадження біометрії в торгівлі здійснюється в наступному векторі:

- в торгівельних центрах, ресторанах та кафе біометричні ідентифікатори використовують як засіб ідентифікації покупця та проведення транзакцій;
- в автоматичних системах проведення розрахунків та в банкоматах застосовуються БСКД, як засіб ідентифікації людини, які заміняють магнітні картки;
- при проведення операцій в електронній комерції біометричні ідентифікатори використовують як засіб дистанційної ідентифікації через Інтернет, а в синтезі із

засобами криптографії забезпечують електронним транзакціям дуже високу надійність інформаційного захисту.

1.3. Біометричні системи контроля доступом на об`єкті інформаційної діяльності

Системи контролю доступу на базі технологій біометрії базі біометричних за своїм принципом мають аналогічні рішенням, що і для входу в корпоративну мережу. Цифрові БШ відвідувача записуються в електронну пам'ять, яка вмонтована в замок дверей або турнікета. Особа при кожному вході або виході проходить процедуру біометричної ідентифікації для відкриття дверей. Це здійснюється завдяки або скануванню палиця, сітківку ока або вимовити кодове слово або речення.

В БСКД реалізуються вищевикладені технології розпізнавання: відбиток пальця, обличчя, форма руки, райдужна оболонка ока, голос.

В інфраструктурі критичного значення на основі таких систем розпізнавання для більш надійного захисту створюється спеціальна підсистема обліку робочого часу. При створенні таких систем використовуються біометричні замки з мережевою архітектурою або звичайні системи біометричного сканування. Крім того, створюються системи цивільної ідентифікації та автоматизовані дактилоскопічні ідентифікаційні системи (АДІС). Системами цивільної ідентифікації заведено називати загальнодержавні біометричні системи ідентифікації особистості під час видачі документів, перетину кордонів, розподілу допомоги та дотацій. Наразі такі системи набули найширшого поширення, оскільки їх почали використовувати під час в'їзду в деякі країни для перевірки особи тих, хто в'їжджає [9]. Насамперед це стосується США, найближчим часом схожу систему планує запровадити Європейський Союз і Росія. Країни-учасниці Шенгенської угоди вже домовилися змінити формат в'їзних віз, в які тепер будуть записуватися біометричні дані. Аналогічні програми розпочалися в багатьох країнах Азії. Необхідно розрізняти системи цивільної ідентифікації (за прийнятою в

зарубіжних країнах термінологією, системи Civil ID) і криміналістичні автоматизовані дактилоскопічні ідентифікаційні системи - АДІС (AFIS). Параметри цих систем принципово різняться.
На відміну від криміналістичних додатків, які вимагають отримання відбитків усіх десяти, цивільні додатки вимагають зображень відбитків двох пальців. Одна з найважливіших відмінностей цих систем - повністю автоматичний пошук і прийняття рішення в Civil ID-системах і необхідність роботи висококваліфікованого експерта-криміналіста в криміналістичних АДІС [10].

1.4. Комплексні біометричні системи контролю доступом

Це системи, що поєднують у собі системи перших трьох класів. Наприклад, спільне використання СКУД і комп'ютерної безпеки з єдиним для обох систем сервером автентифікації, тобто співробітники компанії реєструються в адміністратора системи лише один раз, далі йому автоматично призначаються всі необхідні привілеї як на вхід у приміщення, так і на роботу в корпоративній мережі та її ресурси.
Крім цих основних секторів застосування, нині починається активне використання біометрії і в інших галузях:
- гральний бізнес, казино. Біометрія використовується за двома напрямками: перевірка всіх, хто перебуває за "чорними списками" (аналог масової ідентифікації за обличчями, застосовуваної в аеропортах), а також як система ідентифікації та платіжний засіб постійних клієнтів;
- ідентифікація в мобільних пристроях, таких, як мобільні телефони, КПК тощо;
- у транспорті як платіжний засіб;
- електронні системи голосування (використовуються замість карток);
- медицина. Біометрія застосовується для ідентифікації медичних працівників при отриманні доступу до закритих даних і для електронного підпису записів в історії хвороби.
Загальноприйнятих критеріїв, які можна було б використовувати під час побудови біометричних систем у масштабах будь-якого підприємства, немає.

Тому в цій статті буде надано тільки рекомендації, отримані з досвіду впровадження біометричних систем.

Отже, перше, з чим необхідно визначитися, - це безпосередньо технологія розпізнавання, яку належить використовувати. Для цього потрібно керуватися поєднанням двох критеріїв.

Точність технології. Якісними показниками функціонування алгоритмів біометричної ідентифікації слугують значення: FAR (False Acceptance Rate) - вірогідність помилкового розпізнавання, тобто вірогідність того, що система сплутає два індивідууми, визнавши "чужого" "своїм"; FRR (False Rejection Rate) - вірогідність помилкового нерозпізнавання, тобто того, що система не розпізнає знайомого їй суб'єкта (вірогідність непропуску "свого").

На практиці зменшення FAR завжди призводить до зменшення чутливості методу або, що еквівалентно, до збільшення FRR [4]. Ідеальні характеристики системи - це рознесені показники помилки та відмови ідентифікації, коли водночас при великій надійності ідентифікації (помилка 0,0001%) досягається відмова ідентифікації всього частки відсотка.

Показник помилки ідентифікації визначається обраним підходом, якістю реалізації та налаштування алгоритмів ідентифікації. Для кожного конкретного виробника та його обладнання FAR і FRR вказуються точно. Зазначимо, що показники змінюються залежно від виробника і похибки тестування, але важливо те, що три методи розпізнавання - за відбитком пальця, за тривимірним зображенням обличчя, за райдужною оболонкою ока - мають порівнянну точність. При цьому розпізнавання за двовимірним зображенням обличчя поступається перерахованим методам за точністю на порядок, так само як і інші біометричні методи (розпізнавання за геометрією руки, за голосом тощо).

Зручність використання. Потрібно передбачити, щоб співробітникам компанії було зручно проходити біометричні процедури ідентифікації в рамках розв'язуваного завдання.

Після вибору технології належить вибрати виробника обладнання, яке задовольняло б вашим вимогам, і, що не менш важливо, представника компанії-виробника в країні.

Стійкість до навколишнього середовища. Експлуатаційні якості різних біометричних методів сильно залежать від навколишніх умов і можуть втрачати стабільність при зміні цих умов. Так, сканери відбитків пальців постійно забруднюються і якість роботи їх падає, двовимірні методи розпізнавання обличчя сильно залежать від зовнішньої освітленості тощо.

Стійкість до підробки. Біометрична система має бути стійкою до підробки (несанкціонованого доступу). Систему розпізнавання за двовимірним (2D) зображенням обличчя можна легко "обдурити", пред'явивши фотографію з числа знайомих системі. Для отримання несанкціонованого доступу за відбитком пальця буває достатньо нанести графітову пудру і натиснути через тонку плівку.

Вартість системи. Всупереч думці про дорожнечу впровадження біометричних систем, за останні п'ять років їхня ціна в середньому знизилася в 2 - 3 рази. При оцінці системи потрібно враховувати, що її вартість складається з багатьох складових. Наприклад, для мережевого захисту - це зчитувальні пристрої, сервер автентифікації та призначені для користувача ліцензії до нього, послуги з впровадження та супроводу і, якщо потрібно, окремо розробка модуля інтеграції з будь-яким спеціальним корпоративним програмним забезпеченням.

Швидкість роботи біометричної системи. Із цим критерієм ситуація очевидна: що швидше користувач розпізнається в системі, то краще. Потрібно зазначити, що швидкість залежить від вибору методу розпізнавання: верифікації або ідентифікації, оскільки очевидно, що порівняння шаблонів "один до одного" набагато швидше за порівняння одного шаблону з усією базою зареєстрованих.

Крім цього, існує ще кілька критеріїв оцінювання біометричних систем, але вони мають приватний характер для кожної технології.

Висновки до розділу 1

Застосування біометричних технологій поступово переходить зі сфери альтернативи іншим системам ідентифікації (картковим, парольним тощо) у сфери, в яких розгортається конкуренція тільки між методами біометричної ідентифікації.

Одна з причин популярності біометричних систем зводиться до об'єктивної потреби замовників організувати сучасну, грамотно побудовану систему безпеки у себе на підприємстві, в офісі компанії або в приватному будинку. Більшість прогнозів зводиться до того, що впровадження біометричних систем безпеки на вітчизняний ринок набуде в недалекому майбутньому лавинного характеру. Інтенсивний розвиток мультимедійних, цифрових технологій і, як наслідок, їхнє здешевлення дають змогу не тільки розробити принципово нові підходи в проблемі ідентифікації особистості, а й впровадити їх у широке повсюдне використання. Наразі вдосконалення біометричних технологій відбувається прискореними темпами. Насамперед це призводить до того, що підвищується надійність і знижується вартість цих технологій.

