Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти *другий (магістерський)*

Дослідження методів біометричної ідентифікації

(тема)

Виконав:
студент *2* курсу, групи *ІМІзм-22-1*
Вичужанін С.В.
(прізвище, ініціали)

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

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

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

Керівник *доц. к.т.н. Чеботарьова Д.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 _____ *Вичужанін С.В.*
(підпис) (прізвище та ініціали)

Керівник _____ *Чеботарьова Д.В.*
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *другий (магістерський)*

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

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

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ІМІ_____
(підпис)

"*25*" *січня* 2024р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Вичужаніну Сергію Володимировичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження методів біометричної ідентифікації*

затверджені наказом по університету від "*27*" *жовтня* 2023 р. № *238 Стз*

2. Термін подання студентом роботи до екзаменаційної комісії *25 січня 2024 р.*

3. Вихідні дані до роботи *дослідити процес верифікації користувача в мережі, різні види ідентифікації, процеси ідентифікації та автентифікації осіб на основі біометрії, статичні та динамічні біометричні методи, сфери застосування та перспективи розвитку біометричних технологій, методи багатофакторної ідентифікації, мультибіометричні методи, показники якості біометричних методів; виконати вибір оптимальних методів біометричної та мультибіометричної ідентифікації з урахуванням сукупності показників якості.*

4. Перелік питань, що потрібно опрацювати в роботі

1. Процес верифікації користувача в мережі

2. Біометрична ідентифікація

3. Мультибіометрична ідентифікація

4. Вибір оптимального методу мультибіометричної ідентифікації

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____

Слайди у форматі Power Point (назва, мета та задачі роботи, процес верифікації користувача в мережі, різні види ідентифікації, процеси ідентифікації та автентифікації осіб на основі біометрії, статичні та динамічні біометричні методи, сфери застосування БІ, перспективи розвитку біометричних технологій, методи багатофакторної ідентифікації, мультибіометричні методи, показники якості біометричних методів, вибір оптимальних методів БІ, вибір оптимальних методів МБІ, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*30.10.23*	*Виконано*
2	*Підбір літератури за темою роботи.*	*31.10 - 15.11.23*	*Виконано*
3	*Виконання розділу 1*	*16.11 - 30.11.23*	*Виконано*
4	*Виконання розділу 2*	*01.12 – 15.12.23*	*Виконано*
5	*Виконання розділу 3*	*16.12 – 31.12.23*	*Виконано*
6	*Виконання розділу 4*	*01.01 - 15.01.24*	*Виконано*
7	*Оформлення пояснювальної записки,*		
	презентаційного матеріалу та підготовка		
	до захисту у ЕК	*16.01 - 25.01.24*	*Виконано*

Дата видачі завдання *30 жовтня 2023 р.*

Студент _____ *Вичужанін С.В.*
(підпис) (прізвище, ініціали)

Керівник роботи _____ *доц. Чеботарьова Д.В.*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с., 30 рис., 4 табл.,32 джерела, 2 додатки

Об'єкт дослідження – методи біометричної ідентифікації.

Мета роботи – дослідження біометричних та мультибіометричних методів для ідентифікації користувачів мереж.

Результати – в роботі розглянуто процес верифікації користувача в мережі, проаналізовано особливості різних видів ідентифікації. Досліджено процеси ідентифікації та автентифікації осіб на основі біометрії. Виконано аналіз статичних та динамічних методів, розглянуто сфери застосування та перспективи розвитку біометричних технологій. Досліджено багатофакторну ідентифікацію та роль біометрії в її методах. Виконано оцінку показників якості біометричних методів. Виконано вибір оптимальних методів біометричної та мультибіометричної ідентифікації з урахуванням сукупності показників якості.

БІОМЕТРІЯ, ІДЕНТИФІКАЦІЯ, ІНФОРМАЦІЯ, БЕЗПЕКА, ЗАХИСТ, АВТЕНТИФІКАЦІЯ, МЕТОД, ОЗНАКА, МУЛЬТИБІОМЕТРИЧНИЙ МЕТОД.

THE ABSTRACT

Explanatory note: 76 p., 30 fig., 4 tabl., 32 sources, 2 app.

Object of research - methods of biometric identification.

The purpose of the work is to research research of biometric and multi-biometric methods for identification of network users.

Results - the work examines the process of user verification in the network, analyzes the features of various types of identification. The processes of identification and authentication of persons based on biometrics have been studied. The analysis of static and dynamic methods was performed, the areas of application and prospects for the development of biometric technologies were considered. Multifactor identification and the role of biometrics in its methods are studied. The quality indicators of biometric methods were evaluated. The selection of optimal methods of biometric and multi-biometric identification was carried out, taking into account the set of quality indicators.

BIOMETRY, IDENTIFICATION, INFORMATION, SECURITY, PROTECTION, AUTHENTICATION, METHOD, SIGN, MULTI-BIOMETRIC METHOD.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

БІ – біометрична ідентифікація;
БФІ – багатофакторна ідентифікація;
ВП – відбиток пальця;
ГО – геометрія обличчя;
МБІ – мультибіометрична ідентифікація;
ПГ – параметри голосу;
РВ – розташування вен;
РО – райдужна оболонка ока;
2FA (2 Factor Authentication) – двофакторна автентифікація;
ERR(Erronous Retention Rate) – помилковий коефіцієнт утримання;
FAR (False Acceptance Rate) – коефіцієнт помилкового прийняття;
FER (Failure-to-Enrol Rate) – коефіцієнт відмови в реєстрації;
FMR (False Match Rate) – коефіцієнт помилкових збігів;
FN (False Negative) – відмова законному користувачу;
FNMR (False Non-Match Rate) - коефіцієнт помилкових невідповідностей;
FNR (False Negative Rate) – коефіцієнт помилково негативних результатів;
FP (False Positive) – авторизація незаконного користувача;
FPR (False Positive Rate) – коефіцієнт помилково позитивних результатів;
FRR (False Rejection Rate) – коефіцієнт помилкових відхилень;
MFA (Multi Factor Authentication) – багатофакторна автентифікація;
TN (True Negative) – відмова незаконному користувачу;
TP (True Positive) – авторизація законного користувача.

ВСТУП

За останні кілька десятиліть повсюдне впровадження інтернету та цифрова революція змінили спосіб роботи різних компаній та їхню взаємодію з клієнтами. Одним із найбільш значних зрушень став перехід від фізичних закладів до онлайн-платформ. Основними причинами цього переходу стали: створення присутності в інтернеті, бум електронної комерції, інтеграція соціальних мереж, оптимізація для мобільних пристроїв, прийняття рішень на основі даних, ера контенту, інтеграція екосистеми, поява штучного інтелекту та автоматизації тощо. Крім того зовнішні події, зокрема пандемія Covid-19 та війна, суттєво пришвидшили перехід бізнесу, освіти, медицини та інших важливих галузей до онлайн-функціонування.

У міру того як світ все більше переходить в інтернет, все більша кількість інформації, в тому числі і конфіденційної, зберігається та переміщується в інфокомунікаційних системах та мережах, тому все більш актуальним стає питання безпеки інформації, захисту інформації та розмежування доступу користувачів до даних. Саме тому користувачі постійно ідентифікуються, автентифікуються та авторизуються. Ідентифікація та автентифікація мають конкретні цілі та є необхідними компонентами безпеки даних. Аспект авторизації призначає права та привілеї певним ресурсам. Лише після належної ідентифікації та автентифікації користувача можна отримати авторизований доступ до систем або інформації.

В наш час найбільш перспективними є біометричні методи ідентифікації та автентифікацію. Сьогодні біометрія є найбільш підходящим засобом ідентифікації та автентифікації осіб, надійним і швидким способом, що використовує унікальні біологічні характеристики.

Дана кваліфікаційна робота присвячена дослідженню різноманітних методів біометричної ідентифікації. Аналіз інформаційних джерел за тематикою роботи [1 - 31] підтвердив актуальність цієї тематики, саме тому ця кваліфікаційна робота є актуальною.

1 ПРОЦЕС ВЕРИФІКАЦІЇ КОРИСТУВАЧА В МЕРЕЖІ

У технологічно орієнтованому сучасному світі стрімко розвиваються інформаційні технології та мережі, що спричиняє в свою чергу і появу нових проблем інформаційної безпеки, зокрема нові можливості несанкціонованого доступу до ресурсів мереж. Велику увагу в наш час приділяють дослідженню та вдосконаленню методів та систем захисту інформації.

Захист інформації – це сукупність організаційних, технічних та інших заходів, правових норм щодо запобігання заподіянню шкоди інтересам, потребам особи, суспільства, держави в інформаційній галузі, забезпечення права на інформацію [1].

Важливу роль в захисті інформації відіграє контроль та управління доступом до мереж та даних. Управління доступом є важливою частиною комплексного захисту інформації, який відповідає за коректне використання ресурсів інформаційних мереж та систем. Саме тому сьогодні існує необхідність постійно підтверджувати особу користувача в мережі або в компанії, проходячи ідентифікацію та автентифікацію кілька разів на день для отримання безпечного доступу до пристроїв, мереж, платформ, сайтів, додатків та даних.

Перевірка особи користувача, перш ніж він зможе здійснити транзакції або отримати доступ до ресурсів системи, може запобігти шахрайству з особистими даними та допомогти захистити інформацію у відповідності до глобальних вимог.

Перевірка особи користувача стосується процесу переконання, що кожен клієнт є саме тим, ким він має бути. Перевірка наданої користувачем інформації дає можливість визначити чи є користувач реальною людиною і чи особа, яка намагається отримати доступ до інформації або здійснити транзакцію, є особою, за яку себе видає. З цієї причини перевірка особи користувача корисна як для нових клієнтів, так і для повторної перевірки існуючих клієнтів, які намагаються отримати доступ до своїх облікових записів

В цілому, процес перевірки особи користувача гарантує, що шахраї та зловмисники не зможуть мати доступ до інформації та ресурсів системи. Це також перешкоджає будь-кому здійсненню транзакцій від іншої особи.

Для деяких систем та мереж процес підтвердження особи є просто корисним. Однак для інформаційних мереж, інфокомунікаційних компаній, постачальників фінансових послуг тощо вони є обов'язковою частиною боротьби за інформаційну безпеку.

1.1 Етапи верифікації користувача в мережі

Процес управління доступом, що включає в себе розпізнавання користувача при вході в інформаційну мережу чи систему, перевірку його автентичності та наявності певних прав у цього користувача, називається процесом верифікації. Процес верифікації (рис.1.1) складається з трьох основних етапів:

- ідентифікація,
- автентифікацію,
- авторизаці.

Рисунок 1.1 – Етапи верифікації користувача в системі

Кожен зареєстрований в інформаційній мережі чи системі користувач має в базі деяку інформацію, яка однозначно його ідентифікує як легального (законного) користувача та називається ідентифікатором користувача. Якщо такого ідентифікатора у користувача немає – то такий користувач є нелегальним. Саме тому кожен користувач перш ніж отримати доступ до ресурсів та даних має пройти всі етапи верифікації.

Процедуру проходження користувачем процесу верифікації наведено на рис. 1.2.

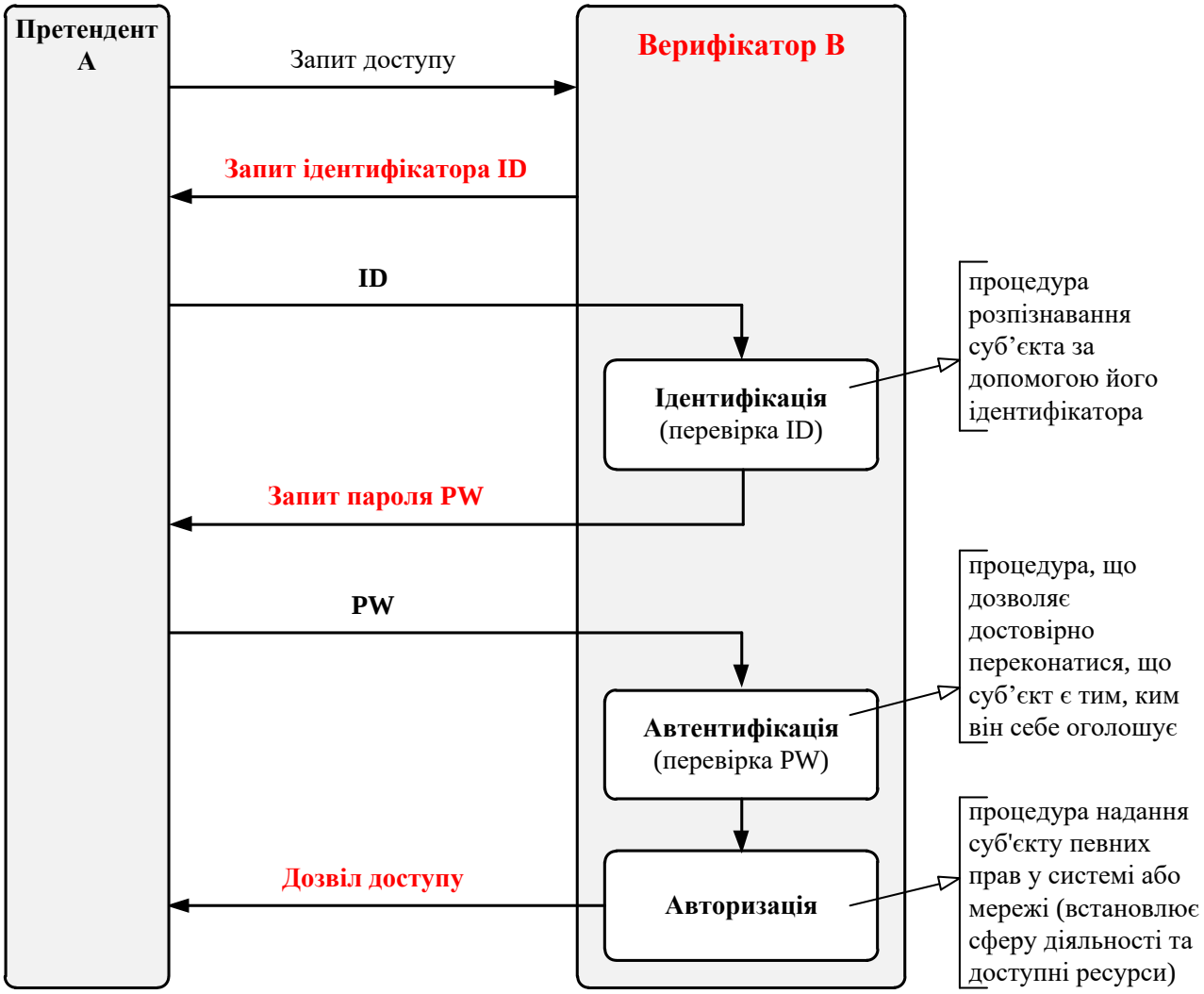


Рисунок 1.2 – Процедура верифікації користувача

Процедура верифікації відбувається наступним чином:

- користувач вносить ідентифікаційну інформацію та входить в систему;

- користувач встановлюєте для майбутнього входу в систему фактор автентифікації (пароль, ключ доступу тощо);

- при кожному наступному вході в систему система запитує ідентифікатор користувача та фактор автентифікації;

- система перевіряє правильність інформації та, якщо так, підтверджує особу користувача та надає йому доступ до систем і ресурсів, авторизованих адміністратором.

