№ 5(33) 2024
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

*УДК 004.056.2:621.397*

*https://doi.org/10.52058/2786-6025-2024-5(33)-731-741*

**Лунгол Ольга Миколаївна** кандидат педагогічних наук, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки, Донецький державний університет внутрішніх справ, вул. Велика Перспективна 1, м. Кропивницький, https://orcid.org/0000-0001-8128-0072

# БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В СИСТЕМАХ АВТЕНТИФІКАЦІЇ: ВИКОРИСТАННЯ ТА ПЕРСПЕКТИВИ

**Анотація**. Біометричні технології в системах автентифікації займають важливе місце в сфері інформаційної безпеки та ідентифікації особи. Стаття присвячена дослідженню сучасних можливостей використання біометричних методів для підтвердження особи в інформаційних системах. В роботі розкрито актуальну проблему сучасного світу – проблему забезпечення високого рівня безпеки в інформаційних системах. Використання біометричних технологій у системах автентифікації є одним з ключових напрямків для подолання цієї проблеми. Ці технології базуються на унікальних фізіологічних чи поведінкових характеристиках особи, таких як відбитки пальців, розпізнавання обличчя, сканування радужки ока, голосові дані, дані ходи людини, відбитки долоні, венозна ідентифікація, серцевий ритм та генетичні дані. Основними перевагами використання біометричних технологій є висока точність і надійність ідентифікації особи, відсутність можливості втрати або запозичення ідентифікатора особи, а також зручність для самих користувачів. Ці технології дозволяють значно підвищити рівень безпеки в інформаційних системах, зменшити витрати на управління паролями та ідентифікаторами, а також спростити процес автентифікації. Проте варто відзначити й потенційні ризики використання біометричних технологій, таких, як можливість підробки біометричних даних, проблеми з приватністю та захистом особистої інформації, а також можливість виникнення фальшивих відмов при ідентифікації. Перспективи наукових досліджень у галузі біометричних технологій в системах автентифікації є досить широкими. Постійний розвиток технологій дозволяє вдосконалювати біометричні методи, розширювати сферу використання, поєднувати наявні досягнення з іншими технологіями та інноваціями, наприклад, можливостями штучного інтелекту. Важливо продовжувати дослідження щодо захисту біометричних даних від можливих атак, витоків та компроментації. Необхідно розвивати стандарти та законодавство щодо використання біометричних технологій, що допоможе в уникненні можливих конфліктів щодо приватності та прав особи.

**Ключові слова**: біометричні дані, сенсори, захист даних, доступ.

**Lunhol Olha Mykolayivna** PhD in Pedagogical Sciences, Docent, Associate Professor of the Department of Operational-search Activities and Information Security, Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0001-8128-0072

## BIOMETRIC TECHNOLOGIES IN AUTHENTICATION SYSTEMS: USAGE AND PERSPECTIVES

**Abstract.** Biometric technologies in authentication systems play a crucial role in the realm of information security and personal identification. The article is dedicated to exploring the modern possibilities of utilizing biometric methods for verifying identity in information systems. It delves into the pertinent issue of the modern world – ensuring a high level of security in information systems. The use of biometric technologies in authentication systems is one of the key directions for addressing this issue. These technologies are based on unique physiological or behavioral characteristics of an individual, such as fingerprints, facial recognition, iris scanning, voice data, gait data, palm prints, vein recognition, heart rhythm, and genetic data. The main advantages of using biometric technologies include high accuracy and reliability in identifying individuals, the absence of the possibility of loss or theft of an individual's identifier, as well as convenience for users themselves. These technologies allow for a significant enhancement in the security level of information systems, reduce costs associated with managing passwords and identifiers, and simplify the authentication process. However, it is worth noting the potential risks of using biometric technologies, such as the possibility of biometric data tampering, privacy and personal information protection issues, and the potential for false rejections during identification. The prospects of scientific research in the field of biometric technologies in authentication systems are quite extensive. The continuous development of technologies allows for the improvement of biometric methods, expanding the scope of their application, and integrating existing achievements with other technologies and innovations, such as artificial intelligence capabilities. It is crucial to continue research on protecting biometric data from possible attacks, leaks, and compromise. Developing standards and legislation regarding the use of biometric technologies is necessary to avoid potential conflicts concerning privacy and individual rights.

