

СУЧАСНІ МЕТОДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ: ТЕНДЕНЦІЇ, ВИКЛИКИ ТА ПЕРСПЕКТИВИ

¹ Вінницький національний технічний університет

Анотація

Розглянуто сучасні методи біометричної автентифікації, зокрема розпізнавання обличчя, райдужки ока, голосу, венозної структури та мультимодальні системи. Підкреслено їхню високу точність, швидкість та зручність для користувачів, а також актуальність у сферах безпеки, фінансів та персональних пристроїв. Особливу увагу приділяється викликам впровадження біометрії: технічним обмеженням, демографічній упередженості, ризикам витоку даних та етичним аспектам. Розглянуто перспективи інтеграції біометрії з блокчейн-технологіями для підвищення захисту персональних даних. Наголошено на необхідності правового регулювання та дотримання етичних стандартів у використанні біометричних систем.

Ключові слова: біометрична автентифікація, розпізнавання обличчя, райдужка ока, голосова біометрія, розпізнавання вен, мультимодальні системи, безконтактна ідентифікація, блокчейн.

Abstract

Modern biometric authentication methods are considered, including facial recognition, iris recognition, voice recognition, venous structure recognition, and multimodal systems. Their high accuracy, speed, and user-friendliness are emphasized, as well as their relevance in the areas of security, finance, and personal devices. Special attention is paid to the challenges of implementing biometrics: technical limitations, demographic bias, data leakage risks, and ethical aspects. The prospects for integrating biometrics with blockchain technologies to enhance personal data protection are considered. The need for legal regulation and compliance with ethical standards in the use of biometric systems is emphasized.

Keywords: biometric authentication, facial recognition, iris recognition, voice biometrics, vein recognition, multimodal systems, contactless identification, blockchain.

Вступ

Розвиток цифрових технологій обумовив суттєве зростання інтересу до біометричної автентифікації як одного з найефективніших засобів захисту персональних даних. На відміну від традиційних методів автентифікації, таких як паролі чи токени, біометричні системи ґрунтуються на унікальних характеристиках конкретної особи. Це дозволяє значно підвищити рівень безпеки при доступі до інформаційних систем, водночас спрощуючи процедуру ідентифікації користувача.

Результати дослідження

Сучасні методи біометричної автентифікації набули широкого застосування завдяки своїй високій точності, швидкості обробки та зручності для користувачів. Ці технології використовуються для підвищення безпеки в банківських системах, при доступі до важливих об'єктів та в особистих пристроях. Але, попри всі їхні переваги, впровадження біометрії в реальну практику стикається з цілою низкою викликів, що пов'язані з технічними, етичними та правовими питаннями. Найбільшими з них є демографічна упередженість, ризики витоку даних, а також проблема поєднання різних біометричних методів у єдину систему [9].

Сучасні методи біометричної автентифікації, включають:

- Розпізнавання обличчя стало надзвичайно популярним завдяки своїй зручності: цей метод не вимагає фізичного контакту і може працювати в реальному часі. Розпізнавання відбувається шляхом порівняння ключових характеристик обличчя, таких як відстань між очима, форма щік, контури підборіддя та інші. Це технологія, що активно використовується в системах відеоспостереження та мобільних пристроях, проте вона має обмеження в умовах поганого освітлення або коли особа частково прихована [1];

- Метод розпізнавання райдужки ока має вищу точність у порівнянні з іншими біометричними методами, оскільки структура райдужки у кожної людини є унікальною. Це робить цей метод дуже надійним для ідентифікації особи. Райдужка ока також не піддається змінам з часом, що робить її стабільною ознакою для тривалої ідентифікації. Водночас метод є більш складним для реалізації через необхідність точного та швидкого зчитування з великої відстані [2];