Процедура верифікації користувача (рис. 1.2) допомагає визначити перевірених користувачів і дозволяє їм безпечно отримувати доступ до облікових записів і мереж. Це механізм безпеки, створений для блокування доступу неавторизованих користувачів або кіберзлочинців до конфіденційних даних і ресурсів [2].

Додавання до ідентифікації користувача кількох рівнів захисту за допомогою надійної автентифікації та авторизації допомагає зменшити ризик крадіжки особистих даних [3].

Першим етапом верифікації є ідентифікація, овна виконується першою при вході користувача в систему. Ідентифікація – це процедура розпізнавання користувача, тобто це перевірка імені облікового запису або ідентифікатору користувача. В середині системи це визначає привілеї доступу. Наприклад, у соціальних мережах власник облікового запису є єдиною особою, яка має право переглядати приватні повідомлення облікового запису. У корпоративному контексті ця ідентифікація визначає набір програм і даних, які може використовувати конкретний користувач.

Другим етапом є автентифікацію, за допомогю якої користувач підтверджує, що він є законним власником облікового запису. Найпоширенішим прикладом цього є пароль. Автентифікація має бути доступною тільки для користувача та постачальника послуг, або, ще краще, лише для користувача [4].

Ідентифікація та автентифікація не є протилежними, вони є послідовними кроками в процесі верифікації. Наприклад в онлайн-банкінгу ім’я користувача є особливим і унікальним для нього, але номер рахунку може використовуватися окремими користувачами (тобто, спільний поточний рахунок). Лише авторизовані користувачі повинні мати повний доступ до облікового запису та повноваження виконувати транзакції. На практиці кожен банк використовує

декілька форм автентифікації, перш ніж дозволити авторизованому користувачеві ввійти.

Третім і останнім етапом верифікації є авторизація. Авторизація в безпеці системи – це процес надання користувачеві прав, тобто дозволу на доступ до певного ресурсу або функції. Прикладами авторизації є надання комусь дозволу завантажити певний файл на сервер або надання окремим користувачам адміністративного доступу до певних програм. У захищеному середовищі авторизація завжди має слідувати за автентифікацією. Перш ніж адміністратори організації нададуть доступ до запитаних ресурсів, користувачі повинні підтвердити, що їх особи справжні.

1.2 Фактори автентифікації

Для підтвердження своєї ідентичності користувач має надати системі інформацію, яка буде ідентифікувати користувача. Така інформація називається фактором автентифікацію. В залежності від сутності наданої інформації визначають три типи факторів автентифікації (рис. 1.3).

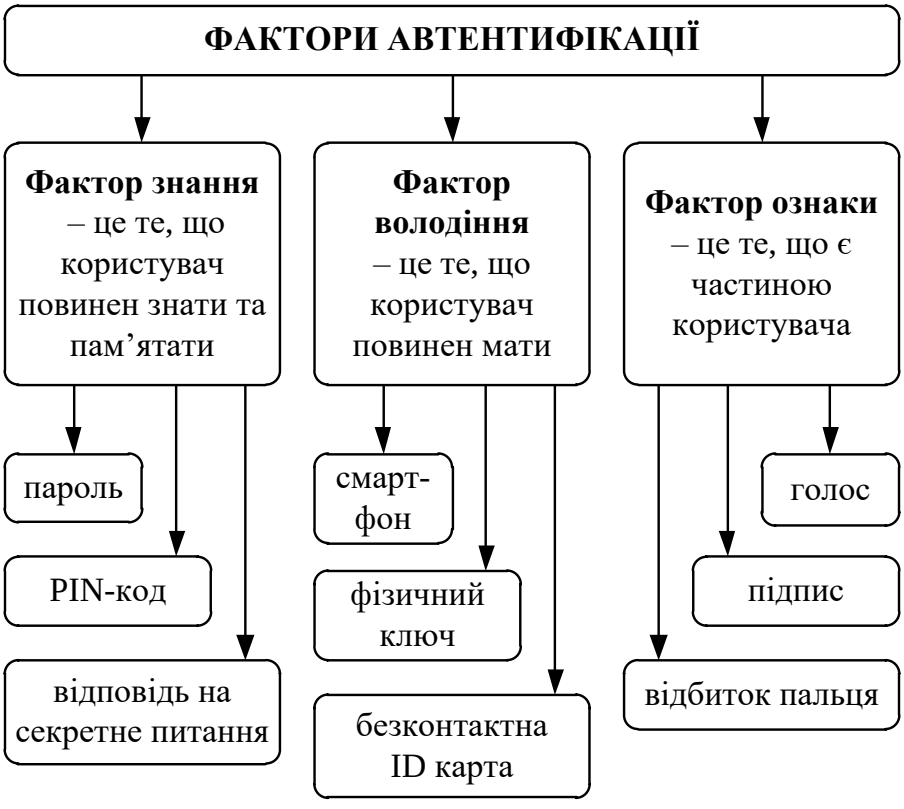


Рисунок 1.3 – Фактори автентифікації

В залежності від типу використовуваного фактору автентифікації, а також від способу дії визначають різні види ідентифікації користувачів інформаційних мереж і систем.

1.3 Переваги та недоліки різних видів ідентифікації користувачів

В наш час існують чотири основні види ідентифікації [5 – 7]: парольна, апаратна, біометрична та багатофакторна ідентифікація (рис.1.4).

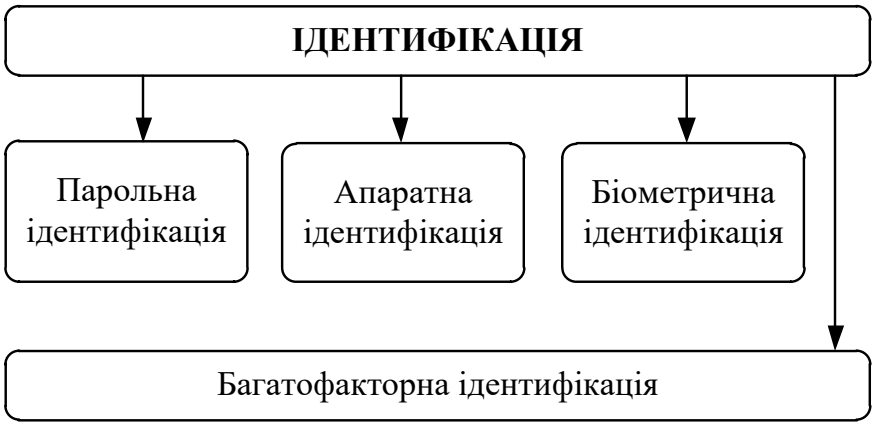


Рисунок 1.4 – Види ідентифікації

В одних системах доцільно використовувати одні види ідентифікації, в інших – інші, оскільки кожен вид ідентифікації має свої особливості, свої переваги і недоліки.

Парольна ідентифікація – це метод, в основі якого лежить фактор знання (рис. 1.3) та який вимагає від користувача для підтвердження своєї особи введення пароля. Після введення облікових даних вони порівнюються зі збереженими обліковими даними в базі даних системи, і якщо облікові дані збігаються, то користувач отримує доступ. Процедуру парольної ідентифікації наведено на рис.1.5, а переваги та недоліки даного методу – на рис.1.6.

Парольна ідентифікація особлива тим, що безпека та надійність ідентифікації безпосередньо залежать від відповідальності користувача. Користувач може забути пароль, комусь передати, необережно вводити на очах у інших або створити простий пароль, який зловмисник зможе підібрати. Але якщо користувач буде відповідальним та уникатиме подібних помилок, то це може повністю ліквідувати негативні моменти цього способу ідентифікації.

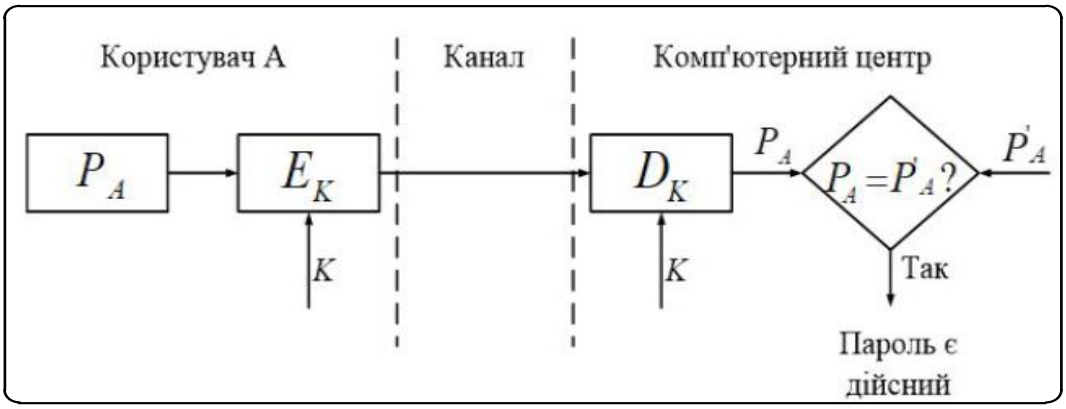


Рисунок 1.5 – Процедура парольної ідентифікації

ПАРОЛЬНА ІДЕНТИФІКАЦІЯ

ПЕРЕВАГИ:	**НЕДОЛІКИ**
- простота використання	- значна залежність надійності ідентифікації від користувачів
- простота реалізації	- можливість забути
- не потребує витрат	- зловмисник може підібрати пароль
- даний процес реалізований у більшості програмних продуктів	- зловмисник може підгледіти процес введення

Рисунок 1.6 – Переваги та недоліки парольної ідентифікації

Апаратна (токенова) ідентифікація – це метод, в основі якого лежить фактор володіння (рис. 1.3) та який вимагає від користувача для підтвердження своєї особи використання певного пристрою (точену, карти тощо). Можливі пристрої апаратної ідентифікації наведено на рис.1.7, а переваги та недоліки даного методу – на рис.1.8.

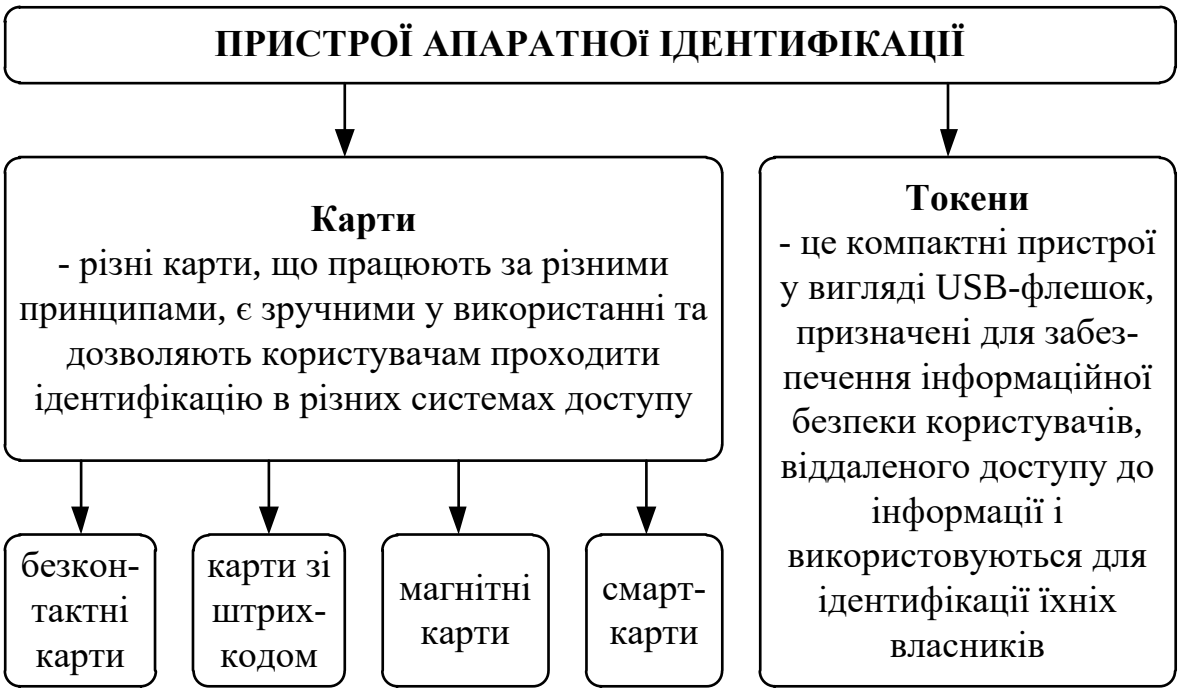


Рисунок 1.7 – Пристрої апаратної ідентифікації

Рисунок 1.8 – Переваги та недоліки апаратної ідентифікації

Біометрична ідентифікація (БІ) – це метод, в основі якого лежить фактор ознаки (рис. 1.3) та який вимагає від користувача для підтвердження своєї особи представлення унікальної властивості або біологічної ознаки користувача. Сьогодні біометрична ідентифікація є дуже актуальною, оскільки забезпечує майже 100% ідентифікацію, вирішуючи проблеми втрати паролів та особистих ідентифікаторів [7]. Переваги та недоліки даного методу наведено на рис.1.9.

Рисунок 1.9 – Переваги та недоліки біометричної ідентифікації

Багатофакторна ідентифікація (БФІ) – це метод, який використовує одночасне використання деякої сукупності різних факторів (ознаки і володіння, ознаки і знання, володіння і знання, декількох факторів ознаки тощо). Сьогодні існують готові пристрої, що поєднують в собі різні види ідентифікації для реалізації БФІ (рис.1.10). Переваги та недоліки даного методу детально розглянуто в третьому розділі пояснювальної записки.

Рисунок 1.10 – Приклади пристроїв БФІ

Останнім часом метод БФІ стає все більш поширеним, оскільки зі збільшенням кількості використовуваних факторів – суттєво підвищується надійність верифікації.

Найбільш широко використовуваним методом перевірки є двофакторна ідентифікація, яка передбачає наявність двох кроків для підтвердження особи користувача. Вона є надійнішою, ніж ідентифікація за одним фактором.

З кожним наступним рівнем (додатковим методом ідентифікації користувача) система стає все більш безпечнішою та запобігає злому облікового запису, навіть якщо один із рівнів вийшов з ладу.