**Keywords:** biometric data, sensors, data protection, access.

**Постановка проблеми.** Сучасні технології дозволяють використовувати біометричні дані, такі як відбитки пальців, сканування райдужної оболонки ока або розпізнавання обличчя для надійної ідентифікації та

автентифікації користувачів. На відміну від традиційних засобів авторизації, таких як паролі чи токени, біометричні дані унікальні для кожної особи і можуть бути використані для забезпечення високого рівня безпеки доступу до систем, платежів та інших критично важливих операцій. Біометричні технології стають все більш поширеними в повсякденному життя, надаючи зручний і безпечний спосіб ідентифікації особи.

Біометрична автентифікація спирається на різноманітні технології, які дозволяють надійно ідентифікувати людину за її унікальними фізіологічними або поведінковими характеристиками. Ключовим елементом цих технологій є сенсори, які зчитують біометричні дані – відбитки пальців, малюнок райдужної оболонки ока, рисунок вен долоні, голос, малюнок обличчя тощо. В той же час, використання біометричних даних для автентифікації становить значні виклики для забезпечення безпеки та конфіденційності. Оскільки біометричні дані, такі як відбитки пальців, райдужна оболонка або риси обличчя, є унікальними, їх складно або неможливо замінити, як пароль чи PIN-код. Компроментація цих даних може призвести до серйозних наслідків для людини, організації або навіть країни.

Актуальним залишається питання подолання можливості компроментації біометричних даних через розвиток нових методів захисту задля запобігання викрадення біометричних даних або використанню фальшивих для обходу системи. Також, важливим є аналіз розвитку стандартів зберігання та обробки біометричних даних з метою забезпечення їхньої конфіденційності та недоступності для несанкціонованого доступу. Постійні дослідження в галузі шифрування, захисту від перехоплення та зламу, а також аналіз можливих ризиків та вразливостей біометричних систем є невід'ємною частиною забезпечення безпеки персональних даних користувачів та організацій.

**Аналіз останніх досліджень і публікацій.** Питання удосконалення та захисту біометричних технології в системах автентифікації є актуальним питанням сьогодення і активно досліджується вітчизняними науковцями. Так, Курченко О., Зубик Л. та Щебланін Ю. [1, с. 56] описують в своїх наукових роботах переваги динамічних біометричних методів ідентифікації. Науковці зазначають, що комбінуючи різні способи біометричної і апаратної автентифікації, можна отримати надійну систему захисту і слід сконцентрувати увагу на підвищенні якості ідентифікації за допомогою динамічних методів біометричної ідентифікації з використанням сучасних методів статистичного і ймовірнісного моделювання.

Клочко А. та Волченко Н. [2] наголошують, що в Україні існує необхідність створення уніфікованої біометричної системи для потреб сфери банківської діяльності. Подібні моделі таких систем вже успішно функціонують в деяких зарубіжних державах.

Короленко М. та Потапова Н. [3] виіляють ключові елементи типової системи автентифікації: суб'єкт (користувач), за даними якого здійснюється процедура автентифікації; особлива відмінна риса даного суб'єкта – його конкретна біометрична характеристика; адміністратор системи автентифікації, який керує роботою системи, несе відповідальність за усі дії, що у ній відбуваються; алгоритм роботи системи автентифікації та механізм управління системою автентифікації, тобто управління доступом. Науковці також зазначають [3, с. 350], що наразі активно досліджуються можливості багатофакторної або комплексної автентифікації користувачів, що ґрунтується на спільному використанні певних факторів автентифікації. Це значно підвищує рівень надійності та захищеності системи, оскільки при наявності лише одного ідентифікатора особи не можна цілковито бути впевненим у надійності його достовірності.

Погоджуюся з думкою Кулика О. та Долгової Н. [4], що системи біометричного захисту інформації не можна вважати абсолютно надійними через можливість виникнення проблем з різних причин, включаючи фізичні фактори. Прогрес в розробці сенсорних технологій, алгоритмів обробки даних та машинного навчання може сприяти подоланню цих проблем і покращенню точності та надійності систем біометричного захисту. Біометричні технології в системах автентифікації потребують постійного вивчення та вдосконалення, щоб і надалі залишатися ефективними засобами безпеки.