РОЗДІЛ 2 ДОСЛІДЖЕННЯ СИСТЕМИ ІДЕНТИФІКАЦІЇ ТА ПІДТВЕРДЖЕННЯ ПРАВА ДОСТУПУ НА БАЗІ ДИНАМІКИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

2.1. Загальні параметри біометричної аутентифікації

Біометричні методи ґрунтуються на визначенні особистості людини за притаманними тільки їй ознаками. Основна перевага біометричних методів полягає в тому, що такі ознаки неможливо вкрасти або передати іншій людині. Біометричні методи поділяють на фізіологічні, поведінкові та комбіновані. Детальну класифікацію представлено на малюнку 1. Поведінкові характеристики складніше розпізнати з високою точністю, але водночас складніше й підробити.

Сучасна біометрична аутентифікація ґрунтується на двох методах :
- статичний метод. Цей метод аутентифікації ґрунтується на розпізнаванні фізичних параметрів людини, якими вона володіє протягом усього життя: відбитки пальців, відмітні характеристики райдужної оболонки ока, малюнок очної сітківки, термограма, геометрія обличчя, геометрія кисті руки і навіть фрагмент генетичного коду);

динамічний метод. Заснований на аналізі особливостей поведінки користувача, які проявляються в процесі виконання повсякденних дій (підпис, клавіатурний почерк, голос тощо).

Біометрична аутентифікація не визначає користувача з абсолютною точністю. У зв'язку з тим, що деякі реалізації стійких криптосистем, наприклад, систем аутентифікації, що ґрунтуються на постквантових перетвореннях, перебувають на етапі теоретичного обґрунтування і прототипного опрацювання , біометричні характеристики користувачів займатимуть основну роль у процесі підтвердження особи. При цьому існує ймовірність допуску помилок першого

(відмова в доступі) і другого роду (помилковий доступ) .

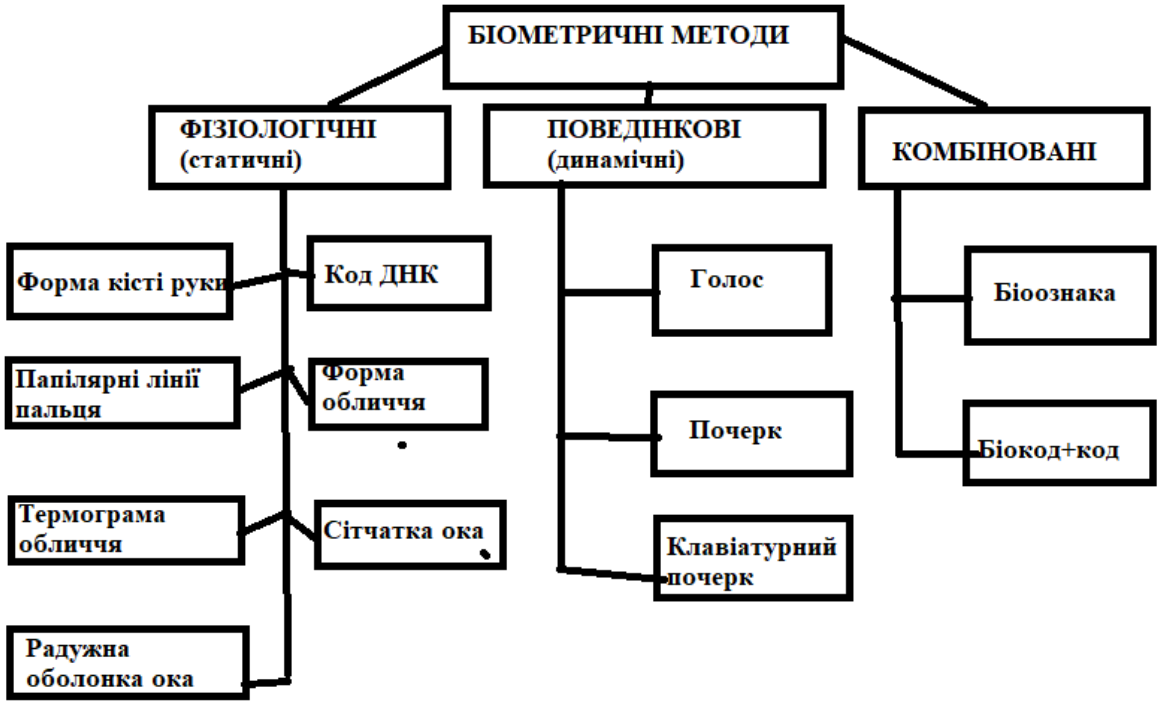

Рисунок 2.1. Класифікація біометричних методів

Ефективність систем біометричної аутентифікації заведено оцінювати за двома характеристиками:

- відмова в доступі – це помилка першого роду (*FRR*) , яка чисельно дорівнює ймовірності того, що система не розпізнає користувача, який було зареєстровано;

- помилковий доступ – це помилка другого роду (*FAA*) , яка чисельно дорівнює імовірності того, що в систему отримав помилково доступ користувач, який не має права доступу.

Процес отримання оціночних даних для конкретної людини передбачає одноразове, періодичне або безперервне отримання даних про її дії при введенні контрольної фрази або набору даних, характерних для її постійної діяльності. Основне місце на ринку біометричного захисту завжди посідав статичний метод, динамічна автентифікація і комбіновані системи захисту інформації займали всього лише 20 % ринку.

Слід зазначити, що класична біометрія, яка використовує статичні методи, має низку проблем [13]:

- ідентифікація користувача тільки на певному етапі взаємодії: вхід, підтвердження транзакції тощо;
- механізми засновані на аналізі персональних даних користувача;
- вимагають впровадження додаткових технічних пристроїв;
- кожен додатковий фактор ідентифікації зменшує успішність транзакції на 15-20 %;
- засновані на зовнішніх (видимих) фізіологічних характеристиках.

Переваги динамічних методів біометричної аутентифікації над статичними очевидні:

- безперервна перевірка автентичності для виявлення несанкціонованого доступу під час усього сеансу;
- не вимагає зміни користувацької поведінки (прихований метод ідентифікації);
- працює на всіх платформах і пристроях без додаткового обладнання.

Слід зазначити, що останніми роками, спостерігається різка тенденція розвитку динамічних методів захисту. Порівняння наявних методів представлено в таблиці 2.1.

Таблиця 2.1. Порівняння надійності методів біометричної аутентифікації

Метод біометричної аутентифікації	FAR - коефіцієнт хибного допуску	FRR-коефіцієнт хибної відмови	Фальсифікація	Комфорт користувача	Вартість
Відбиток пальця	0,001%	0,6 %	Можлива	Середній	Низька
Розпізнавання обличчя 2D	0,1%	2,5 %	Можлива	Середній	Середня
Розпізнавання обличчя 3D	0,0005%	0,1 %	Проблематична	Середній, нижче середнього	Висока
Радужна оболонка ока	0,00001%	0,016 %	Неможлива	Високий	Висока
Сітчатка ока	0,0001%	0,4 %	Неможлива	Низький	Висока
Малюнок вен долоні	0,0008%	0,01 %	Неможлива	Середній	Середня
Голос	0,75%	0,75 %	Можлива	Середній	Низька
Клавіатурний почерк	0.01%	0,01 %	Можлива	Високий	Низька

Ґрунтуючись на наведених даних, можна зробити висновок про те, що застосування динамічних методів біометричної аутентифікації, а саме клавіатурного почерку, є затребуваним. Однак за наявного рівня інтегрованості програмного забезпечення таке застосування можливе лише як допоміжний фактор автентифікації для мобільних пристроїв. Звернемо увагу, що виконуються три основні вимоги до аутентифікації:

- знання якоїсь інформації, відомої тільки користувачеві, наприклад, пароль або контрольна фраза;
- володіння якимось пристроєм, який є тільки у користувача, - телефон;
- унікальності, притаманної користувачеві, яка однозначно ідентифікує особу, - біометричні дані.