2 БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ

2.1 Ідентифікація та автентифікацію на основі біометрії

Біометрія – це наука про ідентифікацію людей за допомогою фізіологічних ознак [8]. Практично будь-яка фізіологічна ознака людини може бути використана для ідентифікації; однак найбільш узагальнені біометричні методи включають автоматичне розпізнавання відбитків пальців, облич, райдужної оболонки та сітківки ока, геометрії руки, голосу та підпису [8]. Біометричні методи є предметом постійних досліджень і розробок, тому вони постійно вдосконалюються.

Біометричні технології використовують різні наукові методи для ідентифікації та автентифікації людей шляхом аналізу їхніх конкретних фізичних характеристик. Загальні біометричні атрибути включають розпізнавання обличчя, відбитки пальців і райдужну оболонку ока. Кожен із цих атрибутів використовується належним чином для певних послуг, наприклад, відбиток пальця для платежів або автентифікація обличчя або райдужної оболонки ока на кордоні [9].

Використання біометрії має багато переваг. Основні з них представлені на рис. 1.9. Але найбільш важливою перевагою є рівень безпеки та точності, які вона гарантує. На відміну від паролів, бейджів чи документів, біометричні дані неможливо забути, загубити, обміняти чи вкрасти. Саме тому біометрія нерозривно пов’язана з питанням ідентичності.

Біометрія є найбільш доцільним засобом ідентифікації та автентифікації осіб надійним і швидким способом за допомогою унікальних біологічних характеристик людини. Біометрія дозволяє ідентифікувати та автентифікувати особу на основі впізнаваних, перевірених, унікальних і конкретних даних [10].

Біометрична ідентифікація полягає у встановленні особистості людини. Мета полягає в тому, щоб отримати елемент біометричних даних цієї особи. Це може бути фотографія обличчя, запис голосу або відбиток пальця. Потім ці дані порівнюються з біометричними даними кількох інших осіб, які зберігаються в базі даних. При цьому виконується процес визначення особи користувача.

Біометрична автентифікація порівнює дані про характеристики людини з біометричним «шаблоном» цієї особи, щоб визначити схожість. Спочатку

зберігається еталонна модель. Потім збережені дані порівнюються з біометричними даними особи, які підлягають автентифікації. При цьому виконується процес визначення чи справді користувач є тією особою, за яку себе видає.

Різницю між біометричною ідентифікацією та біометричною автентифікацію показано на рис. 2.1.

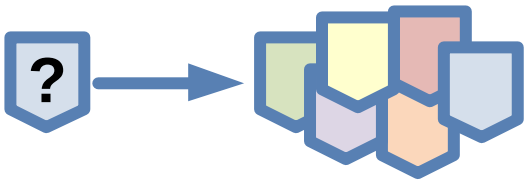
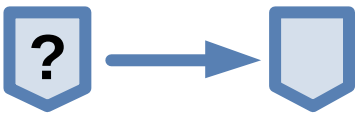
Біометрична ідентифікація	**Біометрична автентифікація**
Визначає особистість людини	Визначає, чи справді людина є тим, за кого себе видає
Відображення один до багатьох  Вартість визначення залежить від кількості записів користувачів	Відображення один до одного  Вартість визначення не залежить від кількості записів користувачів
Зафіксовані біометричні дані походять із набору відомих біометричних характеристик, які зберігаються в системі	Зняті біометричні підписи можуть бути невідомий системі

Рисунок 2.1 – Біометрична ідентифікація та біометрична автентифікація

Основними функціями біометричних систем ідентифікації є реєстрація та розпізнавання, які пояснюються на рис. 2.2.

Біометрія базується на біометричних показниках. Біометричні показники – це вимірювані біологічні (анатомо-фізіологічні) і поведінкові характеристики, які можна використовувати для автоматичного розпізнавання особи. Поведінкова біометрія може розпізнавати користувачів на основі того, що вони роблять, а фізіологічна біометрія може виявляти атрибути притаманні особі користувача. Саме так лікарні використовують біометричні показники для ідентифікації пацієнтів і моніторингу їхнього самопочуття. Сучасні компанії додають біометричні датчики до багатьох своїх пристроїв, які можуть

ідентифікувати користувачів за допомогою програмного забезпечення для розпізнавання обличчя та відбитків пальців [11].

Рисунок 2.2 – Основні функції біометричної ідентифікації

Процедуру процесу біометричної ідентифікації представлено на рис.2.3. Вона містить в собі такі етапи:

- збір даних,
- обробка зразків,
- зіставлення з базою даних шаблонів,
- прийняття рішення про доступ або відмову.

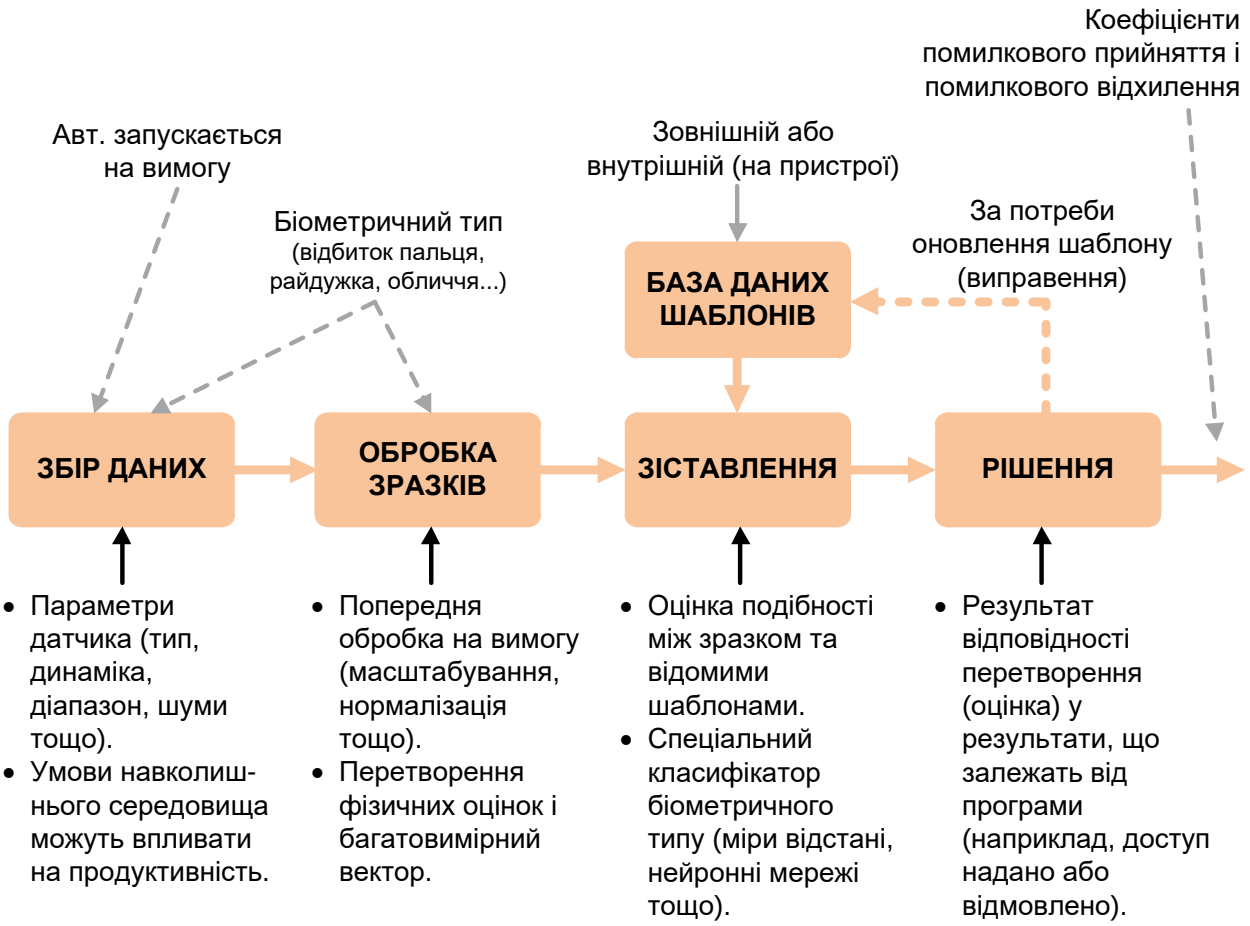


Рисунок 2.3 – Процедура процесу біометричної ідентифікації

Під час використання біометричних показників на особистих пристроях користувача, пристрій спочатку попросить користувача завершити початкове сканування, щоб створити профіль з біометричними показниками. Потім біометричні дані користувача будуть зібрані та збережені для подальшого використання. З цього моменту пристрій користувача порівнюватиме всі майбутні спроби входу з даними, пов’язаними з його профілем.

Існує два види біометричних показників: фізіологічні та поведінкові.

Фізіологічні вимірювання можуть бути морфологічними і біологічними. Морфологічні ідентифікатори в основному складаються з відбитків пальців, форми руки, візерунка вени пальця, ока (райдужної оболонки та сітківки) та форми обличчя. Біологічні ідентифікатори це ДНК, кров, слина, сеча [10].

Поведінкові вимірювання - це розпізнавання голосу, підпису, динаміки почерку (швидкості руху пера, прискорення, тиску, нахилу), динаміки натискання клавіш, ходи, жестів тощо.

Різні види біометричних показників не мають однакового рівня надійності. Наприклад, фізіологічні показники зазвичай забезпечують стабільність протягом життя людини. Також вони не схильні до стресу, на відміну від ідентифікації за допомогою поведінкових вимірювань.

Відповідно до даних з джерела [12] найбільш широко використовуваними для розпізнавання біометричними позниками на сучасному ринку є відбиток пальця та геометрія обличчя (рис. 2.4). В цілому на рис. 2.4 можна побачити розподіл часток ринку методів БІ за різними біометричними показниками.

Рисунок 2.4 – Діаграма розподілу часток ринку БІ

За типом застосовуваних біометричних показників методи біометричної ідентифікації поділяються на два види:

- статичні методи, які ґрунтуються на фізіологічних показниках, що, як правило, є статичними;

- динамічні методи, які ґрунтуються на поведінкових показниках, що, як правило, є динамічними.

2.2 Статичні методи БІ

Статичні методи (рис. 2.5) використовують для розпізнавання особи унікальні властивості, що дані особі від народження і є невід'ємними від неї протягом всього її життя.

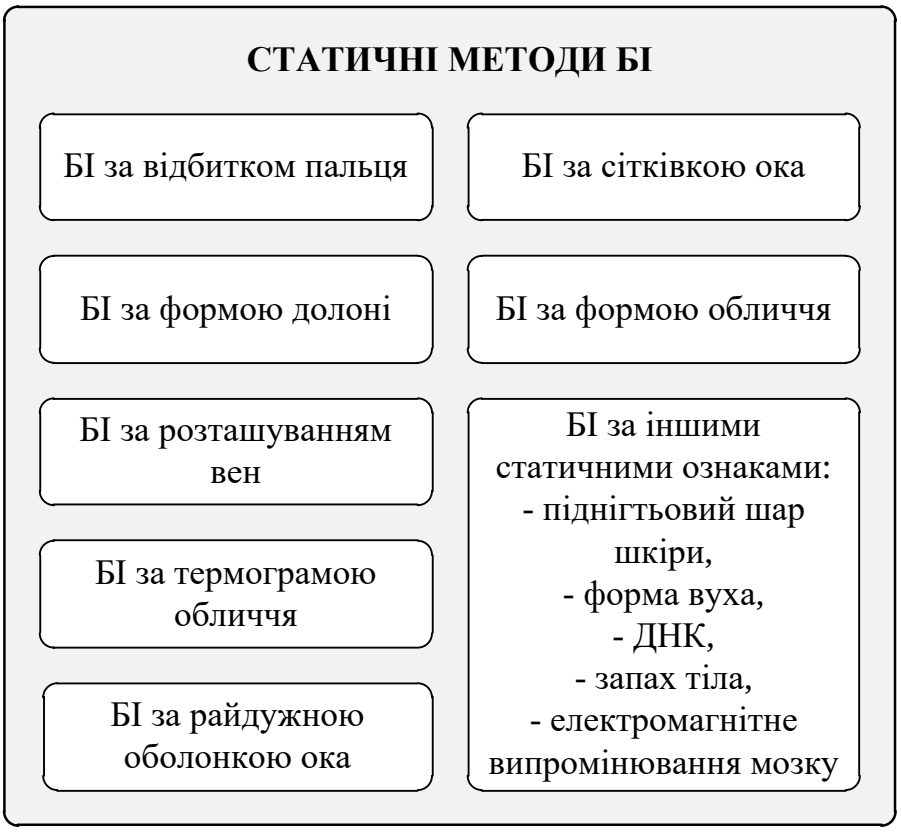


Рисунок 2.5 – Статичні методи біометричної ідентифікації

Статистичні методи, як правило, пов'язані з аналізом зображень і реалізуються за допомогою методів комп'ютерного зору.

Найбільше розповсюдження на сьогоднішній момент отримали такі статистичні методи БІ:

- БІ за відбитком пальця – Fingerprint Recognition,
- БІ за геометрією обличчя – Face Recognition,
- БІ за райдужною оболонкою ока – Iris Recognition,
- БІ за рисунком вен – Vein Recognition.

Одним з найдавніших, найпростіших та найпопулярніших методів є БІ за відбитком пальця. Його частка на ринку – 55% [12]. Основні переваги та недоліки цього методу наведено на рис. 2.6.

Системи біометричного розпізнавання за відбитком пальця вловлюють і оцифровують основні характеристики відбитка пальця, щоб створити біометричний шаблон. Потім ці шаблони зберігаються в наборі даних, який дозволяє системі вибирати відбитки пальців для виконання окремих порівнянь або пошуку у відповідних базах даних залежно від варіанту використання.