**Мета** статті полягає в аналізі сучасних можливостей використання біометричних технологій у системах автентифікації, визначенні їх переваг та ймовірних ризиків.

**Виклад основного матеріалу.** Біометричні технології в сучасному світі стають все більш поширеними в системах автентифікації, забезпечуючи високий рівень безпеки та зручності для користувачів. Біометричні технології базуються на унікальних фізичних або поведінкових характеристиках користувача. До основних видів біометричних технологій відносяться: відбитки пальців, розпізнавання обличчя, сканування радужки ока, голосові дані, дані ходи людини, відбитки долоні, венозна ідентифікація (або ідентифікації за венозним рисунком долоні руки), серцевий ритм, генетичні дані.

Біометрична технологія автентифікації на основі відбитків пальців є однією з найпоширеніших і на сьогодні вважається однією з найефективніших в біометричній ідентифікації. Вона базується на унікальних фізичних особливостях – відбитках пальців, які можуть бути виміряні, аналізовані та використані для ідентифікації. Основні етапи роботи біометричної системи на основі відбитків пальців включають:

- збір відбитків пальців за допомогою спеціального сканеру відбитків пальців. Сучасні сканери можуть бути оптичними, які використовують світлове

випромінювання, або ємнісними, які реєструють електичні параметри на поверхні пальця;

- формування шаблону відбитка пальця. Цей шаблон зазвичай представляється як числовий код, який може бути збережений в базі даних. На цьому етапі проводиться відбір основних характеристик відбитка, таких як довжина ліній, вузли, кінці папіллярних зон і т.д.;
- зберігання шаблону відбитка пальця в базі даних системи. Для безпеки він може бути зашифрований;
- ідентифікація, при якій особа має пройти процедуру зчитування відбитка пальця за допомогою сканера. Система порівнює отриманий відбиток із збереженим у базі даних шаблоном. Якщо вони співпадають, ідентифікація вважається успішною.

Переваги біометричної ідентифікації на основі відбитків пальців включають високу точність (унікальність відбитків), швидкість реакції (зчитування відбитків займає лише кілька секунд) і зручність в експлуатації (не потрібно пам'ятати паролі або PIN-коди). Такі системи використовуються в банках, установах для доступу до комп'ютерів та пристроїв, а також для контролю доступу на об'єктах з підвищеним рівнем безпеки.

Біометрична технологія автентифікації на основі розпізнавання обличчя також є однією з найбільш відомих і широко розповсюджених методів біометричної ідентифікації. Дана технологія базується на унікальних особливостях обличчя людини, таких як форма, розташування очей, вуст, носа та інших відмінних рис. Технологія вимірює і аналізує зазначені характеристики для того, щоб ідентифікувати або автентифікувати особу.

Основні етапи роботи біометричної системи на основі розпізнавання обличчя включають:

- сканування зображення обличчя людини за допомогою спеціальної камери або відеокамери. Такі камери можуть бути вбудовані в різноманітні пристрої, від смартфонів до систем відеоспостереження. Потім це зображення аналізується для вимірювання основних параметрів обличчя, таких як розмір і форма очей, відстань між очима, розмір вуст, форма носа тощо;
- створення шаблону обличчя за допомогою обробки отриманого зображення через спеціальні алгоритми, які виділяють ключові особливості обличчя і перетворюють їх на унікальний шаблон. Цей шаблон може бути представлений у вигляді числового коду або вектора даних, які зручно зберігати і порівнювати при ідентифікації чи автентифікації особи;
- зберігання інформації в базі даних системи для подальшого використання. Зазвичай для безпеки шаблон обличчя шифрується;
- під час ідентифікації особа представляє своє обличчя для сканування камерою. Система порівнює отриманий шаблон обличчя зі збереженими в базі даних шаблонами і визначає, чи відповідає це обличчя

комусь з вже ідентифікованих. У випадку автентифікації система визначає, чи відповідає обличчя власнику системи або доступу.