2.2. Характеристика статичних алгоритмів в динаміці аутентифікації та ідентифікації

Масштабне дослідження біометричних методів, проведене Національним бюро стандартів, дало змогу зробити граничні оцінки: вірогідність правильного розпізнавання користувачів з усталеними навичками роботи з клавіатурою

становила 98 %, що цілком достатньо для того, щоб говорити про успішну практичну придатність подібних систем.

Аналіз клавіатурного почерку має свої переваги і недоліки, так само, як і будь-які біометричні методи.

Перевагами біометричних систем є:

- для біометричної ідентифікації достатньо фізичних параметрів людини і не потрібні ніякі файли, які піддаються копіюванню та паролі, які піддаються зламу;
- унікальні характеристики особистості зручні тим, що їх важко, а іноді не можливо підробити;
- на відміну від паперових ідентифікаторів таких як паспорт, водійські права, страхове свідоцтво, індивідуальний податковий номер, біометричні характеристики не можуть бути забуті або втрачені, їх завжди легко представити.

Недоліками біометричних систем є:

- відсутність довіри від користувачів, так як багата їх кількість поки що не готові до переходу на такої форми ідентифікації;
- наявність ймовірності в точності та достовірності, так як жоден з біометричних підходів не дає сто відсоткову гарантію достовірності;
- висока вартість БСКД, так як витрати, які необхідно здійснити для реалізації та підтримки БСКД, значно вищі за криптографічний захист, а також завжди існує загроза конфіденційності.

При здійснені аналізу клавіатурного почерку виникає певна кількість складнощів, а саме:

- розподіл параметрів клавіатурного почерку залежить від психофізичного стану користувача;
- розподіл параметрів клавіатурного почерку залежить від самої клавіатури, яку користувач використовує. Дослідження клавіатурного почерку користувача з використанням різних клавіатур показало, що розмах імовірності аутентифікації становить 0,5.

- для дослідження клавіатурного почерку необхідна вибірка дуже великого об`єму, так як не існує бази даних зі зразками.

В таблиці 2.1 здійснено порівняння статистичних алгоритмів за деякими критеріями оцінки, характерними для функціональних характеристик людини.

Таблиця 2.1. Порівняння статистичних алгоритмів

Параметри	Тип тестування	Метод розпізнавання	Кількість користувачів	Кількість примірників	FAR	FRR	ERR
Час утримання	Статистичний(Statistical)	Статичний	64	310	0,47	1,32	2,2
	Статистичний	Динамічний	25	1620	-	-	-
	Статистичні класифікатори (Statistical classifires)	Статичний	100	5000	1,4	1,4	1,41
	Гіпотези (Hypothesis)	Статичний	16	3200	4,5	5,5	-
	Манхетенська відстань	Статичний	51	20400	-	-	9,6
	Кутові затримки	Статичний	15	-	3,6	4,7	-
Інтервали між натисканнями	Статистичний	Статичний	44	220	0	2,3	-
	Міра відстані/міра Хемінга	Динамічний	31	-	8,33	2,6	-
	Відносна та абсолютна дистанція	Статичний, динамічний	205	765	0,005	5	0,5
	Ступінь хаосу	Статичний	18	810	0	0,55	-
Час утримання і інтервали між натискання	Статистичний	Динамічний	21	-	9	5	-

Виходячи з отриманих результатів, автентифікацію на основі аналізу клавіатурного почерку можна вважати ефективною, також слід зазначити, що наразі немає застосунку для аналізу клавіатурного почерку для мобільних пристроїв, що підтверджує актуальність подальшого дослідження динамічних методів біометричної автентифікації та подальшої реалізації клієнтського застосунку для мобільних пристроїв.

Крім аналізу клавіатурного почерку було запропоновано спосіб ідентифікації та аутентифікації, в основі якого лежить метод розпізнавання підпису суб'єкта доступу.

Цей підхід має наступні три кроки:

1) отримання геометричних даних підпису з відповідного пристрою або сканеру;
2) перехід в цифрову форму та передача даних в комп`ютерах за допомогою стандартних інтерфейсів;
3) подальший аналіз за допомогою існуючого спеціального програмного забезпечення.

При застосуванні такого методу ідентифікації/автентифікації основними параметрами є кривизна, швидкість, час, натиск і топологічні інваріанти особистості, а саме зв`язність, кількість точок самоперетину.

Вхідна форма формується за рахунок введення підпису в спеціальний планшет, який носить назву джигітайзеру. Після цього здійснюється цифрове перетворення наступних параметрів: координати кінця пера, звуковий тиск, розташування пальців руки. Після цього значення параметрів відображаються в текстовому файлі, структура якого складається з трьох стовпчиків x, y, t, де x, y - координати пера, t - час, протягом якого відбувається набирання тексту на клавіатурі.

Однак, враховуючи високу чутливість джигітайзеру до самої експлуатації його та впливу зовнішніх чинників та достатньо низька поширеність подібного роду пристроїв, відсутня можливість вважати такий підхід в подальшому масово використовувати для проведення ідентифікації та аутентифікації користувачів.

Не зважаючи на вказаний недолік саме цей підхід можна адаптувати для застосування його в мобільних пристроях, в яких присутній сенсорний екран. Даний підхід дає можливість якісно проводити аутентифікацію та ідентифікацію користувачів.

2.3. Реалізація динаміки біометричної аутентифікації для мобільних засобів на основі статистичних алгоритмів

На рисунку 2.2 представлено архітектуру програмного додатку за допомогою якого здійснюється отримання інформації про клавіатурні натискання українською та англійською мовами в неперервному часі та ідентифікації санкціонованих або несанкціонованих дій користувача.

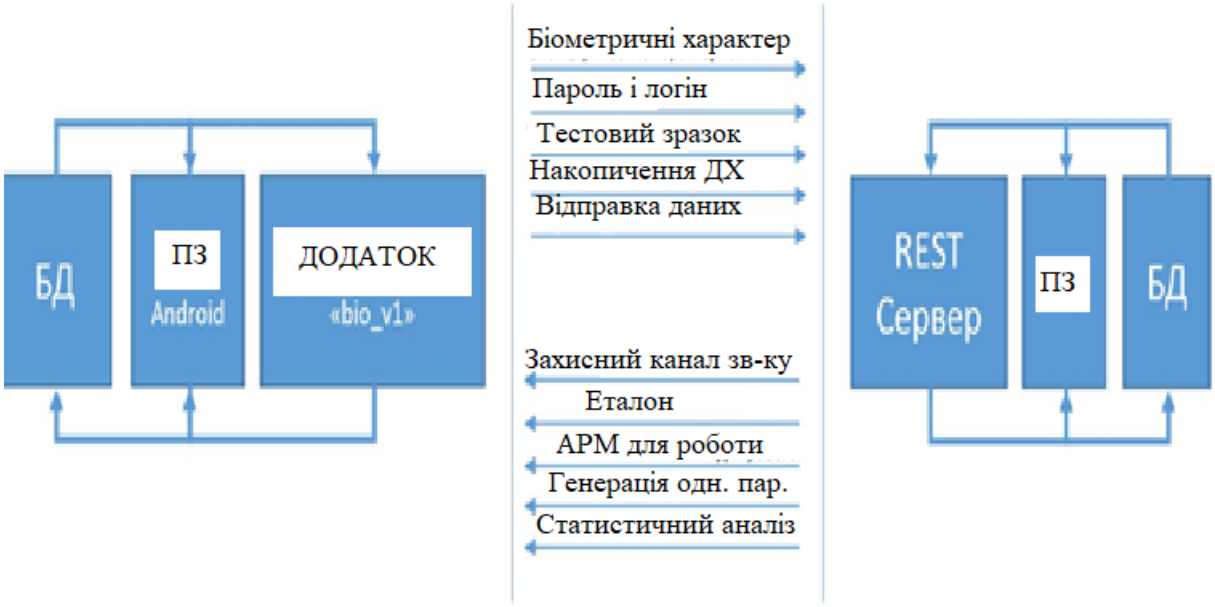

Рисунок 2.2. Архітектура системи аутентифікації та ідентифікації користувачів

Розглянемо, систему реалізації на базі клієнт-серверної архітектури. За допомогою додатка, який знаходиться на стороні клієнта та дозволяє зчитувати біометричні дані, час утримання клавіш. Для тесту, використовували введений пароль та динамічні характеристики, а також ім'я профілю аутентифікації. Тобто, спочатку користувач проходить реєстрацію в застосунку, сформувавши ім'я профілю. Далі, створюється тестовий зразок, протягом всього часу взаємодії із клавіатурою пристрій зчитує час утримання клавіш. Шляхом математичних обчислень сформується еталонний зразок клавіатурного почерку користувача. Бази даних з еталонами аутентифікаційних даних знаходяться на сервері, також на сервері є можливість реалізувати алгоритми порівняння тестових зразків і еталонів. Результатом порівняння є відповідь клієнта від сервера. Для того, щоб

захиститися від атаки «людина по середині» між сервером та клієнтом використовують захищений канал зв’язку.