- Голосова біометрія використовує унікальні характеристики людського голосу, такі як висота, тембр, швидкість мовлення, для ідентифікації особи. Цей метод активно застосовується в телефонних банківських системах та віртуальних асистентах, таких як Amazon Alexa або Google Assistant. Перевагою є безконтактність, але метод має певні обмеження, оскільки голос може змінюватися через хвороби, стрес або вікові зміни [3];

- Метод розпізнавання вен використовує унікальні патерни венозних судин, що проходять під шкірою рук або пальців. Цей метод набуває популярності завдяки своїй високій точності та складності підробки. Він часто використовується в банківських і медичних установах для забезпечення високої безпеки. Розпізнавання вен є безконтактним і може працювати в будь-яких умовах освітлення, однак для його реалізації потрібне спеціалізоване обладнання [4];

- Мультимодальні біометричні системи, які поєднують кілька методів автентифікації (наприклад, відбитки пальців і обличчя), показали значно більшу ефективність у порівнянні з традиційними однофункціональними системами. Ці технології дозволяють досягати більш високої точності при автентифікації, навіть в умовах змін або пошкодження однієї з біометричних ознак [1]. Такі системи не лише зменшують ймовірність помилок, але й забезпечують додатковий рівень безпеки, оскільки для несанкціонованого доступу необхідно підробити кілька біометричних характеристик одночасно.

Водночас, застосування біометрії підвищує важливість етичних аспектів. Один із головних викликів — це демографічна упередженість, коли системи розпізнавання можуть працювати менш ефективно для певних груп населення, наприклад, для осіб з темною шкірою, жінок або людей старшого віку. Це створює серйозні ризики порушення прав людини, зокрема в таких сферах, як право на рівність та недискримінацію [3]. Різні дослідження показали, що алгоритми розпізнавання обличчя та інших ознак не завжди демонструють рівну точність для всіх категорій користувачів, що вимагає коригування існуючих систем і створення більш інклюзивних рішень.

Таким чином, біометрична автентифікація є не лише інструментом для підвищення безпеки, але й складовою частиною загального напрямку цифрової трансформації суспільства. Її активне впровадження в фінансові установи, медицину, мобільні технології та державні сервіси демонструє високий рівень довіри до біометричних систем з боку інституцій та споживачів. У поєднанні з тенденцією до мінімізації фізичних контактів, яка особливо посилилася під час пандемії COVID-19, біометричні методи стали ключовими елементами безконтактної ідентифікації у новій реальності.

Інтеграція біометрії з інноваційними технологіями, такими як штучний інтелект [6], машинне навчання [7] та блокчейн, відкриває нові горизонти для побудови надійних та масштабованих систем захисту даних. У цьому контексті блокчейн здатен забезпечити не лише технічний захист, а й прозорий механізм обліку та контролю доступу до біометричної інформації, надаючи користувачу повноцінний контроль над своїми персональними даними.

Однак масштабне впровадження біометричних рішень потребує системного підходу до врегулювання правових аспектів. Необхідно розробити національні та міжнародні норми, які регулюватимуть обробку біометричних даних, з чітким визначенням понять, механізмів згоди, відповідальності сторін, а також прав людини на приватність. Без відповідного законодавчого підґрунтя біометрія може перетворитися з засобу безпеки на потенційний інструмент тотального спостереження чи дискримінації [10].

Крім того, варто інвестувати в розробку алгоритмів, здатних працювати однаково ефективно незалежно від статі, віку чи раси користувача. Це дозволить зробити біометричні системи більш інклюзивними та уникнути дискримінаційних ефектів, які сьогодні нерідко виникають через обмеження навчальних вибірок або недостатню репрезентативність під час розробки.

Пандемія COVID-19 змусила розглянути безконтактні методи автентифікації як пріоритетні. Поширення масок і соціальна дистанція ускладнили використання традиційних методів, таких як розпізнавання обличчя, і привели до росту інтересу до інших біометричних характеристик, таких як райдужка ока або венозна структура пальців. Ці методи дозволяють забезпечити високу точність без необхідності контакту з користувачем [2].