Переваги біометричної ідентифікації на основі розпізнавання обличчя включають високу швидкість і точність, зручність (не потрібно запам'ятовувати паролі або коди доступу), а також безпечність (унікальність обличчя). Такі системи використовуються для доступу до смартфонів, комп'ютерів, будівель, банківських систем, систем відеоспостереження та інших галузей, де важлива ідентифікація особи.

Біометрична технологія автентифікації на основі сканування радужки ока використовує унікальні характеристики радужки для ідентифікації особи. Радужка ока містить унікальні візерунки, які не повторюються навіть у родичів і не змінюється протягом усього життя.

Як і в попередних методах, спочатку проводиться сканування радужки ока за допомогою спеціального пристрою, який називається сканером радужки. Цей сканер використовує інфрачервоне світло для створення візуального зображення радужки, яке потім аналізується. Далі створюється цифровий шаблон, при якому аналізується радужка для визначення унікальних особливостей, таких як візерунки, кількість вен і волокон, діаметр тощо. Радужковий шаблон представляє собою унікальний числовий код або вектор даних. Створений шаблон зберігається в базі даних системи для подальшого використання. Під час ідентифікації особа наближає до пристрою своє око для сканування. Система порівнює отриманий радужковий шаблон зі збереженими в базі даних шаблонами і визначає, чи відповідає цей радужковий шаблон комусь з вже ідентифікованих. У випадку автентифікації система визначає, чи відповідає радужковий шаблон власнику системи або доступу.

Біометрична технологія сканування радужки ока має кілька важливих переваг, серед яких: висока точність визначення особи через унікальність даних, нестандартність, оскільки радужкова ідентифікація є менш вразливою до змін відбитків (наприклад, внаслідок старіння чи пошкодження), висока швидкість сканування, безконтактність, а отже гігієнічність.

Біометричні технології сканування радужки ока використовуються в системах безпеки, контролю доступу, паспортних контрольних пунктах та інших галузях, де важлива висока ступінь ідентифікації особи.

Біометрична технологія автентифікації за голосовими даними – це метод ідентифікації особи за унікальними особливостями голосу, такими як тон, частота, інтонація, ритм та інші акустичні характеристики. Ці характеристики можуть бути використані для ідентифікації особи в системі безпеки або аутентифікації при доступі до пристроїв чи послуг.

Принцип роботи такої системи автентифікації полягає в тому, що користувачу потрібно зареєструвати свій голос у системі, яка записує та

аналізує його акустичні параметри. Після реєстрації система може порівнювати голосові дані користувача з збереженими унікальними шаблонами, які використовуються для автентифікації. Якщо характеристики голосу відповідають шаблону на достатньому рівні, користувачу надається доступ.

Основні переваги біометричної автентифікації за голосовими даними включають унікальність, зручність, високу точність, можливість використання у реальному часі. Кожна людина має унікальний голос, що робить його надійним методом ідентифікації. Не потрібно запам'ятовувати або носити при собі паролі або ідентифікаційні картки – достатньо просто говорити. Сучасні алгоритми аналізу голосу дозволяють досягти високої точності ідентифікації. Голос важко підробити, тому цей метод автентифікації забезпечує високий рівень безпеки.

Однак існують певні виклики для біометричної автентифікації за голосовими даними, такі як: залежність від умов (шум, екологічні умови, захворювання користувача тощо); важливість забезпечення захисту голосових даних від несанкціонованого доступу та використання; якісне обладнання та програмне забезпечення.

Біометрична технологія автентифікації за голосовими даними є одним з інноваційних методів ідентифікації особи, який має великий потенціал у різних сферах, включаючи безпеку, фінанси, медицину та інші галузі.

Біометрична технологія автентифікації за даними ходи людини [5; 6] (іноді відома як «біометрія ходи» або «біометричний рух») використовується для ідентифікації особи за унікальними характеристиками її ходи. Принцип роботи цієї технології полягає в тому, що спеціальні датчики або пристрої, такі як акселерометри або гіроскопи, фіксують і аналізують унікальні особливості руху особи під час ходи. Ці характеристики можуть включати параметри, такі як швидкість, довжина кроку, час кроку і т.д. Після того як характеристики ходи зареєстровані і збережені у вигляді біометричного шаблону, їх можна використовувати для подальшої ідентифікації.