Основні етапи роботи додатка наведено на рисунку 2.3.

Рисунок 2.3. Етапи реалізації програмного додатку

Описані вище етапи збору характеристик, включають в себе отримання значень параметрів.

Створений клавіатурний шаблон складається із аналізу отримання значень параметрів, основу з яких складає час утримання клавіш, та формується еталонний шаблон, в подальшому з ним буде порівнюватися значення, які отримані під час спроби авторизуватися в системі. Для того, щоб підтримувати БД клавіатурних профілів потрібно оновлювати еталони, що зберігаються в базі даних. Що таке ідентифікація користувача? Ідентифікація користувача - підтвердження особи користувача отримання дозволу/відмови в доступі.

За клавіатурним почерком існує 2 методи реалізації аутентифікації користувача:

- за відомою парольною фразою;
- протягом усього часу взаємодії користувача з пристроєм безперервно відслідковувати клавіатурну активність.

Розглянемо, перший метод. За парольною фразою, потрібно виконати наступні кроки:

- заздалегідь визначеним текстом - «паролем», створена еталона;

- далі відбувається розпізнавання користувача шляхом порівняння отриманих параметрів, які отримуються під час введення парольної фрази, коли відбувалася аутентифікація.

Також, даний метод можна використати на етапі авторизації, але далі використовувати його буде складніше.

Під значенням безперервного моніторингу, потрібно врахувати, що його можна використати, як під час аутентифікації, так і після її проходження:

- відслідковується уся активність користувача його клавіатури. Даний ресурс є ресурсномісткий, бо в базі потрібне зберігання тимчасових міток усіх символів, які колись вводив користувач;
- підхід, який заснований на основі частих біаграм. Зазначимо, що даний метод є менш ресурсномісткий, бо використовує лише пари букв, які найчастіше зустрічаються.

Було розроблено додаток, який оснований на методі розпізнання за парольною фразою для операційної системи Android (рис. 2.4).

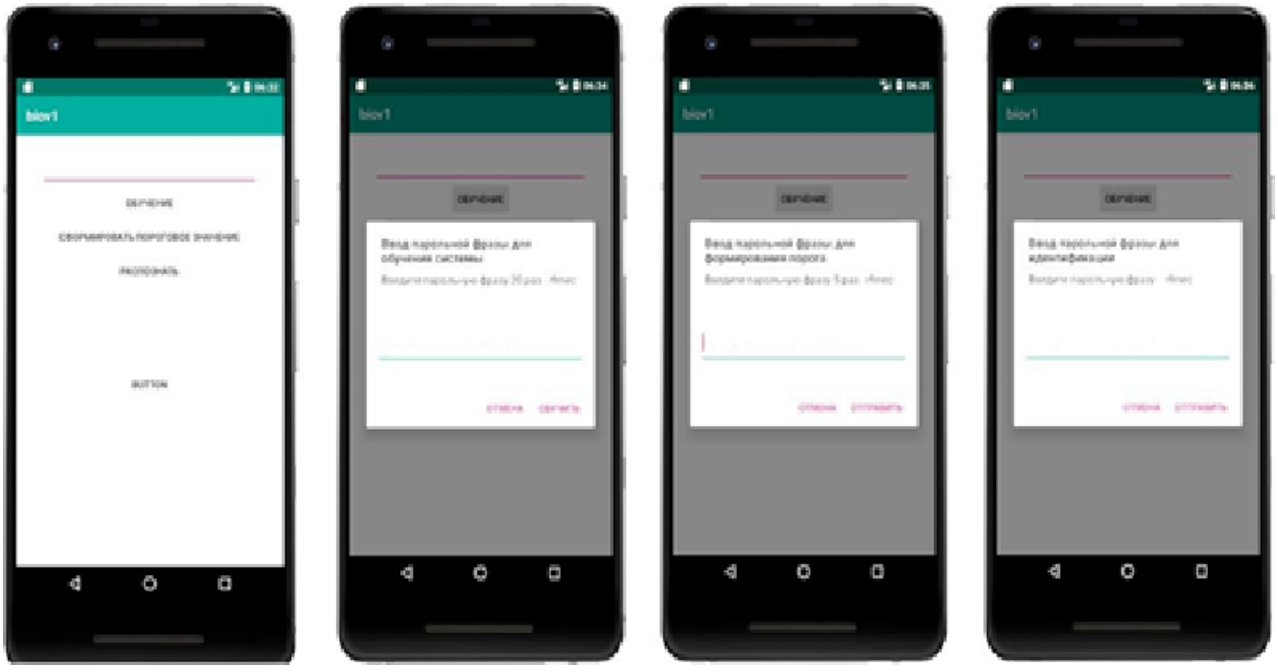

Рисунок 2.4. Етапи роботи додатку

Було реалізовано, три етапи розпізнання клавіатурного почерку:

- навчання;
- формування порогового значення;
- розпізнання.

Коли відбувається навчання користувач вводить парольну фразу 20 разів, та надсилає дані на сервер. Далі, відбувається опрацювання отриманих значень та формується еталон клавіатурного почерку. Еталон створюється процесом вирахування середнього значення даного параметру, як час утримання клавіш. Далі, під час формування порогового значення користувач вводить парольне повідомлення п’ять разів та відправляє дані на сервер.

На цьому етапі на сервері формується відстань Хемінга, тобто формується значення допустимої кількості розбіжностей часових параметрів $A1$ з еталоном $A2$, математично це представлено наступним чином:

$$H = A1 \oplus A2 . \tag{2.1}$$

Для ідентифікації користувача за клавіатурним почерком аналізуються значення двовимірного вектору:

$$P = ((t,r),(t,i)), \tag{2.2}$$

де (t,r) - час утримання; (t,i) - тривалість паузи.

Коли відбувається розпізнання, користувач на екрані спостерігатиме відповідь від сервера, буде або позитивний результат, або негативний, тобто означає «свій» або «чужий», що користувач вводив парольну фразу на етапі розпізнання.

Провели тестування за участю кількох користувачів. Учасниками були два студенти, різної статі та віком 18-23 роки. Під час навчання, було сформована еталон клавіатурного почерку, представлено в таблиці 2.2.

Таблиця 2.2. Початок та процес тестування додатку *bio_v1*

Кількість ітерацій введення слова або речення на етапі навчання	Кількість символів, які було відправлено на сервер для навчання	Значення відстані Хемінга	Кількість ітерацій розпізнавання	FRR	FAR
20	120	User1: 46,6	45	0,44	0
		User2: 46,6		0,53	0,04
40	240	User1: 50	45	0,73	0,044
		User2: 26,66		0,08	0,77
60	360	User1: 52,5	45	0,6	0,42
		User2: 46,6		0,28	0,64

Проаналізувавши таблицю 2.2, було досліджено:

- для першого і другого користувача відповідно, великий відсоток помилки першого роду для першого тестування (44 % і 53 %);
- для другого тестування у першого користувача великий відсоток помилки (73 %), для другого користувача великий відсоток помилки другого роду (77 %);
- для третього тестування у першого користувача великий відсоток помилки першого роду (60 %), для другого 28 %, великий відсоток помилки другого роду у першого користувача 42 %, у другого користувача - 64 %.

Причини, які слідують отриманим результатам:

- користувачі відчували дискомфорт;
- індивідуальний психо-фізіологічний стан на момент проведення тестування;
- повторні однотипні дії протягом невеликого проміжку часу.

Саме на даному етапі відбувається створення еталонного шаблону за одним параметром, тобто за час утримання клавіш та за парольною фразою, яка відома легітимному користувачеві, та і зловмиснику. Навели отримані результати в таблиці 2.3.