Інтеграція біометрії з блокчейн-технологіями відкриває нові можливості для захисту даних користувачів, оскільки блокчейн дозволяє створювати децентралізовані реєстри, які важче піддаються маніпуляціям. Це може стати важливим кроком у захисті біометричних даних, зокрема

при використанні їх у таких сферах, як фінансові послуги або голосування. Блокчейн не тільки забезпечує прозорість і незмінність даних, але й дає можливість користувачам повністю контролювати свої біометричні дані [4]. Така інтеграція дає додатковий рівень безпеки для чутливих біометричних даних, забезпечуючи їх захист від несанкціонованого доступу та зловживань.

Незважаючи на всі переваги, існують і значні правові та соціальні проблеми. Важливо не тільки забезпечити захист даних, але й дотримуватись етичних стандартів при зборі та використанні біометричних даних. Одним з найважливіших аспектів є забезпечення конфіденційності та права людини на приватність. Держава та приватні компанії повинні створювати чіткі правила для обробки біометричних даних, що включають контроль за їх використанням та чітке визначення прав користувачів на доступ до своїх біометричних даних [5].

Штучний інтелект (ШІ), зокрема алгоритми глибокого навчання, відіграють ключову роль у розвитку сучасних біометричних систем. Завдяки нейронним мережам, системи розпізнавання облич, голосу, відбитків пальців та інших біометричних ознак здатні автоматично навчатися на великих обсягах даних, виявляти складні патерни та підвищувати точність і стійкість до зовнішніх впливів. Наприклад, у системах розпізнавання облич ШІ дозволяє досягати високої точності навіть при зміні освітлення, кута огляду чи частковому перекритті обличчя [8].

Крім того, алгоритми ШІ забезпечують виявлення підрбок (Presentation Attack Detection [11], PAD), що дозволяє захистити систему від атак із використанням штучних облич, надрукованих зображень або синтезованого голосу.

Таким чином, біометричні системи автентифікації демонструють високий потенціал у забезпеченні безпеки та зручності для користувачів, але одночасно потребують вирішення численних викликів, включаючи демографічну упередженість, ризики витоку даних і етичні питання. Рішення цих проблем дозволить розвивати біометричні технології та інтегрувати їх в різноманітні сфери, що забезпечить ще більшу безпеку та ефективність в майбутньому.

Висновки

Сучасні біометричні методи автентифікації продемонстрували значний прорив у сфері інформаційної безпеки, забезпечуючи більш високий рівень точності, швидкості та зручності у порівнянні з традиційними методами ідентифікації. Завдяки широкому спектру доступних технологій — від розпізнавання обличчя до аналізу венозного малюнку — користувачі отримують ефективні та зручні засоби захисту доступу до інформаційних систем, фінансових сервісів, мобільних пристроїв та інших важливих об'єктів. Мульти模альні системи, які комбінують декілька біометричних параметрів, довели свою перевагу в забезпеченні додаткового рівня захисту та зменшенні помилок розпізнавання.

Однак попри технологічні досягнення, біометричні системи стикаються з низкою суттєвих викликів:

- Демографічна упередженість, яка знижує ефективність розпізнавання для окремих соціальних груп, загрожує порушенням принципів рівності та справедливості;
- Технічні обмеження — включаючи залежність від умов освітлення, зміни фізіологічних характеристик або потребу в дорогому обладнанні — також знижують універсальність і доступність таких рішень;
- Ризики витоку біометричних даних, які неможливо змінити після компрометації, створюють серйозні загрози конфіденційності та приватності.

Значну увагу необхідно приділяти етичним аспектам та правовому регулюванню, які повинні супроводжувати впровадження біометрії у повсякденне життя. Необхідно забезпечити прозорість процесів збору, зберігання та використання біометричної інформації, а також гарантувати право кожної особи на контроль над своїми персональними даними. У цьому контексті перспективною є інтеграція біометричних систем із технологією блокчейн, яка дозволяє створити децентралізовані, захищені та прозорі реєстри з високим ступенем контролю користувача над власними даними.