Основні переваги біометричної автентифікації за даними ходи людини включають унікальність, «невидимість» для користувача, зручність, важкість підробки, можливість використання на відстані тощо.

Однак існують деякі виклики для біометричної технології автентифікації за даними ходи людини, такі як залежність від умов ходи (наприклад, від погодних умов або типу поверхні), необхідність точної фіксації даних ходи, що потребує відповідного обладнання та налаштування, важливість забезпечення захисту даних ходи від несанкціонованого доступу та використання.

Лобачев М. та Пуріш С. [5] зазначають, що для розпізнавання ходи не потрібний прямий фізичний контакт з датчиками або пристроями, що дозволяє

використовувати цей метод для віддаленої ідентифікації, наприклад, за допомогою відеоспостереження. Науковці звертають увагу, що розпізнавання ходи може бути ефективним в публічних місцях, де інші методи, такі як сканування відбитків пальців чи обличчя, можуть бути менш зручними або несумісними зі звичайною поведінкою користувачів. Розпізнавання ходи може бути використано як частина багатофакторної аутентифікації, поєднуючи його з іншими біометричними методами або паролями для підвищення рівня безпеки. Біометрична технологія автентифікації за даними ходи людини є одним з інноваційних методів ідентифікації, який може бути застосований в різних сферах, включаючи безпеку, медицину, транспорт та інші галузі.

Біометрична технологія ідентифікації за венозним рисунком долоні руки є високоточним і надійним методом автентифікації особи за унікальними характеристиками вен і судин [7]. Принцип роботи цієї технології полягає в тому, що спеціальні пристрої, відомі як венозні сканери, використовуються для зчитування унікальних венозних рисунків у долоні руки. Ці сканери використовують інфрачервоне випромінювання для проникнення в поверхневі шари шкіри і відображення венозних структур. Венозні рисунки формуються через різницю у відбиванні і поглинанні інфрачервоного світла судинами під шкірою.

До основних переваг біометричної ідентифікації за венозним рисунком долоні руки можна віднести: унікальність та стабільність, високу точність, відсутність фізичного контакту з пристроєм, що забезпечує високий рівень гігієни та зручності для користувачів, високу швидкість ідентифікації, що є зручним для великих масштабів використання, наприклад, в організаціях або в транспорті.

Однак, існують певні виклики і обмеження для венозної біометрії: необхідність спеціалізованих дороговартісних на даний час сканерів, важливість захисту даних венозного рисунку від несанкціонованого доступу та використання. Проте, у перспективі, біометрична технологія ідентифікації за венозним рисунком долоні руки представляє собою потужний інструмент для забезпечення безпеки та автентифікації в різних сферах, від корпоративного сектора до медичних установ та урядових органів.

Біометрична технологія автентифікації за серцевим ритмом полягають у вимірюванні і аналізі фізіологічних параметрів серця, таких як частота серцевих скорочень, інтервали між ними, амплітуда і форма електрокардіограми (ЕКГ). До переваг даного методу можна віднести унікальність та стабільність. Проте, як і в попередніх методах існує потреба у спеціальному обладнанні та важливості забезпечення високого рівня захисту даних серцевого ритму від несанкціонованого доступу та використання.

Біометрична технологія автентифікації за генетичними даними полягають у зчитуванні та аналізі генетичної інформації, наприклад, ДНК.

Генетичний код кожної людини є унікальним і не змінюється протягом життя, що робить цей метод надзвичайно надійним. Однак, генетичні дані потребують спеціальних пристроїв та високотехнологічного обладнання для їх зчитування та обробки. Також, збір, зберігання та використання генетичних даних вимагає вирішення етичних питань та дотримання відповідних правил та стандартів.