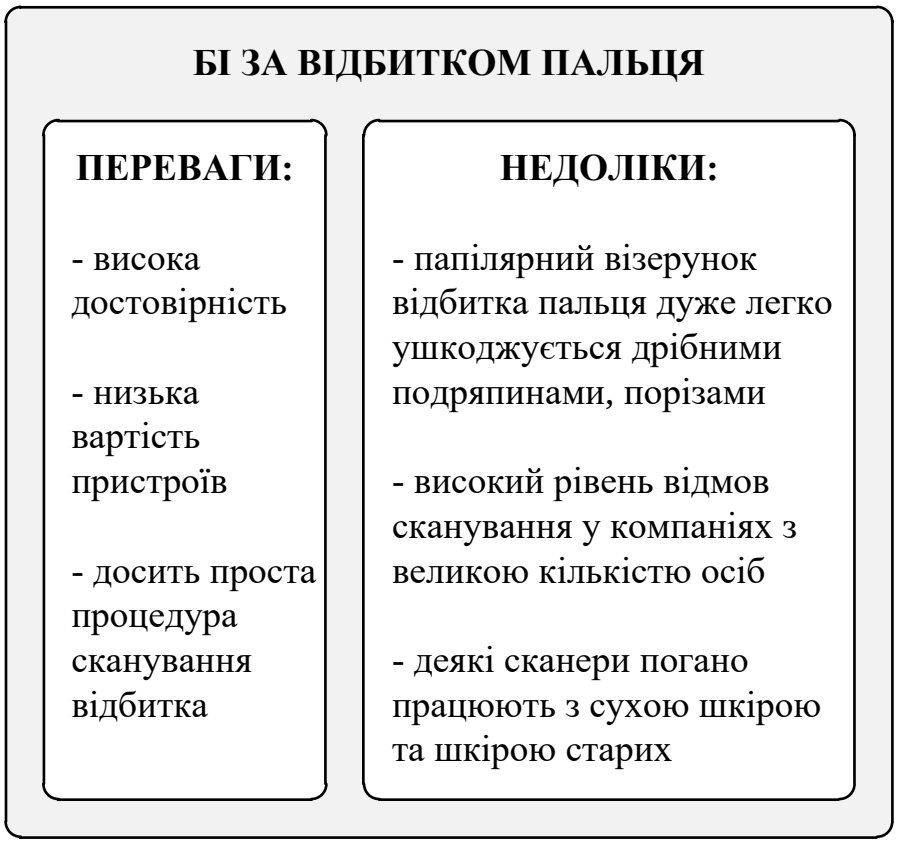


Рисунок 2.6 – Переваги та недоліки БІ за відбитком пальця

Більшість сучасних біометричних додатків використовують для БІ за відбитком пальця спеціальний сканер (палець кладуть на валик або катають по ньому) або безконтактний метод (необхідні деталі фіксуються на необхідній відстані). Безконтактний метод стає все більш популярним через потенційні проблеми з гігієною, пов’язані з кількома записами на той самий валик. Однак будь-який із цих методів реєстрації вимагає співпраці з суб’єктом і часто людського нагляду під час реєстрації для забезпечення якості біометричних даних [13].

Згідно [12] друге місце за популярністю використання займає метод БІ за геометрією обличчя (рис.2.4). Його частка на ринку – 23% [12]. На сьогоднішній день використовують розпізнавання облич за двовимірними (2D) та тривимірними (3D) зображеннями. Кожен з цих методів має свої переваги та недоліки (рис. 2.7 – 2.8), а також сферу застосування. 3D розпізнавання є досить складним завданням з точки зору реалізації, але через його високу ефективність існує багато методів 3D розпізнавання особи.

Рисунок 2.7 – Переваги та недоліки БІ за 2D геометрією обличчя

Рисунок 2.8 – Переваги та недоліки БІ за 3D геометрією обличчя

Біометрія обличчя використовує аспекти області обличчя для перевірки або ідентифікації особи. Існує велика різноманітність методів, які використовуються для статистичного перегляду характеристик обличчя таким чином, що не залежить від віку, виразу обличчя, освітлення чи багатьох інших змінних. Такі методи можуть включати алгоритми машинного навчання, які були навчені на величезних наборах зображень обличчя. Це не передбачає безпосереднього вимірювання відстані між об'єктами.

Сучасні алгоритми обличчя описують форму та зовнішній вигляд рис обличчя, очей, носа чи рота, шляхом застосування обробки зображень для отримання дискримінаційних і стабільних даних, об'єднаних у числове представлення, яке називається шаблоном обличчя [13].

Зображення обличчя можна зафіксувати звичайною камерою або камерою смартфона як портрет або як частину відео, поки об'єкт рухається. Зображення можуть бути зроблені дистанційно та на відстані без співпраці чи відома суб'єкта даних. Поява передових алгоритмів, інструментів машинного навчання та можливостей обробки за останнє десятиліття значно підвищила точність розпізнавання обличчя.

Третє місце за популярністю використання згідно [12] займає метод БІ за райдужною оболонкою ока (рис.2.4). Його частка на ринку – 8% [12]. Основні переваги та недоліки цього методу наведено на рис. 2.9. Метод розпізнавання за райдужною оболонкою ока є одними з найбільш точних серед біометричних методів.

Райдужна оболонка ока – це кольоровий круглий сегмент у передній частині ока, який містить зіницю в центрі. Райдужка контролює розмір зіниці, щоб регулювати кількість світла, що потрапляє в око. Технологія розпізнавання райдужної оболонки ока використовує унікальні візерунки кольорових тканин, які утворюють райдужну оболонку. Ці візерунки фіксуються камерою, яка працює в діапазоні хвиль, близьких до інфрачервоного діапазону. Перші камери райдужної оболонки мали бути близько до очей (але не контактувати з ними), щоб записувати достатньо деталей, але технологічний прогрес тепер дозволяє розміщувати камери на певній відстані і знімати райдужну оболонку очей тих, хто рухається, наприклад вихід на посадку в аеропорту [13].

Система використовує алгоритми розпізнавання шаблонів, подібно до автоматизованих систем розпізнавання відбитків пальців, для виконання порівнянь у біометричній перевірці один до одного (1:1) для автентифікації

запропонованої особи та один до багатьох (1:N) для ідентифікації як зонд для пошуку в базі даних, щоб встановити, чи є якісь інші записи райдужної оболонки потенційної відповідності.

Рисунок 2.9 – Переваги та недоліки БІ за райдужною оболонкою ока

Четверте місце за популярністю використання згідно [12] займає метод БІ за рисунком вен (рис.2.4). Його частка на ринку – 6% [12]. Основні переваги та недоліки цього методу наведено на рис. 2.10. Метод розпізнавання за райдужною оболонкою ока є досить новим серед біометричних методів, широке застосування цього методу почалося близько 10 років тому, можливо саме тому його частка на ринку відносно мала. Але при цьому цей метод один з найбільш точних і найбезпечніших серед інших методів БІ [14].

Розташування вен на пальцях і руках утворює унікальний рисунок, за яким можна ідентифікувати людину. Цей візерунок вен фіксується шляхом освітлення джерела ближнього інфрачервоного (ІЧ) світла через палець чи руку або відбиття його від поверхні шкіри та запису зображення на камеру зарядженого пристрою. Кров у венах і капілярах поглинає ІЧ-проміння інакше, ніж навколишня м’язова тканина, і передає чіткі контури структур назад у

камеру. Цей процес сканування зазвичай швидкий (згідно [13] лише секунди в деяких програмах). Функції витягуються із зображення та зберігаються як цифровий шаблон. Процес реєстрації та перевірки однаковий і вимагає співпраці з особою, хоча контакт із ІЧ-сканером або камерою пристрою не потрібен.

Рисунок 2.10 – Переваги та недоліки БІ за рисунком вен

При застосуванні БІ за рисунком вен витрати на обробку є вищими, ніж у деяких інших методів БІ, але це може бути компенсовано в програмах, які потребують високого рівня гарантії ідентифікації, вищих рівнів точності, які забезпечують судинні біометричні системи. Рисунок вен не схильний до старіння, пошкодження, фізичної деградації або негативних факторів навколишнього середовища на відміну від рис обличчя або папілярних гребнів пальців і рук.

Безконтактна реєстрація та процедури верифікації роблять судинні біометричні системи придатними для ситуацій, які вимагають стерильних або суворо гігієнічних умов [13].

2.3 Динамічні методи БІ

Динамічні методи (рис. 2.11) будуються на особливостях, характерних для підсвідомих рухів особи у процесі відтворення будь-якої дії. Технології динамічної БІ складно використовувати, оскільки ці біометричні показники можуть суттєво змінюватись протягом життя людини. Крім того, при її використанні необхідно більше часу для проведення ідентифікації, оскільки потрібно зібрати обсяг даних, достатній для біометричної ідентифікації.

Рисунок 2.11 – Динамічні методи біометричної ідентифікації

Динамічні методи базуються на поведінковій біометрії. Поведінкова біометрія – це звички та схильності, які люди розвивають з часом, враховуючи їхню взаємодію з різними пристроями. Пов’язані методики, які використовуються для фіксації та оцінки біометричної поведінки, можуть бути надзвичайно ефективними для визначення того, чи правильна особа входить до облікового запису, чи поведінка особи відповідає звичайним моделям цієї особи на відміну від поведінки шахрая.

Зі збільшенням використання цифрових пристроїв і онлайн-транзакцій поведінкова біометрія стає важливим інструментом для компаній і організацій для зміцнення довіри та зменшення шахрайства. Динамічні методи перевірки включають динаміку натискання клавіш, аналіз пальців і дотиків, взаємодію миші та когнітивну біометрію.

Серед всіх динамічних методів, як видно з рис. 2.4, найбільш популярним є метод БІ за параметрами голосу, він займає п’яте місце і його частка на ринку – 6% [12]. Основні переваги та недоліки цього методу наведено на рис. 2.12.

Рисунок 2.12 – Переваги та недоліки БІ за параметрами голосу

Голос людини (його звук) є результатом поєднання відмінних фізичних характеристик (довжина голосових зв’язок, форма горла) і поведінкових характерних (акцент, тембр, гучність, висота, інтенсивність, динаміка). Людський голос створює довжину хвилі, яку можна виміряти.

Голос збирається та аналізується за допомогою програмного забезпечення, яке використовує методи штучного інтелекту та машинного

навчання для створення величезного масиву даних, отриманих за такими факторами, як модуляція мови, тони, акцент, частота тощо. Ці елементи дозволяють системі створювати еталонний шаблон голосу (відбиток голосу або модель голосу), який можна використовувати для ідентифікації мовця. Подібна технологія використовується, щоб дозволити пристроям розуміти, перекладати та взаємодіяти з голосовим командами, наприклад, під час розмови з розумними колонками, мобільними пристроями, побутовою технікою, віртуальними помічниками. Розпізнавання параметрів голосу можна використовувати для ідентифікації (1:N) і для автентифікації (1:1).

Процеси реєстрації та перевірки голосу, а також розпізнавання голосу можуть працювати в будь-якому середовищі, де немає надмірного шуму. Він особливо ефективний як дистанційно керована біометрія за допомогою електронних засобів зв'язку. Отже, він ліг в основу ряду різноманітних випадків використання, коли особистість мовців потрібно підтвердити, щоб вони могли запитувати послуги, здійснювати транзакції, видавати команди або записувати складну вербальну інформацію [13].

Одним з динамічних методів є ідентифікація осіб за стилем ходи, який використовується як біометрична перевірка один до одного (1:1) і як ідентифікація один до багатьох (1:N). У кожної людини свій спосіб ходьби і бігу. Такі біометричні показники, як загальна статура об'єкта, довжина та ширина кроку, швидкість руху, різні кути, утворені суглобами в тазостегнових, колінних і гомілковостопних суглобах, а також кути тулуба, стегон і стоп можна зафіксувати на камери для аналізу [13]. Особливості ходи можуть бути зафіксовані камерами на деякій відстані, крім того цей процес ненав'язливий і не вимагає співпраці особи. На жаль, ця технологія відноситься до таких, які можна зафіксувати на відстані, і тому потенційно може використовуватися для цілей спостереження без відома особи.

Серед динамічних методів сьогодні набуває все більшої популярності БІ за клавіатурним почерком. Ідентичність, діяльність і навіть продуктивність віддалених працівників можна відстежувати за допомогою їх використання клавіатури та запобігати несанкціонованому використанню шляхом аналізу натискань клавіш. Дії, пов'язані з набором тексту на клавіатурі, можна використовувати для ідентифікації особи, коли для порівняння буде записаний еталонний сеанс його набору тексту. Окремих операторів клавіатури можна відрізнити за такими характеристиками, як час, витрачений на вибір,

натискання та відпускання певних клавіш або послідовність клавіш, основну динаміку та ритм натискань клавіш, спритність кожної руки та типові помилки, що повторюються. Важливо відзначити, що змінні фактори можуть впливати на динаміку натискання клавіш і порушувати її, наприклад, втома, температура навколишнього середовища, поза, тип клавіатури тощо.

Біометрія натискання клавіш поєднується з іншими програмами безпеки або біометричними програмами для формування процедур багатофакторної автентифікації, які починають замінювати стандартні протоколи паролів у багатьох онлайн транзакціях і налаштуваннях робочого місця при віддаленій роботі.

2.4 Сфери застосування БІ

Сьогодні актуальними проблемами безпеки в інформаційних мережах є шахрайство з документами, крадіжки особистих даних, тероризм і кіберзлочинність, саме тому зараз відбуваються глобальні зміни законодавства та впроваджуються нові рішення безпеки, особливо біометричної. Підвищення популярності серед користувачів, суттєве підвищення точності, багата пропозиція та падіння цін на датчики, IP-камери та програмне забезпечення полегшують встановлення біометричних систем. Сьогодні багато програм використовують БІ.

Зручність швидкодоступних онлайн-сервісів є безцінною, а використання розумних речей стає все більш поширеним, але все це призводить до більшої потреби в надійній безпеці даних і конфіденційності в технології перевірки особи. Саме тому зростає ї роль біометричної ідентифікації в різних галузях.

Першими використання біометричних технологій ініціювали органи влади для контролю доступу військових та ідентифікації злочинців або цивільних осіб відповідно до жорстко регламентованої правової та технічної бази. Сьогодні такі сектори, як банківська справа, роздрібна торгівля та мобільна комерція, демонструють великий попит на біометричні технології.

За останні роки підвищилися обізнаність і визнання серед звичайних громадян. Сьогодні мільйони користувачів смартфонів розблоковують свої телефони за допомогою відбитка пальця або обличчя [10].

Компанії та державні органи все частіше сприяють цифровій трансформації суспільства, пропонуючи легкодоступні онлайн-послуги. Однак

для цього потрібна довіра кінцевих користувачів. Біометрія вже задовольняє цю вимогу, забезпечуючи як високий рівень безпеки, так і зручність у програмах. Вже сьогодні користувачі активно використовують біометрію в таких процедурах:

– підтвердження платежу (використання розпізнавання обличчя або відбитків пальців для автентифікації власника та підтвердження транзакції),

– подорож літаком (скорочення часу очікування на контрольно-пропускних пунктах в аеропорту, таких як реєстрація, служба безпеки, посадка тощо),

– доступ до різних приміщень (дозвіл доступу до офісів або конфіденційних місць),

– реєстрація в онлайн-сервісах (користувач може довести, ким він є у віртуальному контексті за допомогою свого мобільного пристрою),

– відкриття нових облікових записів онлайн (для конфіденційних послуг , які потребують підтвердження особи нового абонента),

– автентифікація водія та моніторинг поведінки для виявлення втоми, що підвищує безпеку,

– розслідування злочинів та встановлення потерпілих (швидке та надійне встановлення особи),

– доступ до логічної системи або моніторинг стану (за допомогою біометричних мозкових комп’ютерних інтерфейсів) [9].