Підсумовуючи, можна стверджувати, що майбутнє біометричної автентифікації напряму залежить від балансу між технологічним прогресом, етичними принципами та ефективним регулюванням. Успішне вирішення наявних викликів дозволить розширити можливості біометрії, зробивши її не лише ефективним засобом захисту, але й основою довіри у цифровому суспільстві. Біометричні технології мають потенціал стати стандартом ідентифікації у світі, де цифрова безпека — це не привілей, а необхідність.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Yildirim M. A Novel Multimodal Biometric Authentication System using Machine Learning and Blockchain // arXiv. – 2021. – URL: <https://arxiv.org/abs/2109.03014> (дата звернення: 10.06.2025).
2. Gupta R. Biometrics in the Era of COVID-19: Challenges and Opportunities // arXiv. – 2021. – URL: <https://arxiv.org/abs/2102.09258> (дата звернення: 10.06.2025).
3. Zhang J. Demographic Bias in Biometrics: A Survey on an Emerging Challenge // arXiv. – 2021. – URL: <https://arxiv.org/abs/2003.02488> (дата звернення: 10.06.2025).
4. Khan H. Integrating Biometric Authentication Methods in Cloud Storage Systems // arXiv. – 2024. – URL: <https://arxiv.org/pdf/2311.13416> (дата звернення: 10.06.2025).
5. Peterson C. Biometric Identification in Criminalistics // Науковий вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. – 2024. – URL: <https://nzlubp.org.ua/archive/biometric-identification-in-criminalistics> (дата звернення: 10.06.2025).
6. Tekhnologichni trendy v kontroli fizychnoho dostupu: rozvytok biometriyi, shtuchnoho intelektu ta mobil'nykh rishen // GreenVision. – URL: <https://greenvision.ua/ua/blog/tekhnologichni-trendy-v-kontroli-fizychnoho-dostupu-rozvytok-biometriyi-shtuchnoho-intelektu-ta-mobilnykh-rishen> (дата звернення: 10.06.2025).
7. Biometrychna avtentifikatsiia: suchasni tendentsii ta doslidzhennia // Електронний архів НТУУ «КПІ імені Ігоря Сікорського». – URL: <https://ela.kpi.ua/server/api/core/bitstreams/b1880b6c-1111-4f9f-b6a7-daec958a0a32/content> (дата звернення: 10.06.2025).
8. Jain, A. K., Ross, A., & Nandakumar, K. Introduction to Biometrics. – Cham: Springer, 2022. – 312 p. – URL: https://www.researchgate.net/publication/387616031_Introduction_to_Biometrics (дата звернення: 10.06.2025).
9. Біометрична автентифікація: сучасні тенденції та дослідження // Електронний архів НТУУ «КПІ імені Ігоря Сікорського». – URL: <https://ela.kpi.ua/server/api/core/bitstreams/7f1251ba-7156-4730-8a08-3ae82ddbc1f3/content> (дата звернення: 10.06.2025).
10. Біометричні дані: збір і захист у Європі, США та Україні // Юридична газета. – URL: <https://yur-gazeta.com/publications/practice/inshe/biometrychni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html> (дата звернення: 10.06.2025).
11. Presentation Attack Detection: definition, methods and importance // Fraud.com. – URL: <https://www.fraud.com/post/presentation-attack-detection> (дата звернення: 10.06.2025).

Марценюк Катерина Володимирівна — студентка групи ЗКІТС-23б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: kata2006.01.27@gmail.com

Науковий керівник: **Зоря Ірина Сергіївна** — асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет

Martsenyuk Kateryna V. — student of group ЗКІТС-23b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: kata2006.01.27@gmail.com

Supervisor: **Zorya Iryna S.** — assistant professor, Department of Management and Security of Information Systems, Vinnytsia National Technical University