Проаналізувавши літературу [1 – 9] можна стверджувати, що серед перелічених методів біометричної технологія автентифікації до найбільш надійних на даний час можна віднести відбитки пальців, оскільки вони використовуються протягом багатьох років, мають високий рівень точності та широко застосовуються у біометричних системах. Найбільш перспективними можуть бути голосові дані та розпізнавання обличчя. Голосові технології постійно розвиваються, особливо у напрямку використання штучного інтелекту для підвищення точності. Розпізнавання обличчя також має потенціал у значній кількості галузей, включаючи безпеку та зручність в різних системах. Найбільш дороговартісними можуть бути венозна ідентифікація (ідентифікація за венозним рисунком долоні руки) та сканування радужки ока. Ці технології вимагають спеціального обладнання для збору даних і більш складних алгоритмів обробки, через що може зростати вартість їх впровадження. Найбільш зручними для користувачів можуть бути відбитки пальців та розпізнавання обличчя.

**Висновки.** Біометричні технології в системах автентифікації відіграють значущу роль у сфері інформаційної безпеки та ідентифікації особи. Дослідження сучасних можливостей застосування біометричних методів для підтвердження особи у інформаційних системах є актуальним питанням сьогодення. Використання біометричних технологій у системах автентифікації є одним із ключових напрямків для вирішення цієї проблеми. Ці технології базуються на унікальних фізіологічних або поведінкових характеристиках особи, таких як відбитки пальців, розпізнавання обличчя, сканування радужки ока, голосові дані, дані ходи людини, відбитки долоні, венозна ідентифікація, серцевий ритм та генетичні дані. Основними перевагами використання біометричних технологій є висока точність і надійність ідентифікації особи, відсутність можливості втрати або використання чужого ідентифікатора, а також зручність для користувачів. Ці технології значно підвищують рівень безпеки в інформаційних системах, зменшують витрати на управління паролями та ідентифікаторами, а також спрощують процес автентифікації. Проте слід відзначити потенційні ризики використання біометричних технологій, такі як можливість підробки біометричних даних, проблеми з приватністю та захистом особистої інформації, а також можливість виникнення фальшивих відмов при ідентифікації.

Перспективи наукових досліджень у галузі біометричних технологій в системах автентифікації є досить обширними. Постійний розвиток технологій дозволяє удосконалювати біометричні методи, розширювати область їх застосування, а також поєднувати наявні досягнення з іншими технологіями та інноваціями, включаючи можливості штучного інтелекту. Важливо проводити подальші дослідження щодо захисту біометричних даних від кібернебезпек. Необхідно розвивати стандарти та законодавство щодо використання біометричних технологій, що сприятиме уникненню можливих конфліктів щодо приватності та прав особи.

***Література:***

1. Курченко О.А., Зубик Л.В., Щебланін Ю.М. Аналіз застосування біометричних технологій в забезпеченні інформаційної безпеки. Proceedings of the XVI International Scientific and Practical Conference «Principles of science. Ideals, norms, values in science and style of scientific thinking». April 17 – 18, 2023. Tallinn, Estonia. С. 52 – 56.

2. Клочко А.М., Волченко Н.В. Біометричні технології для безпеки проведення банківських операцій в Україні та зарубіжних державах. Часопис Київського університету права. Київ, 2021. № 1. С. 299-304.

3. Короленко М.В., Потапова Н.А. Ідентифікація та автентифікація користувачів на основі біометричних даних. Прикладні інформаційні технології. 2023. С. 349-351.

4. Кулик О.В. Важливість біометричного захисту приватної інформації. Матеріали XV-ої Міжнародної науково-практичної конференції «Free and Open Source Software», Харків, 13-14 лютого 2024 р. Харків: Харківський національний економічний університет імені Семена Кузнеця, 2024. С. 32.

5. Лобачев М.В., Пуріш С.В. Системи біометричної ідентифікації на базі розпізнавання ходи. In The 10 th International scientific and practical conference “European scientific congress” (October 29-31, 2023). Barca Academy Publishing, Madrid, Spain. 2023. p. 212.

6. Лобачев М., Пуріш С. Методи ідентифікації людини за ходою за умов різної швидкості ходи. Наука і техніка сьогодні. 2023. №13 (27), С. 784 – 795.

7. Новіцький Г.М. Розвиток методу ідентифікації особистості за венозним рисунком долоні руки. Оптико-електронні інформаційно-енергетичні технології, № 38(2). 2019. С. 54 – 61.