Біометричні системи надзвичайно важливі та ефективні там, де ідентифікація та автентифікація є критичними. Сьогодні найбільш типовими сферами використання біометричних технологій є наступні:

– правоохоронні органи та громадська безпека (ідентифікація злочинців та підозрюваних),

– військові (ідентифікація противників та союзників),

– прикордонний, подорожній та міграційний контроль (ідентифікація мандрівників, мігрантів, пасажирів),

– цивільна ідентифікація (ідентифікація громадян, резидентів, виборців),

– охорона здоров’я та субсидії (ідентифікація пацієнтів, бенефіціарів, медичних працівників),

– фізичний і логічний доступ (ідентифікація власників, користувачів, працівників, підрядників, партнерів),

– комерційні програми (ідентифікація споживачів та клієнтів).

2.5 Перспективи розвитку біометричних технологій

У світі систем контролю доступу біометричні досягнення дозволяють застосовувати більш безпечні заходи ідентифікації та безперебійні процеси безпеки. Дослідження показало, що понад 80% смартфонів мають увімкнений біометричний захист, порівняно з 68% кілька років тому – лише ця статистика показує траєкторію біометричних рішень безпеки [15].

Біометричні технології безупинно розвиваються: зростає продуктивність існуючих методів, з’являються нові алгоритми для підвищення складності підробки, значно покращуються показники безпеки (рис. 2.13).

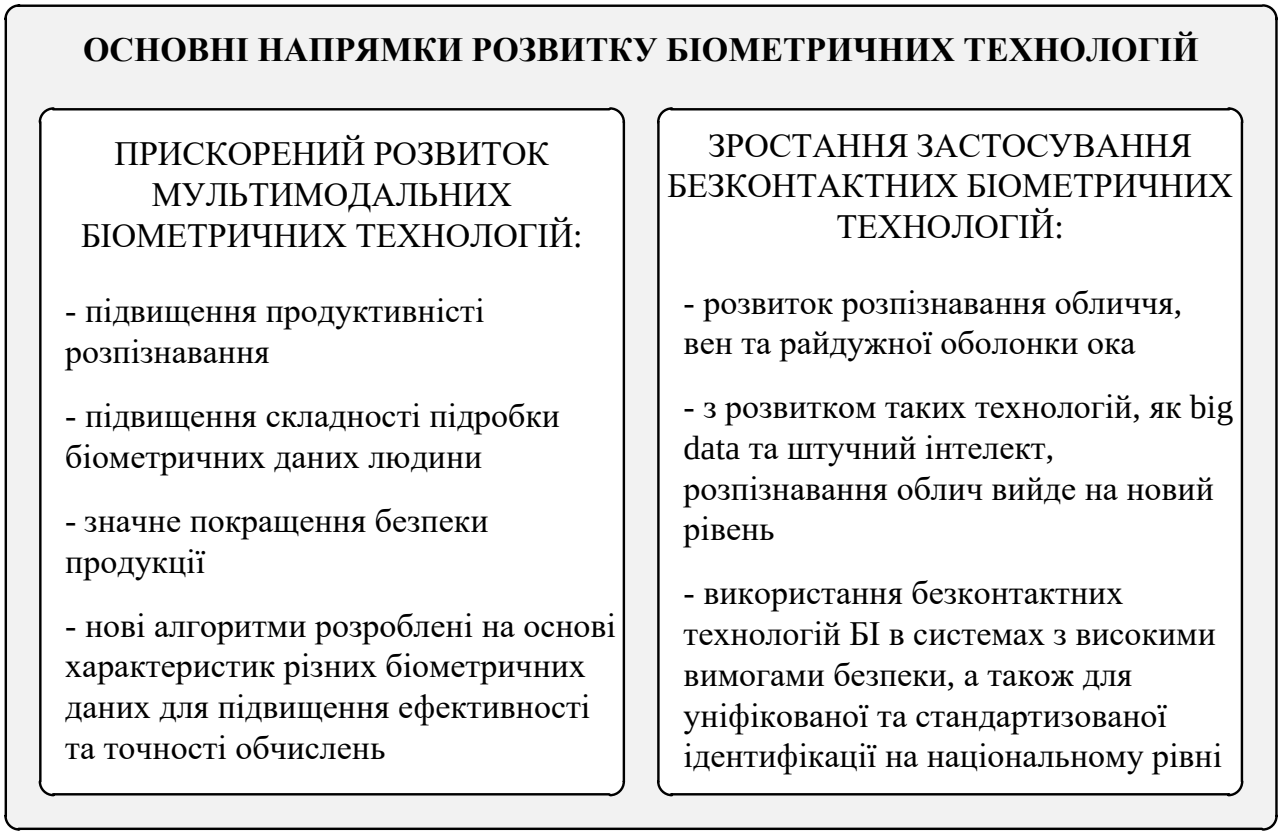


Рисунок 2.13 – Напрямки розвитку біометричних технологій

Основні тренди біометричних технологій 2022 – 2024 рр. [15 –18] представлені на рис. 2.14. Динаміку ринку біометричних систем згідно з прогнозом [17] наведено на рис. 2.15.

Рисунок 2.14 – Основні тренди біометричних технологій (2022 – 2024)

Важливим трендом є хмарна біометрія . Хмара запропонувала нові та інноваційні способи зберігання величезних обсягів даних. У поєднанні з біометрією ця тенденція дозволить фахівцям із безпеки відмовитися від виділеного сервера та зберігати дані в хмарі. Хмарна біометрія полегшує розпізнавання облич в реальному часі та інші заходи безпеки, що потребують інтенсивної обробки, а також дозволяє здійснювати дистанційний моніторинг, що стане необхідним у нову еру гібридної роботи.

Багатофакторна автентифікація поступово стає нормою. Вона вже сьогодні широко використовується для захисту облікових записів і є життєво важливою для безпеки контролю доступу. Багатофакторна автентифікація додає ще один рівень безпеки, поєднуючи традиційний пароль із розпізнаванням обличчя або відбитків пальців. Раніше цей підхід використовувався для дуже конфіденційних даних, але через зростання кількості кіберзлочинів незабаром його використовуватимуть повсюдно.

Рисунок 2.15 – Динаміка ринку біометричних систем

Набирає обертів безконтактна біометрія. Безконтактна біометрія в поєднанні з інтегрованими системами та алгоритмами дозволяє користувачам легко пересуватися без шкоди для безпеки. Наприклад, найновіші біометричні засоби можуть впустити попередньо авторизовану особу в приміщення, повідомити відповідних осіб про її прибуття, викликати ліфт, і все це без необхідності чогось торкатися.

Все більш популярноє стає етична біометрія. Користувачі дбають про безпеку і хочуть вірити в те, що їхні дані будуть захищені відповідно до законів про конфіденційність, а біометрична система, яку вони використовують, буде неупередженою. Цей новий стандарт для галузі стабільно зростає, але найближчі роки принесуть суворіші очікування щодо етичної безпеки [15].

Більше користувачів, ніж будь-коли, використовують цифрові ідентифікатори. Від звичайного цифрового гаманця на смартфоні до більш складних програм, що використовуються для контролю доступу, фізичні картки

відходять в минуле. Ця зміна вимагала (і вимагатиме й надалі) повного перегляду існуючої інфраструктури, щоб забезпечити нові форми ідентифікації.

Перелік перспективних біометричних технологій (рис. 2.16), які можуть бути використані в системах безпеки, постійно розширюється.

Рисунок 2.16 – Нові перспективні біометричні методи

Все частіше біометричні технології використовують в інфокомунікаціях, інформаційній безпеці, фінансових операціях, електронному уряді та багатьох інших сферах. Перспективні напрямки використання біометричних технологій представлені на рис. 2.17.

Спектр галузей, в яких застосовуються біометричні технології, великий і він постійно розширується. Сьогодні застосовують біометрію навіть при виробництві продуктів харчування та напоїв – цей бізнес також вимагає безпеки. При цьому біометричні дані можуть бути інтегровані для дистанційного відстеження рівнів доступу співробітників і дозволів, оскільки це мінімізує ризик. Крім того, він взагалі забороняє небажаним особам проникати на територію [17].

Рисунок 2.17 – Перспективні напрямки використання біометричних технологій

Таким чином, розвиток біометрії та БІ досить стрімкий. Завдяки останнім біометричним тенденціям безконтактні заходи безпеки стануть нормою. З прогресом у хмарній біометрії та цифрових ідентифікаторах новітні технології продовжуватимуть створювати нові та інноваційні рішення безпеки. Суворішими стають вимоги до етичної біометрії та конфіденційності даних. Всі ці новації та нові тенденції дадуть змогу вирішувати проблеми безпеки на новому високому рівні.

3 МУЛЬТИБІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ

3.1 Багатофакторна ідентифікація

У все більш взаємопов’язаному цифровому світі захист конфіденційної інформації та забезпечення безпечного доступу до онлайн-сервісів є надзвичайно важливими.

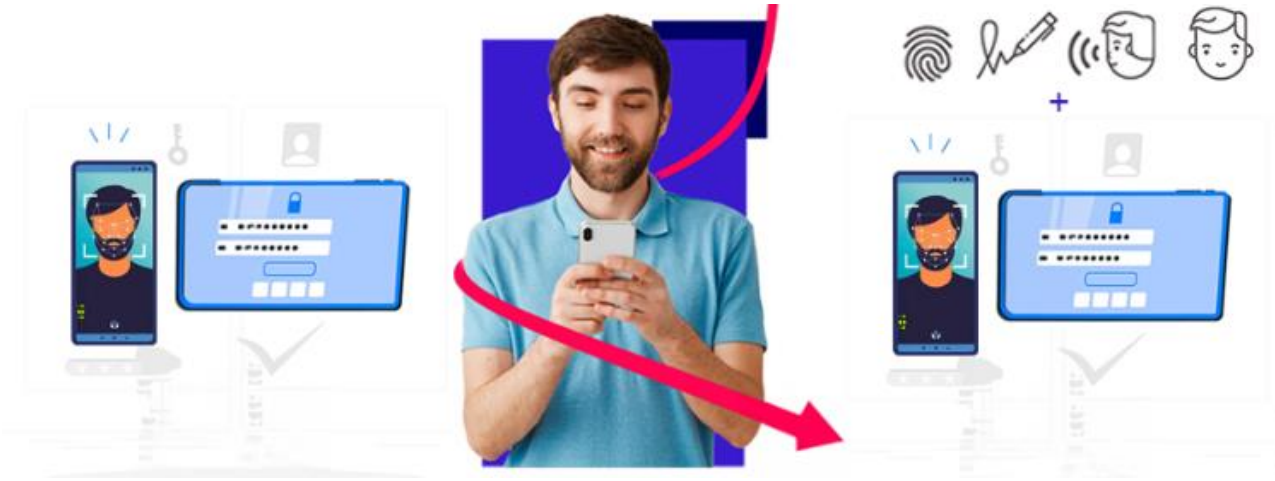
Традиційну ідентифікацію, при якій для розпізнавання особи застосовують один фактор автентифікації (наприклад пароль) називають однофакторною або слабкою, оскільки її надійність є не високою. За наявності певних ресурсів, перехоплення або підбір пароля є справою часу. Не останню роль в цьому грає людський чинник - чим стійкішим до злому методом підбору є пароль, тим його важче запам'ятати і тим вища ймовірність, що він буде додатково записаний, що підвищить ймовірність його перехоплення або викрадення. З іншого боку, легкі для запам'ятовування паролі (наприклад, часто вживані слова або фрази, дати народження, імена близьких, назви моніторів чи найближчого обладнання) в плані стійкості до злому є дуже слабкими. Як вихід, впроваджуються одноразові паролі, проте іхне перехоплення також можливе.

Саме тому, за необхідності, використовується сильна або багатофакторна ідентифікація. В цьому випадку використовується не лише інформація відома користувачеві, а й додаткові фактори. В наш час, коли кібератаки стають все складнішими і частішими, покладатися на один фактор автентифікацію ненадійно.

Багатофакторна ідентифікація/автентифікація (Multi Factor Authentication, MFA) – це протокол безпеки, який запроваджує додатковий рівень перевірки, крім звичайного імені користувача та пароля. Цей багатофакторний метод вимагає від користувача надання двох або більше доказів особистості для отриманя доступу і входу в обліковий запис. Тільки після введення всієї необхідної інформації користувач отримає доступ до облікового запису. Це може бути адреса електронної пошти, номер телефону, відповідь на якесь відоме лише користувачу секретне питання тощо.

Таким чином, багатофакторна ідентифікація/автентифікація – це система контролю доступу, яка потребує двох або більше методів ідентифікації з різних категорій, які перевіряють особу користувача для входу, що суттєво підвищує якість ідентифікації та є основним компонентом безпечної мережі [19]. Багатофакторний метод значно зменшує ймовірність віртуальних атак, які можуть бути причиною несанкціонованого доступу до конфіденційної інформації. Кожен додатковий фактор додає ще один рівень безпеки, оскільки хоча кіберзлочинець може скомпрометувати один фактор автентифікації, але значно складніше скомпрометувати два або більше одночасно [20].

Багатофакторний метод може об'єднувати будь-яку кількість факторів автентифікації, але найбільш популярним та розповсюдженим є двофакторна ідентифікація/автентифікація (2 Factor Authentication, 2FA). 2FA – ще один термін, який використовується для позначення того самого механізму безпеки, що й MFA, але при перевірці особи користувача вимагається від нього надати два різні докази або фактори (рис. 3.1).



Двофакторна ідентифікація / автентифікація (2FA)

Багатофакторна ідентифікація / автентифікація (MFA)

Рисунок 3.1 – Двофакторний та багатофактоний методи

В процесі двофакторної перевірки, користувач спочатку вводить свої початкові облікові дані (ім’я користувача та пароль) як перший фактор, а потім йому пропонується надати другий фактор, яким може бути біометрична перевірка, код, надісланий на мобільний пристрій, або фізичний маркер, який потрібно вставити. Двофакторна перевірка – це ефективний захід безпеки, який

допомагає зменшити ризики, пов’язані зі зломом пароля, фішинговими атаками та крадіжкою облікових даних [21].

Впровадження двофакторної ідентифікації із застосуванням найкращих практик може покращити безпеку системи, платформи чи служби, одночасно забезпечуючи позитивну та зручну взаємодію з користувачем.

Часто необхідність використання більше ніж 2 фактори може бути викликана невдалою ідентифікацією у 2FA або підозрілими діями передбачуваної особи. Це є можливим для систем 2FA, які мають можливість переходу до MFA. Це може також знадобитися для забезпечення додаткової безпеки при доступі до більш важливих файлів або конфіденційних даних (наприклад, фінансова інформація). Додаткові рівні безпеки в процесі входу в систему можуть забезпечити гарантію того, що особиста інформація користувачів залишиться захищеною і не потрапить до зловмисників.