Таблиця 2.3. Результати тестування додатку *bio_v1*

Кількість ітерацій введення парольного слова на етапі навчання	Користувач	Значення часового параметру для символу "r",в мс	Значення часового параметру для символу "f", в мс	Значення часового параметру для символу "n", в мс	Значення часового параметру для символу "e", в мс	Значення часового параметру для символу "c", в мс
	User1	80,5	75	97	79	60
20	User2	89	94,5	96,4	87,5	86,5
40	User1	86	96	84	87,5	88,5
	User2	102	101	88,5	86	78
60	User1	85	83,5	91,5	92	69,5
	User2	95	80,5	81,5	90,5	103,5

Із таблиці 2.3 слідують наступні висновки:

- ніяке значення параметра еталонного шаблону клавіатурного почерку в користувача не збіглося, тобто в результаті, кожна людина має індивідуальний, унікальний клавіатурний почерк;
- під час першого тестування найменша відмінність при утриманні клавіші "n" (0,6мс), найбільша - для клавіші "f" (19,5мс);
- під час другого тестування найменша відмінність спостерігається для утримання клавіші "e" (1,5мс), найбільша - для клавіші "r" (16мс);
- під час третього тестування найменша відмінність спостерігається для утримання клавіші "e" (1,5мс), найбільша відмінність - для утримання клавіші "c" (34мс).

Отже, виконавши тестування, можна зробити висновок, що під час помилки першого і другого роду помилка, зумовлена малою кількістю отримання інформації на сервері, щоб сформувати еталонний клавіатурний почерк, а

також одного параметру, щоб сформувати еталонний клавіатурний почерк недостатньо. Тестування проводилося для трьох експериментів. Некомфортним для користувача є введення інформації відомою фрази протягом певного проміжку часу. Тому, подальші тестування потрібно проводити з перервами протягом тривалого часу, для того, щоб якісно простежити зміну клавіатурного почерку протягом одного періоду часу. Введення незмінної фрази призводить до спотворення результатів, тому актуально проводити тестування з введенням вільного тексту.

Висновки до розділу 2

Отже, якщо поєднувати клавіатурний почерк із іншими методами, то це підвищить надійність системи захисту мобільних пристроїв. Це не вимагає додаткових ресурсів чи продуктивних потужностей, а лише збільшить кількість дій для користувача. Актуальним є питання про трудові витрати, але кожен користувач вибере варіант із додатковими часовими витратами на догоду своїй безпеці.

Але, актуальна проблема оцінки стійкості та індивідуальності біометричних характеристик. Даний підхід дасть змогу визначити осіб, в кого клавіатурний почерк надійно їх ідентифікує. Потрібно подальше проводити досліджувати, яка підвищить точність результатів, модернізує графічний інтерфейс, оптимізує швидкість роботи.

Під час дослідження, виявлено наступні переваги:

- не має потреби купити жодне додаткове обладнання;
- від користувача не потрібно ніяких додаткових навичок і дій;
- є можливість прихованої аутентифікації, тобто користувач може бути в не курсі , що ввімкнена додаткова перевірка.

Результат показав, що ефективне розпізнання користувача на основі динамічних методів біометричної автентифікації досягає 92,14 %, що говорить про високий

потенціал для того, щоб застосовувати даний метод в межах розроблення систем доступу до мобільних пристроїв.

РОЗДІЛ 3 РОЗВИНЕННЯ БІОМЕТРІЇ В СИСТЕМИ КОНТРОЛЯ З ОБМЕЖЕНИМ ДОСТУПОМ НА ОБ`ЄКТІ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1. Порівняльна характеристика видів систем конторолю доступом

Фізичні носії часто використовують ідентифікатори, які мають важливий недолік, а саме розкрадання або підробка ідентифікатора. Саме, це знижує рівень безпеки об’єкта на якому використовується даний метод. Для того, щоб мінімізувати ризики, потрібно використовувати біометричні зчитувачі, які призначені для ідентифікації користувача, які за основу використовують унікальні фізичні особливості. Тобто, якщо використовувати дані можливість, то знизиться ризик несанкціонованого доступу до інформації. Типи фізіологічних ідентифікаторів, які основані з них:

- Відбиток пальця
- Райдужна оболонка ока
- Сітківка ока
- Малюнок вен
- Розпізнавання обличчя 3D

Біометричні системи можуть складатися як з апаратного, так і з програмного забезпечення. Біометричний прилад ідентифікації збирає, зчитує і порівнює біометричні дані. Біометричні дані - це комплекс даних, з яких потрібно витягти унікальні дані для користувача. Впроваджене програмне забезпечення всередині біометричної системи включає в себе "біометричний двигун", який обробляє зібрані біометричні дані. Програма зазвичай працює в комплексі з обладнанням для управління процесом збору біометричних даних,

обладнанням вилучення даних і проведення порівняння, включно з зіставленням даних.

В БСКД існують недоліки, притаманні тільки даним типам систем. Біосистеми не передбачають видачу тимчасових перепусток . Наразі, на відміну від фізичних ідентифікаторів, є ймовірність не розпізнати біометричні параметри, це пов'язано передусім із наявністю ймовірнісних і динамічних характеристик, наприклад, запотівання та висихання долонь. Нестабільність падає залежно від виду зчитувача. Головними, для оцінки будь-якої біометричної системи, є два параметри. Першим таким параметром є *FAR* - коефіцієнт помилкового пропуску, тобто відсоток виникнення ситуацій, коли система дозволяє доступ користувачеві, незареєстрованому в системі. Другим таким параметром є *FRR* - коефіцієнт помилкової відмови, тобто відмова в доступі справжньому користувачеві системи.

Обидві характеристики отримують розрахунковим шляхом на основі методів математичної статистики. Що нижчі ці показники, то точніше розпізнавання об'єкту.

Для найпоширеніших на сьогоднішній день методів біометричної ідентифікації середні значення *FAR* та *FRR* мають наступне представлення, як показано в таблиці 3.1.

Таблиця 3.1. Математичне сподівання значень *FAR* та *FRR*

БСКД ВИКОРИСТОВУЄ	**FAR**	**FRR**
Відбиток пальців	0,001%	0,6%
Розпізнавання обличчя 3D	0,0005%	0,1%
Радужна оболонка ока	0,00001%	0,016%
Сітчатка ока	0,0001%	0,4%
Малюнок він	0,0008%	0,01%

Саме, біометрія зменшить ймовірність несанкціонованого доступу традиційних систем доступу. Відсутність передачі ідентифікаторів іншому користувачеві ефективно підвищує рівень безпеки. Біометричний ідентифікатор не можна забути або загубити, що підвищує захист, актуально для об’єктів, які мають постійну плинність користувачів.

Актуально, на даний момент технології розпізнавання обличчя, відбитків пальців, райдужної оболонки ока. Лідирують об’єкти, які найчастіше застосовують дану систему, це державні проекти та банківський сектор.

У даній системі, лідирує Північна Америка, яка має високий рівень застосунку. Також, активно зростає застосування в Китаї та Японії. У приватних об’єктах, є також багато переваг:

- підвищити загальну захищеність ІС, зможить відсутність смарт-карт або токенів;

- унікальні біометричні дані параметри не дасть змогу отримати дані зловмиснику;
- застосування зменшить витрати на перепустки, а також на обладнання, щоб їх запрограмувати.

Дана система допоможуть не тільки в організації БСКД, а й у створенні систем обліку робочого часу (СОРЧ), бо підробити унікальну ознаку неможливо, що підтримує коректний облік відпрацьованого співробітників часу.

3.2. Біометричні системи контролю доступом за відбитками пальців

3.2.1. Відбитки пальців як ідентифікатор особистості

Саме, ідентифікація користувача за відбитком пальця є актуальним та сучасним. Дана технологія є точна та легкою у використанні. Користувачами технології є різноманітні організації, а саме в США, ФСБ, Секретна служба та інші.

Перевагою, як зазначалося раніше є простота та надійність. Статичні моделі відбитків пальців навели у статті [12]. Обдурити систему важко, майже не можливо, наприклад від рубаним пальцем, бо вимірюється фізичні параметри шкіри, температури та пульс [13].

Розпізнати відбитки пальців, можна за алгоритмом, який поділяється на два класи [14]: розпізнати за окремими деталями та за рельєфом усієї поверхні пальця. Коли використовується перший випадок, то аналізується ділянка, яка унікальна конкретному відбитку та визначає їхнє взаємне розташування. А в другому відбувається обробка зображення всього відбитку. Якщо дані способи комбінувати, рівень захисту підвищиться. Зареєструвати відбиток пальця займає небагато часу. CCD-камера виконує знімок відбитка пальця. Далі, знімок перетвориться на унікальний шаблон відбитка. Потім, він шифрується та записується в базу даних для аутентифікації користувача.

Використання для ідентифікації відбитка пальця, є найзручнішим із запропонованих ідентифікації біометричним способом. Якість розпізнавання об’єкта залежить від ряд показників, а саме від стану поверхні пальця, його положення відносно елемента, що сканується, чистоти пальця і вікна сканера, а також від низки інших умов.