8. Лунгол О.М., Агішева А.В. Технології створення та застосування систем захисту інформаційно-комунікаційних систем. In The 2 nd International scientific and practical conference “Topical aspects of modern scientific research”. October 26-28, 2023. CPN Publishing Group, Tokyo, Japan. p. 255.

9. Лунгол О. Удосконалення професійної підготовки майбутніх фахівців правоохоронної діяльності засобами інформаційних технологій. Наука і техніка сьогодні. 2022. № 7. С. 152 – 162.

***References:***

1. Kurchenko, O.A., Zubyk, L.V., & Shcheblanin, Yu.M. (2023). Analiz zastosuvannia biometrychnykh tekhnolohii v zabezpechenni informatsiinoi bezpeky [Analysis of Biometric Technology Applications in Information Security] – *Proceedings of the XVI International Scientific and Practical Conference «Principles of science. Ideals, norms, values in science and style of scientific thinking»*. (pp. 52-56). Tallinn, Estonia. [in Ukrainian].

2. Klochko, A.M., & Volchenko, N.V. (2021). Biometrychni tekhnolohii dlia bezpeky provedennia bankivskykh operatsii v Ukraini ta zarubizhnykh derzhavakh [Biometric Technologies for Security of Banking Operations in Ukraine and Foreign Countries]. *Chasopys Kyivskoho universytetu prava – Kyiv University Law Journal*, 1, 299-304 [in Ukrainian].

3. Korolenko, M.V., & Potapova, N.A. (2023). Identyfikatsiia ta avtentyfikatsiia korystuvachiv na osnovi biometrychnykh danykh [User Identification and Authentication Based on Biometric Data]. *Prykladni informatsiini tekhnolohii – Applied Information Technologies*, 349-35 [in Ukrainian].

4. Kulyk, O.V. (2024). Vazhlyvist biometrychnoho zakhystu pryvatnoi informatsii [The Importance of Biometric Protection for Private Information]. – *Materialy KhV-oi Mizhnarodnoi naukovo-praktychnoi konferentsii «Free and Open Source Software» – Materials from the XV International Scientific and Practical Conference «Free and Open Source Software»*. (p. 32). Kharkiv: Kharkivskyi natsionalnyi ekonomichnyi universytet imeni Semena Kuznetsia [in Ukrainian].

5. Lobachev, M.V., & Purish, S.V. (2023). Systemy biometrychnoi identyfikatsii na bazi rozpiznavannia khody [Biometric Identification Systems Based on Gait Recognition]. *In The 10 th International scientific and practical conference «European scientific congress»*. (p. 212). Barca Academy Publishing, Madrid, Spain [in Ukrainian].

6. Lobachev, M., & Purish, S. (2023). Metody identyfikatsii liudyny za khodoiu za umov riznoi shvydkosti khody [Methods of Human Identification by Gait at Varying Walking Speeds]. *Nauka i tekhnika sohodni – Science and Technology Today*. 13 (27), 784 – 795 [in Ukrainian].

7. Novitskyi, H.M. (2019). Rozvytok metodu identyfikatsii osobystosti za venoznym rysunkom doloni ruky [Development of the Method for Personal Identification Based on Palm Vein Pattern]. *Optyko-elektronni informatsiino-enerhetychni tekhnolohii – Optoelectronic Information-Energy Technologies*, 38(2), 54 – 61 [in Ukrainian].

8. Lunhol, O.M., & Ahisheva, A.V. (2023). Tekhnolohii stvorennia ta zastosuvannia system zakhystu informatsiino-komunikatsiinykh system [Technologies for the Creation and Application of Information and Communication Systems Security]. *In The 2 nd International scientific and practical conference «Topical aspects of modern scientific research»*. (p. 255). CPN Publishing Group, Tokyo, Japan [in Ukrainian].

9. Lunhol, O. (2022). Udoskonalennia profesiinoi pidhotovky maibutnikh fakhivtsiv pravookhoronnoi diialnosti zasobamy informatsiinykh tekhnolohii [Improving the Professional Training of Future Law Enforcement Specialists Using Information Technology Tools]. *Nauka i tekhnika sohodni – Science and Technology Today*. 7, 152 – 162 [in Ukrainian].