3.2 Переваги та недоліки багатофакторної ідентифікації

Поєднуючи кілька факторів, багатофакторна перевірка особи значно посилює безпеку, оскільки зловмиснику потрібно володіти не лише паролем користувача, щоб отримати несанкціонований доступ. Навіть якщо один фактор скомпрометовано, додаткові фактори виступають як перешкода для запобігання шахрайству.

Важливо також зазначити, що на відміну від класичних факторів перевірки особи (знання, володіння та ознаки), що наведено на рис.1.3, в багатофакторній ідентифікації також додатково може використовуватися ще один фактор – фактор місцезнаходження (розташування користувача). Це може бути діапазон IP-адрес джерела або геолокація. Цей фактор передбачає встановлення місцезнаходження користувача в обліковому записі та його перевірку за допомогою GPS. У разі будь-яких розбіжностей доступ до облікового запису не надається [22]. Деякі програми та служби вимагають, щоб користувач перебував у певному місці, щоб отримати до них доступ [20]. Звичайно використовувати цей фактор варто виключно разом із іншими більш безпечними факторами для підвищення рівня захисту.

Багатофакторна ідентифікація має багато переваг [19, 22]. Додавання іншої форми ідентифікації (мобільної, біометричної, фізичної чи ін.) створює багатошаровий захист. Крім того, цей протокол безпеки створює захист, що

відповідає сучасним нормативним вимогам. З одного боку, це позбавляє організацію від штрафів, що виникають через порушення правил безпеки, а з іншого – це захищає апаратні та програмні системи організації від вторгнення. Звичайно окрім переваг, багатофакторний метод має і деякі недоліки. Основні переваги та недоліки MFA наведено на рис. 3.2.

Рисунок 3.2 – Переваги та недоліки багатофакторної ідентифікації

Багатофакторний метод стає все більш популярним та широко застосовується різними онлайн-платформами, банківськими установами, постачальниками електронної пошти та іншими службами, які надають пріоритет безпеці. Він забезпечує ефективний засіб захисту облікових записів користувачів і конфіденційної інформації, знижуючи ризик крадіжки особистих даних, витоку даних та інших інцидентів безпеки [21].

3.3 Використання біометрії в багатофакторній ідентифікації

Однофакторні перевірки, які раніше вважалися достатніми, стають дедалі вразливішими до злому та атак. У результаті інтеграція багатофакторної ідентифікації/автентифікації набула популярності, а біометрія стала ідеальним поєднанням для підвищення безпеки в MFA. Біометрія пропонує кілька переваг, які роблять її ідеальною для підвищення безпеки онлайн-облікових записів і служб [21]: унікальність і невід'ємна безпека, зручність і досвід користувача, покращена стійкість до атак, постійна автентифікація та присутність користувача, інтеграція з існуючими пристроями, конфіденційність і відповідність вимогам.

Біометричні ознаки за своєю суттю є унікальними для різних людей. На відміну від паролів або токенів, які можна забути, втратити або вкрасти, біометричні характеристики важко відтворити або підробити. Використання біометрії як одного з факторів у процесі MFA додає додатковий рівень безпеки, прив'язуючи автентифікацію до фізичних атрибутів особи.

Біометричні методи пропонують бездоганний і зручний досвід. Користувачі можуть ідентифікувати себе, просто надавши сканування відбитків пальців, розпізнавання обличчя або зразок голосу для перевірки за допомогою голосової біометрії.

У порівнянні із запам'ятовуванням і введенням паролів або носінням фізичних маркерів, біометрія спрощує процес перевірки та усуває клопоти, пов'язані з традиційними методами. Ця зручність заохочує ширше впровадження MFA та зменшує опір користувачів щодо впровадження додаткових заходів безпеки.

Біометрія забезпечує підвищену стійкість до різних векторів атак. Біометричні характеристики важко вгадати або відтворити, що зменшує ймовірність успішних атак грубою силою. Крім того, біометричні системи часто використовують розширені алгоритми для виявлення та запобігання спробам спуфінгу, таким як представлення зміненого зображення обличчя. Ці заходи посилюють загальну безпеку процесу MFA, захищаючи облікові записи користувачів від шахрайського доступу [21].

Біометрична ідентифікація може полегшити постійну перевірку користувача протягом сеансу. Наприклад, на пристроях, оснащених сканерами відбитків пальців або камерами для розпізнавання обличчя, користувачам може

періодично пропонуватися ідентифікуватися, гарантуючи, що схвалений користувач залишається присутнім протягом усього сеансу.

Біометричні технології стають все більш повсюдними в сучасних пристроях, включаючи смартфони, планшети та ноутбуки. Використання цих вбудованих біометричних датчиків або камер для MFA усуває потребу в додаткових апаратних пристроях. Користувачі можуть використовувати біометричні можливості своїх існуючих пристроїв, роблячи впровадження MFA більш зручним і економічно ефективним.

Біометричні дані можуть запропонувати додатковий рівень конфіденційності порівняно з традиційними методами ідентифікації. Хоча паролі можна перехопити або вкрасти, біометричні дані зазвичай зберігаються локально на пристрої користувача або надійно зашифровані на серверах, мінімізуючи ризик розголошення. Крім того, біометрична ідентифікація узгоджується з правилами конфіденційності, оскільки біометричні шаблони, які використовуються для перевірки, є незворотними [21].

Таким чином, у еволюції цифрової безпеки інтеграція багатофакторної перевірки особи з біометричними даними виявляється ідеальним поєднанням. Унікальні характеристики біометричних характеристик у поєднанні зі зручністю, підвищеною стійкістю до атак і покращеним користувальницьким досвідом позиціонують біометрію як сильний і безпечний компонент у процесі MFA.

Використовуючи внутрішні сильні сторони біометрії, компанії та організації можуть підвищити безпеку своїх систем, захистити облікові записи користувачів і зміцнити довіру у все більш цифровому світі.

Таким чином, біометрія стає важливим компонентом процесів багатофакторної ідентифікації/автентифікації, відіграючи вирішальну роль у захисті цифрової ідентифікації.

3.4 Мультибіометрична ідентифікація

Система ідентифікації з одним біометричним фактором може бути недостатньою для відповідного застосування з точки зору таких властивостей, як універсальність, відмінність, прийнятність тощо. Однофакторним біометричним системам бракує операційних переваг, що стосуються продуктивності та точності [23]. Стовідсоткова точність може бути недоступна

в однофакторних системах через такі обмеження, як шум в датчикак, варіації всередині класу, подібність між класами, відсутність універсальності, проблеми взаємодії, атаки підробки та інші вразливості. Мультифакторна або мультимодальна біометрична система або мультибіометрична система – це удосконалена система, яка включає заходи для усунення недоліків, які виникають в однофакторній біометричній системі.

Мультимодальна біометрія – це система, яка поєднує результати, отримані з більш ніж однієї біометричної ознаки з метою ідентифікації особи [23 – 27]. Мультибіометричні системи більш надійні, оскільки використовується багато незалежних біометричних факторів. Використання кількох біометричних факторів може призвести до високоточної та безпечної системи біометричної ідентифікації, оскільки унімодальна біометрична система може не забезпечити точну ідентифікацію через неуніверсальність. Наприклад, оскільки деякий відсоток людей може мати потерті, порізані або невпізнані відбитки, біометрія відбитків пальців може дати помилкові результати. У мультимодальних біометричних системах збій будь-якої однієї технології може серйозно не вплинути на індивідуальну ідентифікацію, оскільки можна успішно використовувати інші технології [23]. Отже, спуфінг можна суттєво мінімізувати; тим самим підвищуючи ефективність всієї системи. Зменшення рівня невдач для зарахування у мультимодальному оцінюванні є дуже значним, і це є однією з головних переваг цієї системи.

Загальна біометрична система в основному включає наступні основні модулі:

– сенсорний модуль (модуль датчика),

– модуль вилучення ознак,

– модуль відповідності,

– модуль прийняття рішень.

У сенсорному модулі потрібен відповідний інтерфейс користувача, що містить біометричний датчик або сканер, щоб вимірювати або записувати вихідні біометричні дані користувача. Ці необроблені біометричні дані збираються, а потім передаються в наступний модуль для вилучення ознак. Конструкція сенсорного модуля впливає на різні фактори, такі як вартість і розмір.

У модулі вилучення ознак спочатку оцінюється якість отриманих біометричних даних від датчика для подальшої обробки. Таким чином

генерується орієнтовне цифрове представлення базових рис або факторів. Після виділення ознак вони передаються як вхідні дані до відповідного модуля для подальшого порівняння.

Порівняння отриманих функцій із шаблонами в базі даних дає оцінку відповідності. Цей результат відповідності може контролюватися якістю наданих біометричних даних. Модуль відповідності генерує оцінку відповідності і використовується для підтвердження заявленої особи.

Модуль прийняття рішень визначає, чи є користувач справжнім користувачем чи самозванцем на основі результатів відповідності. Вони використовуються або для підтвердження ідентичності особи, або для визначення рейтингу зареєстрованих ідентифікацій для визначення особи.

Послідовність робочих процедур системи мультибіометричної ідентифікації (МБІ) наведено на рис. 3.3.

Алгоритм мультибіометричної ідентифікації складається з наступних етапів:

– спочатку зразок біометричних характеристик фіксується у користувача, коли користувач хоче отримати доступ,

– отримані біометричні дані проходять попередню обробку, яка включає видалення небажаних даних, шуму та виділення помітної ознаки, за якою потрібно розпізнати особу,

– вилучену функцію порівнюють із зареєстрованими зразками, які зберігаються в базі даних, щоб переконатися, що обидва зразки мають подібність,

– зареєстрований зразок і взятий зразок порівнюються під різними кутами з використанням деяких визначених алгоритмів, і відображається точність відповідності;

– на підставі рівня точності приймається рішення, справжній користувач чи самозванець.

– якщо одна біометрична система забезпечує точність недостатню для прийняття будь-якого рішення, використовується інша система з іншою біометричною функцією для виконання тієї ж процедури,

– кінцеві результати, отримані від усіх підсистем, масштабуються та перетворюються у загальний формат, а рішення відображається на екрані.

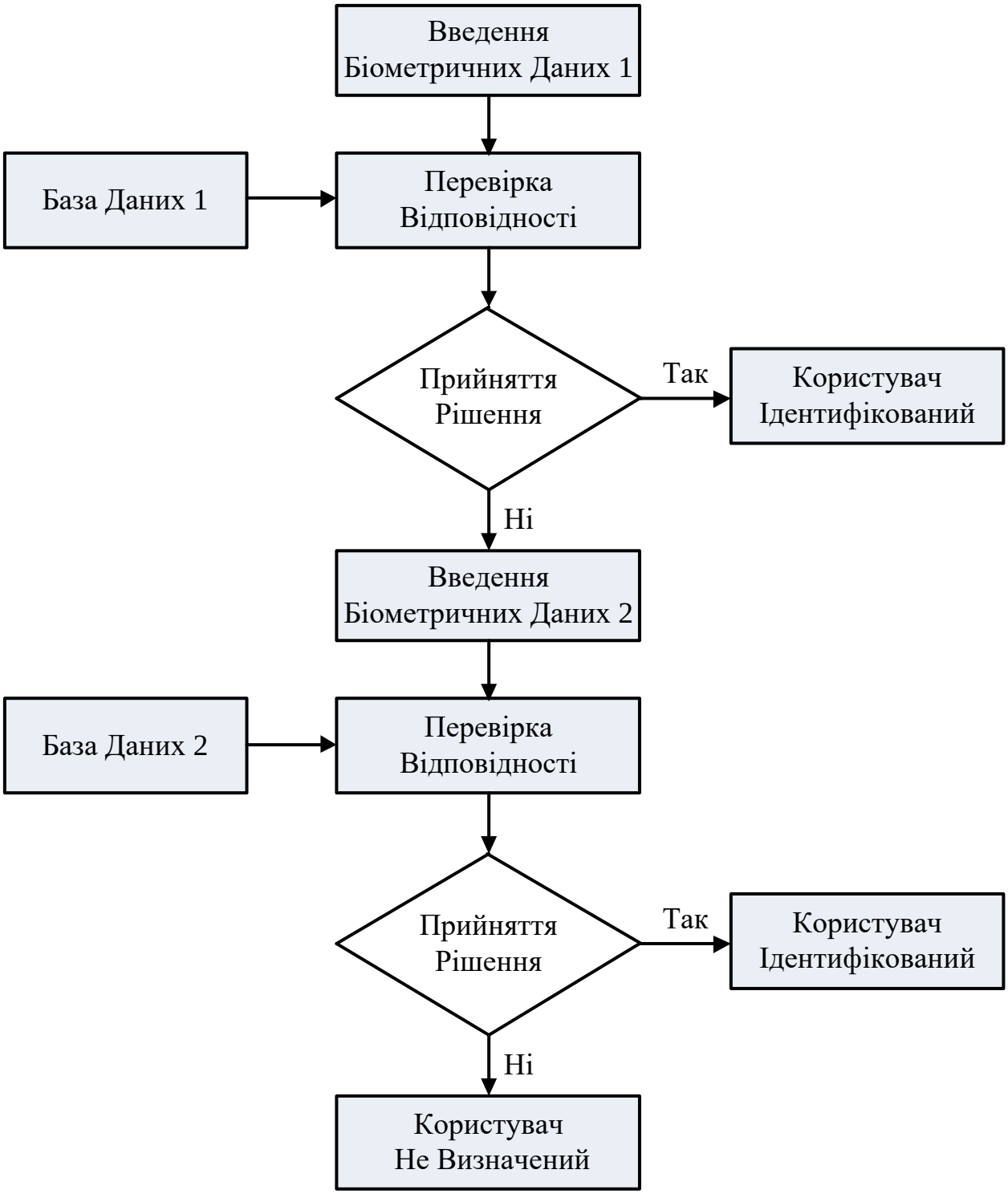


Рисунок 3.3 – Блок-схема алгоритму мультибіометричної ідентифікації

Існує два основних режими роботи в мультибіометричних системах:

– послідовний режим,

– паралельний режими.

У послідовному режимі роботи кілька джерел інформації отримуються не одночасно, тобто користувач проходить поетапний процес ідентифікації

(рис. 3.3). Таким чином, час розпізнавання зменшується в послідовному режимі, оскільки рішення приймається до отримання всіх ознак.

У випадку паралельного режиму роботи розпізнавання здійснюється шляхом одночасного отримання кількох джерел інформації. Це призведе до зниження ефективності системи та, у свою чергу, створить незручності для користувача.

Обидва способи роботи мають свої переваги та недоліки. Дослідження показують, що комбіноване використання обох режимів може привести до системи, яка забезпечує високу ефективність і зручність користувача [23].