За допомогою, папілярних візерунків формується сукупністю виступів і западин на шкірі. Вони відрізняються і у близнюків. На відбитках, можна визначити два типи ознак, а саме глобальні та локальні. Глобальні можна побачити неозброєним оком.:

- візерунок типу "петля" (ліва, права, центральна, подвійна);
- візерунок типу "дельта", або "дуга" (проста і гостра), - зона, де виступ розгалужується на три лінії, які потім сходяться в одній точці;
- візерунок типу "спіраль" (центральна і змішана).

В стандартах "Інформаційні технології. Формати обміну біометричними даними. Дані зображення відбитка" [15] детально описано локальні ознаки або мінуції. За допомогою, даного стандарту можна визначити:

- Папілярні гребені - це гребені шкіри долонної поверхні кистей і пальців рук, що безпосередньо контактують із поверхнею під час зіткнення. Унікальний рельєф, утворений папілярними гребенями на пальці, формує відбитки пальців.

Далі, зображено, темні смуги гребені, а западини – світлими.

Рисунок 3.1. Приклади основних типів глобальних ознак відбитків пальців: а) дуга; б) петля; в) завиток

Контрольні точки (мінуції) - точки порушення безперервності гребенів, які можуть мати вигляд закінчення, поділу гребенів або мати складнішу складову форму. ДСТУ [15] визначає два основні типи мінуцій, як це представлено на рисунку 3.2:

- біфуркація (роздвоєння) гребеня - точка, що відповідає ділянці, у якій відбиток гребеня розділяється на два гребеня;

- закінчення гребеня - точка, що відповідає ділянці, в якій відбиток гребеня закінчується або починається.

Отже, ідентифікація за відбитком пальців – найпоширеніша біометрична технологія. Її застосування дуже високе.

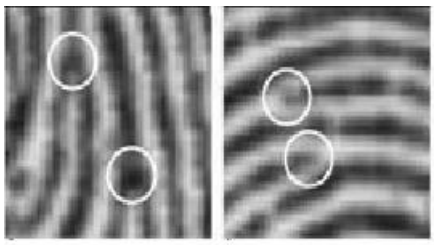

Рисунок 3.2. Приклади закінчення і біфуркації (роздвоєння) гребеня

Зазначимо, що сканери надійні та доступні за ціною. Використовують три основні технології: оптична, напівпровідникова та ультразвукова. Найкращі сканери *BioLink U – Match*3.5. Відносяться до сканерів першого типу. Застосовуються, співробітниками комерційних компаній та державними структурами.

Відбитки, які отримані під контролем фахівця, зазвичай мають високу якість та містять достатню кількість індивідуальних ознак, як зображено на рисунку 3.3. Алгоритми опрацювання та порівняння таких відбитків досить добре опрацьовані [12].

Рисунок 3.3. Відбитки гарної якості

Відбитки, які отримують на контролях доступ, які зазвичай є поспіхом, призводять до отримання неякісного зображення, як показано на рисунку 3.4.. Тому, потрібно підвищити якість зображення, тобто сегментацію з чітким відображенням гребні для надійного виділення мінуцій і подальшого розпізнавання.

Рисунок 3.4. Приклад відбитку пальця не достатньої якості

Один із методів описаний в роботі [15], проте спочатку потрібно підвищити якість зображення. Для підвищення зображення, потрібно слідкувати наступним крокам .

1. Нормалізація зображення. Виконати нормалізацію вихідного зображення відбитка пальця, щоб після перетворення воно мало задані середнє значення і середньоквадратичне відхилення. .

2. Обчислення локальної орієнтації. Обчислити орієнтаційне зображення з нормалізованого зображення відбитка пальця.
3. Оцінка локальної частоти хребтів. Обчислити матрицю частот на базі нормалізованого та зображень відповідної орієнтації.
4. Сегментація відбитка. Створити маску відбитку шляхом розбиття нормалізованого зображення на блоки та виконання класифікації кожного блоку, розділивши їх на відбитки, які містять хребти, і ті, які їх не містять. Потім маску згладити за допомогою морфологічних фільтрів.
5. Фільтрація нормалізованого зображення. Застосувати набір фільтрів, які носять назву Габора, або його подібних і які налаштовані на локальну орієнтацію виступів і частоту виступів, до пікселів хребтів і западин у нормалізованому зображенні для отримання поліпшеного зображення відбитка пальця. Для побудови шаблону відбитка використовувати частину зображення, яке отримано після фільтрації зображення, що потрапило в маску, побудовану на кроці 4.

3.2.2. Організація біометричного контролю доступом

Схема автономного біометричного термінала для контролю доступу на об`єкті інформаційної діяльності представлено на рисунку 3.5.

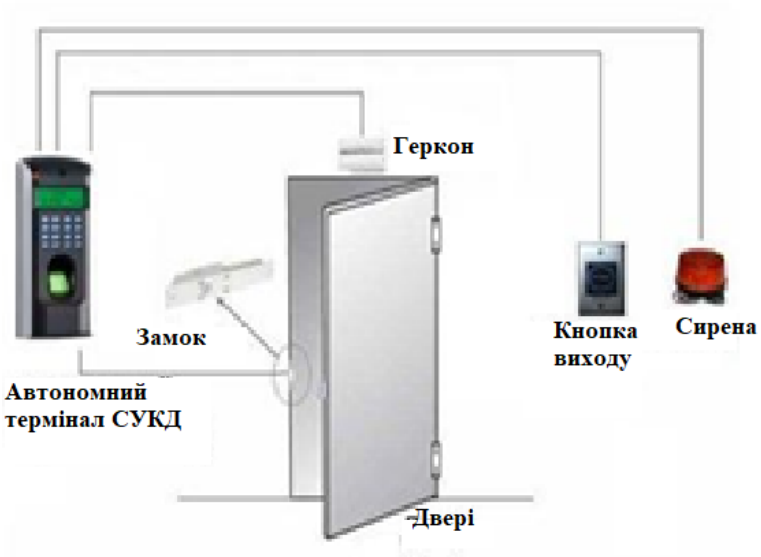

Рисунок 3.5. Схема автономного біометричного терміналу

Точкою проходу (дверима) керує автономний біометричний термінал без під’єднання до комп’ютера. Саме, це є контролером та зчитувачем сенсору відбитку пальців у єдиному корпусі. Щоб відкрити двері, користувач повинен прикласти палець до відбитку. Коли результат буде позитивний, то користувачу відкриються двері. Для того, щоб вийти потрібно скористатися кнопкою виходу.

Також, можна приєднати сирену для оповіщення про злом пристрою. Також, технологія застосовується СКУД на одній точці проходу або в декількох. Автономне живлення від вбудованих пальчикових батарейок живлення є перевагою. Схема мережевого біометричного термінала для контролю доступу на ОІД представлено на рисунку 3.6.

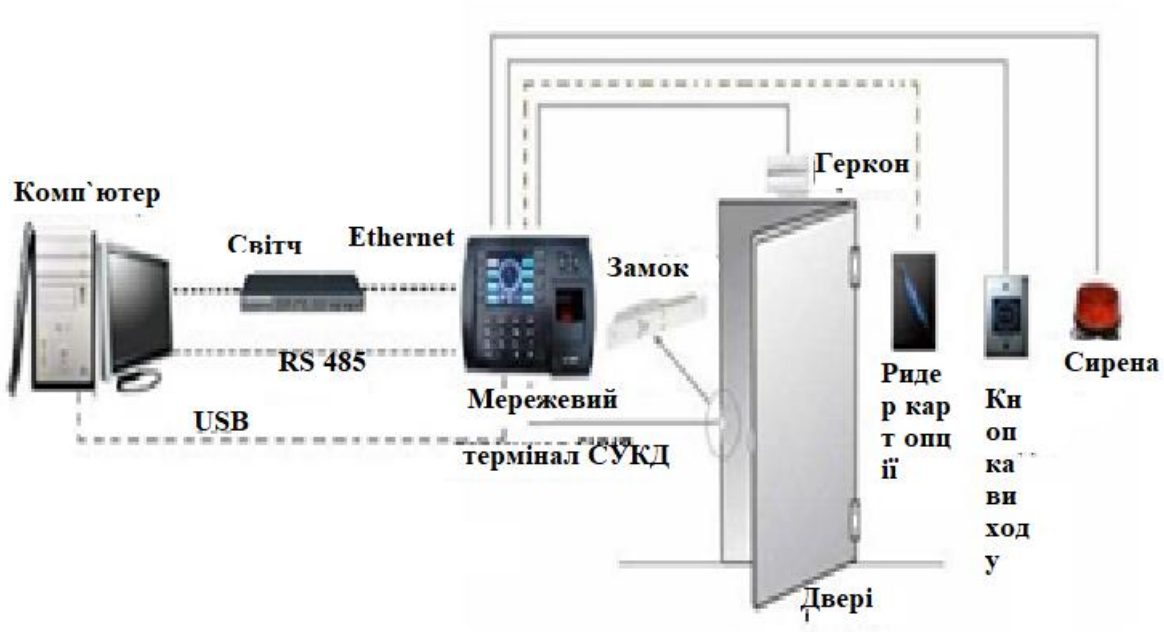

Рисунок 3.7. Схема мережевого біометричного терміналу

Мережевий термінал доступу може підключатися до комп'ютера за мережевими інтерфейсами *RS*485, *Ethernet*. Для того, щоб порівняти відбитки пальців виконуються дії, як на самому терміналі, так і на сервері з використанням режиму серверної ідентифікації. На сервері створюються не обмежені за розміром бази даних шаблонів відбитків. Для створення розподілених мережевих систем контролю доступу використовують мережеві термінали. Програмне забезпечення керує одночасно великою кількістю терміналів. Є