При паралельному режимі, використовуючи інформацію, доступну в будь-якому з модулів, можна розробити об’єднання в багатомодальній біометричній системі. Різні біометричні ідентифікатори, що використовуються в мультимодальній біометричній системі, їх інформація з індивідуального ідентифікатора береться разом і може бути об’єднана на різних рівнях об’єднання, наприклад об’єднання на рівні датчика, об’єднання на рівні ознак, об’єднання на рівні оцінки відповідності та об’єднання на рівні рішення.

Мета розробки мультибіометричної системи полягає в тому, щоб розробити ефективну схему злиття біометричних даних для консолідації численних доказів для прийняття рішення щодо ідентифікації особи.

В залежності від того які біометричні ознаки об’єдніються для ідентифікації особи, мультибіометричні ситеми бувають:

– мультибіометричні системи на основі фізіологічних особливостей (використовують для ідентифікації особи комбінацію двох або більше фізіологічних ознак),

– мультибіометричні системи на основі поведінкових особливостей (використовують для ідентифікації особи комбінацію двох або більше поведінкових ознак),

– мультибіометричні системи на основі комбінаційних характеристик (для ідентифікації особи об’єднують разом фізіологічні та поведінкові ознаки) [24].

Мультибіометрія використовіє декілька джерел біометричної інформації для встановлення ідентичності особи. Мультибіометричні системи поєднують біометричні докази, надані декількома:

– біометричними датчиками (наприклад, 2D і 3D датчиками обличчя),

– алгоритмами (наприклад, збіги відбитків пальців на основі дрібниць і хребтів),

– зразками (наприклад, фронтальні зображення обличчя та зображення обличчя),

– одиницями (наприклад, ліва та права райдужка) або

– ознаками (наприклад, обличчя та райдужка) для підвищення точності розпізнавання біометричної системи.

В залежності від ознак, датчиків і наборів функцій існує багато різних типів мультибіометричних систем:

– одна біометрична ознака та кілька датчиків (однакові біометричні характеристики реєструються за допомогою кількох датчиків, а дані, отримані з різних датчиків, об’єднуються на рівні функції або на рівні відповідності, щоб покращити продуктивність системи);

– декілька біометричних ознак (об’єднують декілька біометричних ознак, а для захоплення вибірки кожної біометричної характеристики використовуються різні датчики);

– декілька одиниць одних і тих самих біометричних ознак (два чи більше двох пальців одного користувача можна використовувати як біометричну ознаку, це недорогий спосіб покращити продуктивність системи, оскільки не вимагає кількох датчиків або включення додаткових функцій модулів вилучення або відповідності);

– декілька знімків однієї біометрії (у цьому випадку для розпізнавання використовується більше ніж один екземпляр тієї самої біометрії, як-от кілька відбитків одного пальця або кілька зразків голосу, які фіксуються для ідентифікації особи);

– декілька алгоритмів відповідності для тієї самої біометрії (для виділення ознак і відповідності біометричних характеристик можна застосовувати різні методи) [27].

Таким чином, різноманітні методи мультибіометрії підвищують точність та надійність ідентифікації особи, додаючи високий рівень безпеки.

4 ВИБІР ОПТИМАЛЬНОГО МЕТОДУ МУЛЬТИБІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Дослідження ефективності методів БІ є важливими з різних причин:

1) дослідники досягли значного прогресу в біометричних системах за останні кілька десятиліть, але належних досліджень у сфері оцінки ефективності недостатньо [28];

2) при вирішенні реальних задач для розгортання та використання методів БІ потрібні точні та надійні показники оцінки ефективності;

3) поки що не існує узгодженого підходу для оцінки та порівняння різних біометричних систем, а також для звітування про показники, крім того, багато широко використовуваних одночислових метрик, що використовуються в цій галузі, мають очевидні недоліки та обмежені області [28];

4) методи ідентифікації на основі біометрії швидко змінюються і такі питання, як активні супротивники та вроджені упередження, а також справедливість, вимагають додаткових досліджень у цій галузі.

Саме тому важливими та перспективними є дослідження ефективності методів БІ, а також надійності, контексту використання, сильних та слабких сторін важливих показників оцінювання та інших впливових параметрів.

Вибір оптимального методу БІ серед існуючих є актуальним завданням та суттєво залежить від специфіки галузі, в якій він застосовується. Активний розвиток біометрії робить проблему оптимального вибору методу БІ досить складною і для компаній, і для користувачів. Навіть при всій унікальності біометричних ознак ці методи ідентифікують особу лише з певною ймовірністю і не дозволяють стовідсотково ідентифікувати одного користувача з великої кількості інших без додаткових способів ідентифікації.

4.1 Показники оцінки ефективності методів БІ

Для оцінки ефективності біометричних методів використовують велику кількість параметрів (табл. 4.1). Використовуючи таку сукупність показників якості, можна досить точно оцінити різні методи БІ, порівняти їх та обрати метод, що максимально відповідає вимогам певної системи захисту.

Таблиця 4.1 – Показники якості біометричних методів ідентифікації

Показник якості	Зміст
FMR (False Match Rate) – коефіцієнт помилкових збігів	частка спроб незаконних користувачів, які помилково визнані відповідними шаблону або ймовірність помилкового співпадіння параметрів
FNMR (False Non-Match Rate) - коефіцієнт помилкових невідповідностей	частка спроб законного користувача, які помилково визначені невідповідними шаблону особи або ймовірність помилкового неспівпадіння параметрів
FAR (False Acceptance Rate) – коефіцієнт помилкового прийняття	відсоток випадків неправильної ідентифікації, коли система дозволяє доступ незаконному користувачу
FRR (False Rejection Rate) – коефіцієнт помилкових відхилень	відсоток випадків неправильної ідентифікації, коли законному користувачу було відмовлено або ймовірність відмови доступу людині, яка має допуск
FER (Failure-to-Enrol Rate) – коефіцієнт відмови в реєстрації	відсоток невдалих спроб створення шаблону із введених даних через їхню низьку якість
ERR(Erronous Retention Rate) – помилковий коефіцієнт утримання	ймовірність того, що автоматизована система не зможе визначити, коли біометричні дані представлені правильно
FPR (False Positive Rate) – коефіцієнт помилково позитивних результатів	ймовірність авторизації незаконного користувача
FNR (False Negative Rate) – коефіцієнт помилково негативних результатів	ймовірність відмови законному користувачеві
Рівень безпеки	точність та надійність ідентифікації особи
Розмір даних	параметр, що характеризує обсяг ресурсів, необхідних для обробки даних
Вартість	загальна вартість обладнання та організації процесу ідентифікації

Продовження таблиці 4.1

Показник якості	Зміст
Універсальність	наявність у кожної людини даної біометричної характеристики
Унікальність	гарантія того, що немає двох ідентичних осіб з точки зору даної біометричної ознаки
Постійність	незмінність характеристики з часом (біометрична ознака має бути максимально незмінною протягом певного періоду часу)
Продуктивність	це властивість, спрямована на оцінку точності ідентифікації і часу обчислення, необхідного для одного розпізнавання, а також операційних факторів, які можуть впливати на них
Прийнятність	готовність користувачів без заперечень надавати ці біометричні дані
Стійкість до фальсифікації	ступінь складності фальсифікації чи підробки цієї біометричної ознаки
Чутливість	ступінь чутливості до впливу зовнішніх факторів
Швидкість	швидкість виконання процедури перевірки особи
Безконтактність	відсутність необхідності безпосереднього контакту користувача зі сканером
Комфорт користувача	легкість вимірювання без будь-яких незручностей для користувача
Ймовірність помилки	загальна ймовірність помилкового прийняття або помилкового відхилення (сумарна ймовірність помилок I та II роду)

За своєю суттю біометрична система може допускати два основні типи помилок: помилковий збіг і помилкова невідповідність.

У контексті біометричної ідентифікації FNMR і FMR зазвичай називають частотою помилкових відхилень (FRR) і частотою помилкових прийомів (FAR) відповідно. Однак вони мають різницю. FMR і FNMR еквівалентні FAR і FRR

відповідно в тому випадку, коли система використовує одну спробу користувача зіставити збережений шаблон. Таким чином, у системах ідентифікації FAR і FRR часто використовуються для заміни FMR і FNMR.

Коефіцієнт помилкових позитивних результатів (FPR) – це ймовірність авторизації самозванця. Коефіцієнт помилково негативних результатів (FNR) – це ймовірність відмови законному користувачеві. FPR часто називають частотою помилкових прийомів (FAR), а FNR називають частотою помилкових відхилень (FRR). Це є дві основні помилки, які може зробити система ідентифікації [28]. Пара (FAR, FRR) є основним показником для оцінки продуктивності метеду БІ. Розрахунок параметрів FAR і FRR можна виконати за наступними співвідношеннями:

$$FAR = FPR = \frac{FR}{FP + TN}\ , \tag{4.1}$$

$$FRR = FNR = \frac{FN}{TP + FN}\ , \tag{4.2}$$

де TP – це авторизація законного користувача (true positive, TP),
FP – це авторизація незаконного користувача (false positive, FP),
TN – це відмова незаконному користувачу (true negative, TN),
FN – це відмова законному користувачу (false negative, FN).

4.2 Вибір оптимального методу БІ

Для виконання порівняння було обрано найбільш популярні за даними [12] методи БІ (рис.2.4): БІ за відбитком пальця (ВП), БІ за геометрією обличчя (ГО), БІ за райдужною оболонкою ока (РО), БІ за розташуванням вен (РВ) та БІ за параметрами голосу (ПГ). В результаті опрацювання великої кількості сучасних джерел, зокрема [8, 28 – 31] були визначені значення показників якості цих методів. Результати порівняння наведено в табл. 4.2. та 4.3.

Значення FAR і FRR розраховують за формулами (4.1) та (4.2) з використанням методів математичної статистики. Значення цих характеристик залежать від сканера, що використовується для зчитування біометричної

ознаки, тому в різних джерелах значення FAR і FRR можуть відрізнятися. В табл.4.2 представлено середні значення показників надійності.

Таблиця 4.2 – Порівняння методів БІ за показниками надійності

№	Метод БІ	FAR, %	FRR, %	Ймовірність помилки	Надійність
1	ВП	0,001	0,6	1/1000	Середня
2	ГО (2D)	0,1	2,5	1/100	Низька
3	ГО (3D)	0,005	0,1	1/500	Середня
4	РО	0,00001	0,016	1/1200000	Висока
5	РВ	0,0008	0,01	1/1100000	Висока
6	ПГ	0,1	6	1/30	Низька

Для виконання порівняння було обрано наступні показники якості: рівень безпеки, розмір даних, вартість, універсальність, унікальність, постійність, продуктивність, прийнятність, стійкість до фальсифікації, чутливість, швидкість, безконтактність, комфорт користувача та ймовірність помилки.

В джерелах [8, 28 – 31] значення параметрів, за якими оцінюють методи БІ, визначаються поняттями «високий», «середній» і «низький», або «ймовірно», «малоймовірно» і «неймовірно». В даній роботі всі значення параметрів формалізовані в оцінки показників якості, що мають числові значення від 1 до 3, де 1 – низький, а 3 – високий.

Для приведення оцінок показників якості до стандартного вигляду було виконано інвертування оцінок тих параметрів, які для покращення системи потрібно мінімізувати (а саме: розмір даних, вартість, чутливість та ймовірність помилки). Наприклад, ймовірність помилки була також оцінена за 3 бальною шкалою, але оцінки були інвертовані, таким чином 3 – мінімальне значення ймовірності помилки, а 1 – максимальне (талб. 4.3).

За безумовним критерієм переваги всі системи виявилися Парето-оптимальними, що не дивно враховуючи велику кількість показників якості.

Для вибору єдиного оптимального методу БІ з множини Парето було використано метод заснований на побудові скалярної функції цінності, максимізація якої дозволить визначити оптимальний варіант. В якості додаткової інформації для побудови умовного критерію переваги задані

коефіцієнти відносної важливості кожного з показників якості c_j (табл.4.3).

Для вибору єдиного варіанту з підмножини Парето було використано умовний критерій переваги, що базується на максимізації скалярної цільової функції у вигляді:

$$F(k_1,k_2,...,k_m)=\sum_{j=1}^{m}c_j k_j, \qquad (4.3)$$

де c_j - коефіцієнти відносної важливості показників якості, причому $\sum_{j=1}^{m}c_j=1$,

k_j - оцінки показників якості.

Розрахунок значень скалярної цільової функції для кожного варіанту виконано згідно (4.3) та результати представлено в табл. 4.3.

Таблиця 4.3 – Порівняння методів біометричної ідентифікації

№	Показники якості	Методи БІ					c_j
		ВП	ГО	РО	РВ	ПГ	
1	Рівень безпеки	2	1	3	3	1	0,15
2	Розмір даних (min)	3	1	1	2	3	0,05
3	Вартість (min)	3	2	1	1	2	0,05
4	Універсальність	2	3	3	3	2	0,05
5	Унікальність	3	1	3	3	1	0,05
6	Постійність	3	2	3	2	1	0,05
7	Продуктивність	3	1	3	3	1	0,05
8	Прийнятність	2	3	1	2	3	0,05
9	Стійкість до фальсифікації	1	1	3	3	1	0,05
10	Чутливість (min)	1	3	2	2	3	0,05
11	Швидкість	3	1	3	3	3	0,05
12	Безконтактність	1	2	3	2	3	0,05
13	Комфорт користувача	2	2	3	2	3	0,15
14	Ймовірність помилки (min)	2	2	3	3	1	0,15
$F(k_1,k_2,...,k_{14})$		2,15	1,75	2,65	2,5	1,9	$\sum c_j=1$

В результаті багатокритеріального аналізу найбільш популярних методів БІ (табл. 4.3), можна зробити наступні висновки. Мінімальною оцінкою, яку можна було отримати використовуючи 3-бальну систему оцінювання та приведення до сумарного скалярного значення, є 1, а максимальною – 3. З табл. 4.3 видно, що систем, які б мали мінімальні або максимальні оцінки немає. При цьому, всі методи мають достатньо високі значення скалярної оцінки і не дуже сильно відрізняються між собою.

Найбільше значення скалярної оцінки (2,65) отримав метод БІ за райдужною оболонкою ока, тому цей метод є оптимальним з урахуванням сукупності показників якості. Але варто відмітити, що метод БІ за розпізнаванням вен також має досить високу оцінку (2,5), що говорить про його високу загальну ефективність.

На жаль, жоден із розглянутих методів не дає повної гарантії коректної ідентифікації/автентифікації, тому за можливості бажано використовувати не один метод, а комбінувати декілька (тобто використовувати мульти-біометричнні методи).

4.3 Вибір оптимального методу мультибіометричної ідентифікації

Через обмеження систем ідентифікації, що використовують одну біометричну ознаку, сьогодні багато користувачів вдаються до мультибіометричної системи для забезпечення максимального рівню точності ідентифікації [23 – 28]. Ефективність переваг сукупності біометричних характеристик використовується для підвищення продуктивності в багатьох аспектах, включаючи точність, шумостійкість і універсальність, підробку атак і зниження продуктивності у великих програмах баз даних. У наш час з’являються нові алгоритми та застосування мультимодальної біометрії. В рамках мультибіометричних систем в поєднанні з іншими ознаками найбільш часто використовуються геометрія обличчя та відбитки пальців.

Різні дослідники запропонували такі комбінації ознак [23]: відбитки пальців + райдужна оболонка ока, відбитки пальців + рисунок вен, відбитки пальців + видбиток долоні, геометрія обличчя + відбитки пальців, геометрія обличчя + райдужна оболонка ока, геометрія обличчя + рисунок вен та інші комбінації.

В даній роботі виконано багатокритеріальний аналіз методів БІ, що використовують такі комбінації біометричних ознак: ВП+ГО, ВП+РО, ВП+РВ, ВП+ПГ, ГО+РО та ГО+РВ. Значенням оцінки кожного показника є сума значень оцінки показників кожної складової (з табл. 4.3).

За безумовним критерієм переваги всі системи є Парето-оптимальними. Для вибору єдиного оптимального методу БІ з множини Парето було використано метод заснований на побудові скалярної функції цінності, максимізація якої дозволить визначити оптимальний варіант. Особливу увагу було приділено заданню коефіцієнтів відносної важливості кожного з показників якості (табл. 4.4). В мультибіометричній системі такі показники як вартість, швидкість та комфорт користувача є особливо важливими, тому вони мають найбільш високі значення коефіцієнтів відносної важливості.

Таблиця 4.4 – Порівняння методів мультибіометричної ідентифікації

№	Показники якості	Методи мультибіометричної ідентифікації						Cj
		ВП+ГО	ВП+РО	ВП+РВ	ВП+ПГ	ГО+РО	ГО+РВ	
1	Рівень безпеки	3	5	5	3	4	4	0,08
2	Розмір даних (min)	4	4	5	6	2	3	0,08
3	Вартість (min)	5	4	4	5	3	3	0,2
4	Універсальність	5	5	5	4	6	6	0,02
5	Унікальність	4	6	6	4	4	4	0,02
6	Постійність	5	6	5	4	5	4	0,02
7	Продуктивність	4	6	6	4	4	4	0,02
8	Прийнятність	5	3	4	5	4	5	0,02
9	Стійкість до фальсифікації	2	4	4	2	4	4	0,02
10	Чутливість (min)	4	3	3	4	5	5	0,02
11	Швидкість	4	6	6	6	4	4	0,2
12	Безконтактність	3	4	3	4	5	4	0,07
13	Комфорт користувача	4	5	4	5	5	4	0,15
14	Ймовірність помилки (min)	4	5	5	3	5	5	0,08
$F(k_1, k_2, ..., k_{14})$		4,07	4,81	4,67	4,73	4,02	3,88	$\sum c_j = 1$

Для вибору оптимального варіанту було використано умовний критерій переваги, що базується на максимізації скалярної цільової функції. Розрахунок значень скалярної цільової функції для кожного варіанту виконано згідно (4.3) та результати представлено в табл. 4.4.

В результаті багатокритеріального аналізу деяких методів мультибіометричної ідентифікації (табл. 4.4), можна зробити наступні висновки. Найбільше значення скалярної оцінки (4,73) отримав метод, що для ідентифікації користувача використовуватиме комбінацію таких біометричних ознак «відбиток пальців + райдужна оболонка ока», тому він є оптимальним серед розглянутих. Але варто зазначити, що метод МБІ, що використовує комбінацію «відбиток пальців + голос» має досить високу оцінку (4,73) і при інших коефіцієнтах відносної важливості може бути оптимальним.

ВИСНОВКИ

Зі стрімким зростанням розвитку цифрових технологій зростає кількість та якість проблем безпеки, зокрема кількість крадіжок особистих даних, шахрайства, ризик втрати, розголошення або пошкодження конфеденційної інформації. Методи, розроблені для захисту інформації раніше, втрачають свою ефективність та потребують вдосконалення.

Сьогодні в системах безпеки широко використовується біометрія, яка надає ефективний захист інформації, оскільки біометричні ознаки не можна забути, загубити, вкрасти або підробити. Банківська справа, фінанси, домашня безпека, охорона здоров'я, комерція, державні організації активно застосовують біометричні методи захисту.

В найбільш важливих системах для підвищення точності, надійності та ефективності захисту, доцільно використовувати мультибіометричну ідентифікацію, що заснована на застосуванні двох або більше біометричних ознак.

В роботі було розглянуто та проаналізовано ряд питань, що стосуються біометричних та мультибіометричних методів ідентифікації осіб.

В першому розділі виконано огляд процесу верифікації користувача в мережі, розглянуто етапи верифікації, фактори автентифікації, а також різні види ідентифікації, їх особливості, переваги та недоліки.

В другому розділі проаналізовано процеси ідентифікації та автентифікації осіб на основі біометрії. Виконано аналіз статичних та динамічних методів БІ, розглянуто сфери застосування БІ та перспективи розвитку біометричних технологій.

Третій розділ присвячено дослідженню багатофакторної ідентифікації. Розглянуто переваги та недоліки БФІ. Особливу увагу приділено використанню біометрії в БФІ та мультибіометричним методам ідентифікації осіб, які є надзвичайно ефективними та перспективними в наш час.

В четвертому розділі виконано оцінку основних показників якості біометричних методів. Проведено порівняльний аналіз найбільш популярних методів біометричної ідентифікації та виконано вибір оптимального методу з урахуванням сукупності показників якості. Оптимальним виявився метод БІ за райдужною оболонкою ока. Також було розглянуто деякі варіанти

мультибіометричних методів та виконано вибір оптимального з урахуванням сукупності показників якості. Оптимальним виявився метод МБІ, що для ідентифікації користувача використовує комбінацію таких біометричних ознак: «відбиток пальців + райдужна оболонка ока». В будь якому разі використання мультибіометричних методів розпізнавання допомагає точніше ідентифікувати особу в порівнянні з використанням біометричних методів з однією ознакою для розпізнавання.

Результати роботи було апробовано на п’ятій міжнародній науково-практичній конференції «Наукоємні технології в інфокомунікаціях» НІСТ-2023 та опубліковано тези доповіді [32] за тематикою кваліфікаційної роботи.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Інформаційні мережі зв’язку. Ч.4. Технології надання інформаційних послуг: навч. посібник. / [В. М. Безрук, В. М. Корольов, В. А. Золотарьов та ін.]. – Харків: ХНУРЕ, 2011. – 424 с.

2. Grigutytė M. What is user authentication, and why is it important? [Електронний ресурс] / Monika Grigutytė // NordVPN. – 2023. – Режим доступу до ресурсу: https://nordvpn.com/uk/blog/what-is-user-authentication/.

3. Gupta D. Authentication, Identity Verification, and Identification: What\'s the Difference [Електронний ресурс] / Deepak Gupta // LoginRadius. – 2023. – Режим доступу до ресурсу: https://www.loginradius.com/blog/identity/authentication-identity-verification-identification/.

4. Identification vs. Authentication: What’s the Difference? [Електронний ресурс] // HYPR. – 2023. – Режим доступу до ресурсу: https://blog.hypr.com/identification-vs-authentication.

5. Іванюк В. А. Дослідження методів ідентифікації особи в системах контролю доступу на об’єкт [Електронний ресурс] / В. А. Іванюк, П. М. Повідайко // Житомирський державний технологічний університет. – 2022. – Режим доступу до ресурсу: http://eztuir.ztu.edu.ua/bitstream/handle/123456789/1254/76.pdf?sequence=1.

6. Колган В. А. Ідентифікація користувачів інформаційнокомп’ютерних систем [Електронний ресурс] / В. А. Колган // 2022 – Режим доступу до ресурсу: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/33705/Колган.pdf?sequence=1&isAllowed=y.

7. Сачанюк-Кавецька Н. В. Ідентифікація суб’єктів в системах контролю доступу за допомогою ідентифікаційної логіко-часової функції, як ефективний метод комплексного захисту інформації / Н. В. Сачанюк-Кавецька, О. І. Бондаренко. // Оптико-електронні інформаційно-енергетичні технології. – 2018. – С. 14 – 23.

8. Luis-Garcia R. Biometric identification systems / Rodrigo de Luis-Garcia, Carlos Alberola-Lo'pez, Otman Aghzout, Juan Ruiz-Alzola // Signal Processing. – 2003. –№83. – С. 2539 –2557.

9. Thales TruE Technology: responsible biometrics [Електронний ресурс] // Thales. – 2023. – Режим доступу до ресурсу: https://www.thalesgroup.com/en/worldwide/group/magazine/thales-true-technology-responsible-biometrics.

10. Biometrics: definition, use cases, latest news [Електронний ресурс] // Thales. – 2023. – Режим доступу до ресурсу: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.

11. Stouffer C. What is biometrics + is sensor-based security safe? [Електронний ресурс] / Clare Stouffer // Norton. – 2023. – Режим доступу до ресурсу: https://us.norton.com/blog/iot/what-is-biometrics.

12. Forecast and analysis of the current market status and development trend of the global biometrics industry in 2021 [Електронний ресурс] // JAEMONT. – 2021. – Режим доступу до ресурсу: https://www.jaemont.com/new/The-market-development-trend-of-the-biometrics-industry-in-2021.html.

13. Types of Biometrics [Електронний ресурс] // Biometrics Institute. – 2024. – Режим доступу до ресурсу: https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

14. Jain T. A study of vein recognition system / Tarshi Jain, Rajendra Kumar // Acta Informatica Malaysia (AIM). – 2019. –№3(1). – С. 13 –15.

15. McCayna B. The latest trends in biometrics for access control (2023 advancements) [Електронний ресурс] / Ben McCayna // SourceSecurity. – 2023. – Режим доступу до ресурсу: https://www.sourcesecurity.com/insights/latest-trends-biometrics-access-control-2023-co-1666076487-ga.1675261932.html.

16. Marley R. Top 10 Biometric Technology Trends to Watch For in 2022 / Richard Marley [Електронний ресурс] // Shufti Pro. – 2022. – Режим доступу до ресурсу: https://shuftipro.com/blog/top-10-biometric-technology-trends-to-watch-for-in-2022/.

17. Biometric System Market by Authentication Type (Single Factor, Fingerprint, Iris, Face, Voice; Multi-factor), Type (Contact-based, Contactless, Hybrid), Offering Type, Mobility, Vertical & Region (2022-2027) [Електронний ресурс] // Markets And Markets. – 2022. – Режим доступу до ресурсу: https://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html?gclid=CjwKCAjw7cGUBhA9EiwArBAvovegYkxeZcumKd0eBLWEmUggnEw2Jed1G4yRV_D599OITjLXE19kxhoCmTMQAvD_BwE.

18. Castillo L. Critical Biometric Trends [Recent Study] [Електронний ресурс] / Lorena Castillo // Gitnux Marketdata Report 2024. – 2023. – Режим доступу до ресурсу: https://gitnux.org/biometric-trends/.

19. Benefits of multi-factor authentication [Електронний ресурс] // Imprivata. – 2021. – Режим доступу до ресурсу: https://www.imprivata.com/uk/node/103705.

20. Trevino A. Types of Multi-Factor Authentication (MFA) [Електронний ресурс] / Aranza Trevino // Keeper. – 2023. – Режим доступу до ресурсу: https://www.keepersecurity.com/blog/2023/06/27/types-of-multi-factor-authentication-mfa/.

21. Campillo R. What is Multifactor Authentication (MFA) or Two Factor Authentication (2FA) [Електронний ресурс] / Rafael Campillo // Mobbeel. – 2023. – Режим доступу до ресурсу: https://www.mobbeel.com/en/blog/what-is-multi-factor-authentication-mfa-or-two-factor-authentication-2fa/.

22. Kaur R. Multi-Factor Authentication: Meaning, Advantages and Disadvantages [Електронний ресурс] / Rupandeep Kaur // TechThirsty. – 2021. – Режим доступу до ресурсу: https://www.techthirsty.com/multi-factor-authentication-meaning-advantages-and-disadvantages/.

23. Sheena S. A Study Of Multimodal Biometric System / S. Sheena, M. Sheena. // IJRET: International Journal of Research in Engineering and Technology. – 2014. – Volume: 03, Special Issue:15. – P. 93–98.

24. Mishra K. A Framework Towards Using Multibiometric System Based Techniques For Personal Identification : for the award of the degree of doctor of philosophy in engineering / Mishra Kamta Nath. – Ranchi, India, 2013. – 228 с.

25. Sahana J. S. Multi Biometric Recognition System / J. S. Sahana, R. R. Tarun, C. R. Manjunath. // International Journal of Computer Science and Mobile Computing. – 2019. – Vol.8 Issue.6. – P. 89–94.

26. Gouri V. Comparative Analysis Of Multimodal Biometrics / V. Gouri, D. Chitra, M. Sanjay. // International Journal of Pharmacy & Technology. – 2016. – Vol. 8, Issue №4. – P. 22969–22981.

27. Kaur G. Comparative Analysis Of Multimodal Biometric System / G. Kaur, S. Singh, N. Kaur. // An International Journal of Engineering Science, Special Issue. – 2018. – Vol.27. – P. 129–137.

28. Hong Y. Performance Evaluation Metrics for Biometrics-based Authentication Systems [Електронний ресурс] / Yuxuan Hong // Bryn Mawr College. – 2021. – Режим доступу до ресурсу:

https://scholarship.tricolib.brynmawr.edu/server/api/core/bitstreams/28396e90-37e8-4d0c-aab0-4c6fb94d04ce/content.

29. Finger Vein Recognition [Електронний ресурс] // Mofiria. – 2020. – Режим доступу до ресурсу: https://www.mofiria.com/en/about/.

30. Palma D. Biometric-Based Human Recognition Systems: An Overview / David Palma and Pier Luca Montessoro [Електронний ресурс] // Recent Advances in Biometrics. – 2022. – Режим доступу до ресурсу: https://www.intechopen.com/online-first/80031.

31. Методи і технології біометричної ідентифікації за результатами літературних джерел / Л. Г. Коваль, С. М. Злепко, Г. М. Новіцький, Є. Г. Крекотень. // Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. – 2019. – Том 30 (69). Ч. 1.– №2. – С. 104 – 112.

32. Чеботарьова Д.В. Аналіз методів біометричної ідентифікації з урахуванням сукупності показників якості / Д. В. Чеботарьова, С.В.Вичужанін // Тези доповідей Науково-практична конференція "Наукоємні технології в інфокомунікаціях" НІСТ’2023. – Харків-Кам’янець-Подільський. – 2023.