можливість підключити usb-сканер відбитків пальців для реєстрації відбитка пальця користувача в системі. Шаблони відбитків дозволених користувачів можна завантажити в усі термінали в мережі.

Схема мережевого біометричного термінала для контролю доступу до інформаційних ресурсів на ОІД представлено на рисунку 3.7.

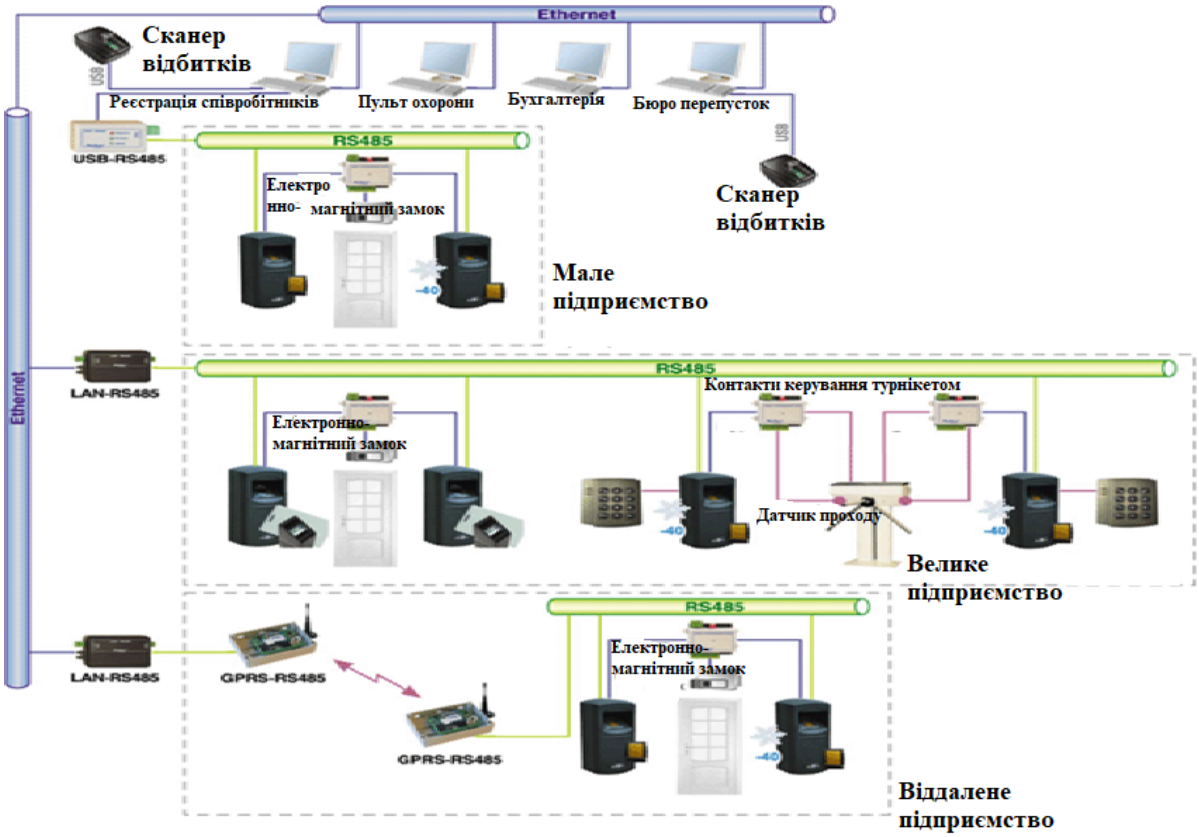

Рисунок 3.7. Схема мережевого біометричного термінала для контролю доступу до інформаційних ресурсів

Дана схема відкрита для інтеграції з пристроями інших виробників і за необхідності може нарощуватися. Організація мережі будується з використанням інтерфейсу *RS*485 та виділених ліній зв'язку *Ethernet* або стільникових мереж формату *GSM*. Біометричні термінали об'єднуються в магістраль *RS*485 кількість яких досягається 255 примірників.

3.3. Рекомендації по впровадженню біометричних систем контролю доступом на ОІД

Як зазначалося раніше, біометрія є хорошою процедурою, при використанні СКУД, яка підвищить рівень безпеки як ідентифікація або як один із способів аутентифікації. Відзначимо, різницю між ідентифікацією та верифікацією. Верифікація виконує малу кількість порівнянь, а ідентифікація здійснює порівняння з великою кількістю біометричних даних, що вимагає високої продуктивності системи, а в протилежному разі можна використовувати дешевшу ЕОМ.

Коли використовується біометрія, то використовується більше ресурсів ЕОМ. Рекомендуємо, біометрію зробити частиною процедурою верифікації на об’єктах КІІ. Також, з’являється багатофакторна автентифікація, яка є гарним рішення у підвищенні безпеки, зокрема і у об’єктах комп’ютерного почерку.

Приклад типової схеми інтеграції біометричних блоків доступу в СКУД на ОІД представлено на рисунку 3.8.

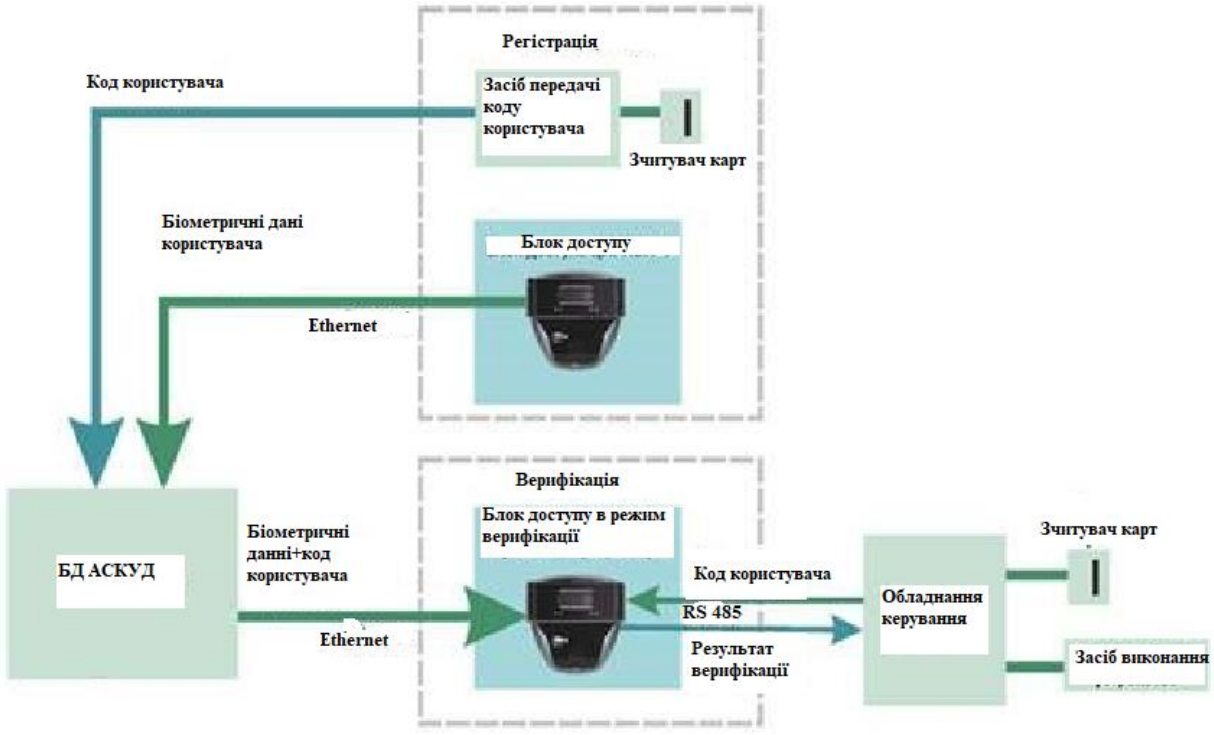

Рисунок 3.8. Загальна функціональна схема біометричного терміналу

Висновок до розділу 3

Отже, надавши переваги, можна зробити висновок, що ідентифікація біометричним способом є проста та актуальна. Рекомендуємо, організаціям використовувати систему аутентифікації застосувавши біометрію. Подібні системи і надалі застосовуються у багатьох практичних реалізаціях, про те їх опис алгоритмів в літературі відсутній. У розділі описані основні алгоритми оброблення та аналізу зображень відбитка пальця різної якості, подано схеми трьох варіантів організації біометричної системи контролю доступу в приміщення та до інформаційних ресурсів.

ВИСНОВОК

1. Технології, засновані на біометричній ідентифікації з кожним роком, набувають дедалі ширшого поширення і популярності як з боку співробітників інформаційної безпеки, так і з боку користувачів, які активно взаємодіють з ними. Яскравим прикладом є повсюдне впровадження цієї технології в портативні персональні пристрої, зокрема в смартфони. Використання цієї технології на ОІД насамперед призведе до підвищення загальної надійності систем захисту.

2. Впровадження біометрії на ОІД вже показало себе з позитивного боку. На даний момент технологією вже користуються багато банків.

3. Важливим є створення та реалізацію державного проекту під назвою єдина біометрична система, спрямований на загальну ідентифікацію громадян, які користуються банківськими послугами за біометричною інформацією.

4. Основне завдання виробників засобів захисту і розробників СКУД з використанням біометричної ідентифікації це правильна інтеграція засобів захисту.

5. Очевидним є те, що в різних галузях нові технології впроваджуються з різною швидкістю. Природно, це стосується і біометрії.

6. На теперішній час будинок та автомобіль уявляють собою об`єкти, які швидкими темпами розумнішають і насичуються різноманітними цифровими технологіями. Це означає, що саме ці галузі в недалекому майбутньому стануть драйверами розвитку біометричних технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. Abdalla Ali A.A. Biometricheskaya identifikatsiya lichnosti [Biometric person identification]. Fizika i radioelektronika v meditsine i ekologii : Sbornik trudov 8 Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii «s nauchnoy molodezhnoy shkoloy imeni I.N. Spiridonova [Physics and radioelectronics in medicine and ecology : proceedings of the 8th International Scientific Conference «with the scientific youth school named after I.N. Spiridonov], 2008, Book 2, pp. 145–147. Available at: http://freme.vlsu.ru/trudy_pdf/freme_2008_book_2.pdf

2. Averin A. I., Sidorov D. P. Autentifikatsiya polzovateley po klaviaturnomu pocherku [User authentication base on keystroke dynamics]. Ogarev-onlayn [Ogarev-online], 2015, no. 20 (61). Available at: http://journal.mrsu.ru/wp-content/uploads/2015/10/averin-sidorov.pdf

3. Vasilev V. I., Kalyamov M. F., Kalyamova L. F. Identifikatsiya polzovateley po klaviaturnomu pocherku s primeneniem algoritma registratsii chastykh bigramm [Identification of users by keyboard handwriting using the algorithm of frequent bigrams registration.]. Modelirovanie, optimizatsiya i informatsionnye tekhnologii [Modeling, Optimization and Information Technologies], 2018, vol. 6, no. 1, pp. 399–407. Available at: https://www.elibrary.ru/item.asp?id=34971186

4. Brumshteyn Yu. M., Kharitonov D. V., Ivanova M. V. Analiz effektivnosti ispolzovaniya razlichnykh programmno-apparatnykh reshcheniy dlya issledovaniya dinamiki vypolneniya podpisi chelovekom. Fizika i radioelektronika v meditsine i ekologii : sbornik trudov XI Mezhdunarodnoy nauchno-tehnicheskoy konferentsii «s nauchnoy molodezhnoy shkoloy imeni I.N. Spiridonova [Physics and radioelectronics in medicine and ecology : proceedings of the XI International Scientific Conference with the scientific youth school named after I.N. Spiridonov]. 2014,

5. Putyato M. M., Makaryan A. S. Klassifikatsiya messendzherov na osnove analiza urovnya bezopasnosti khranimykh dannykh [Classification of messengers based on analysis of the security level of stored data]. Prikaspiyskiy zhurnal: upravlenie

i vysokie tekhnologii [Caspian Journal: Control and High Technologies], 2019, pp. 135–143. Available at: https://elibrary.ru/item.asp?id=41869982

6. Savinov A. N., Sidorkina I. G. Reshenie problem vozniknoveniya oshibok pervogo i vtorogo roda v sistemakh raspoznavaniya klaviaturnogo pocherka [Analysis of the solution problems the origin of type i errors and type ii errors in system of recognition of keystroke dinamics]. IKT: obrazovanie, nauka, innovatsii : trudy III Mezhdunarodnoy nauchnoprakticheskoy konferentsii [ICT: education, science, innovation : proceedings of the Third International ScientificPractical Conference]. Almaty, MUIT Publ., 2012. Available at: https://cyberleninka.ru/article/n/analiz-resheniyaproblem-vozniknoveniya-oshibok-pervogo-i-vtorogo-roda-v-sistemah-raspoznavaniya-klaviaturnogo-pocherka

7. Sidorkina I. G., Savinov A. N. Tri algoritma upravleniya dostupom k KSII na osnove raspoznavaniya klaviaturnogo pocherka operatora [Three algorithms of control access to the KSII on the basis of recognition of keystroke dynamics]. Vestnik Chuvashskogo universiteta [Bulletin of Chuvashia University], 2013, no. 3. Available at: https://www.elibrary.ru/download/elibrary_21115327_21253793.pdf

8. Kakova strategiya bezopasnogo dostupa dlya bankovskikh produktov [What is a secure access strategy for banking products]. Available at: http://www.smartsecurity.tech/wp-content/uploads/2017/03/Smart-Security.pdf

9. Metody biometricheskoy identifikatsii: sravnitelnyy analiz [Biometric authentication methods: a comparative analysis]. Available at: http://www.biometrics.ru/news/metodi_biometricheskoi_identifikacii_sravnitelnii_analiz/

10. El-Hadidi Kamal M. Biometrics. What and How. Available at: http://www.net-security.org/dl/articles/Biometrics.pdf

11. Sovremennye metody biometricheskoy identifikatsii [Modern methods of biometric identification]. Available at: https://www.azone-it.ru/sovremennye-metody-biometricheskoy-identifikacii

12. Modern statistical models for forensic fingerprint examinations: A critical review / J. Abraham [et al.] // Forensic Science International. – 2013. – Vol. 232, no. 1–3. – P. 131–150.

13. Handbook of fingerprint recognition / D. Maltoni [et al.]. – N.Y. : Springer-Verlag, 2009. – 494 p.

14. Muñoz-Briseño, A. Fingerprint indexing with bad quality areas / A. Muñoz-Briseño, P. 1839–1846.

15. Haber, R.N. Experimental results of fingerprint comparison validity and reliability : A review and critical analysis / R.N. Haber, L. Haber // Science and Justice, 2014. – Vol. 54. – P. 375–389.

16. Biometric identification [electronic resource] URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html (date of access: 11.04.2021).

17. Biometrics from "A" to "Z" a complete guide to biometric identification and authentication [electronic resource] URL: https://securityrussia.com/blog/biometriya.html (date of access: 11.04.2021).

18. Overview of the international market of biometric technologies and their application in the financial sector [electronic resource] URL: https://www.cbr.ru/Content/Document/File/36012/rev_bio.pdf (date of access: 11.04.2021).

19. The effectiveness of biometric control and access control systems in the implementation of customs control [electronic resource] URL: https://novainfo.ru/article/4909 (date of access: 15.04.2021).

20. Typical scheme of the PAPILLON ZIRCON-4 access unit in the current ASCUD [electronic resource] URL: http://www.papillon.ru/rus/50 (date of access: 10.05.2021).