

УДК 004.056.52

DOI: <https://doi.org/10.17721/3041-2323.2024.312-319>

Євген РІМЕК, директор  
ORCID ID: 0009-0008-1934-7625  
e-mail: e.rimek@biosol.ua

Товариство з обмеженою відповідальністю  
"Біосол Україна", Київ, Україна

В'ячеслав КОЛОМИЦЕВ, заст. директора  
ORCID ID 0009-0003-9739-2636  
e-mail: v.kolomysev@biosol.ua  
Товариство з обмеженою відповідальністю  
"Біосол Україна", Київ, Україна

Артем РІМЕК, магістр  
ORCID ID: 0009-0007-7500-4267  
e-mail: a.rimek@biosol.ua  
Товариство з обмеженою відповідальністю  
"Біосол Україна", Київ, Україна

## ВИКОРИСТАННЯ ІННОВАЦІЙНИХ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ У ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

*Досліджено основні новітні методи та технології біометричної ідентифікації особи, їхню класифікацію та розглянуто практичне використання в прикладних інформаційних системах із боку актуальних задач і ризиків сьогодення, які можна розв'язувати, застосовуючи біометричну ідентифікацію користувача.*

*Розглянуто основні типи задач, а саме: а) контроль доступу до приміщень і важливих зон; б) доступ до інформаційних ресурсів, документів, баз даних, прикладних інформаційних систем тощо; в) ідентифікацію користувача на робочому місці чи віддалено та вхід в операційну систему або прикладні інформаційні системи без використання паролів, PIN-кодів для підвищення захисту від шахрайства, хакерських атак та інсайдерських загроз; г) використання біометрії для підтвердження особистості в бізнес-процесах.*

**Ключові слова:** *біометричні методи, біометричні технології, ідентифікація особи, захист інформаційних систем, контроль доступу, захист інформації, інформаційна безпека.*

© Ріmek Євген, Коломицев В'ячеслав,  
Ріmek Артем, 2024

## **Вступ**

Сучасний світ вирізняють стрімким розвитком різноманітних інноваційних технологій, а також появою нових загроз у сфері використання інформаційних систем, що зумовлює потребу в оновленні та вдосконаленні підходів, розробок і методів, а також у їх активному впровадженні в прикладні інформаційні системи, зокрема й у технології та методи біометричної ідентифікації особи.

Використання сучасних інформаційних методів і технологій біометричної ідентифікації особи дає можливість значно покращити безпеку інформаційних систем, прискорити й оптимізувати їхнє застосування, а також надати можливість подальшого їх розвитку, в тому числі з використанням методів штучного інтелекту та великих масивів даних, аналітики та комфортності праці користувачів (Jain, Nandakumar, & Ross, 2016).

## **Результати**

### ***Основні поняття та методи біометричної ідентифікації.***

Сучасні біометричні методи розглядають як складову інформаційних технологій, що базована на використанні різноманітних математичних підходів. Вони забезпечують розвиток систем розпізнавання та підтвердження особи, підвищуючи надійність упровадження біометричних рішень у сучасних системах контролю доступу, управління даними, документами та бізнес-процесами. Такий прогрес стає можливим завдяки впровадженню високоефективних методів у різних галузях, що підвищує рівень безпеки як у державному, так і в приватному секторі. Поняття "біометрія" охоплює широкий спектр математико-статистичних методів, призначених для кількісного опису біологічних процесів. Біометричні технології, зазвичай, означають автоматизовані способи встановлення або розпізнавання особистості за унікальними біологічними характеристиками людини. Використання сучасних засобів аналізу даних, методів штучного інтелекту (ШІ) й оброблення великих масивів інформації (Big Data) відкриває нові можливості для вдосконалення підходів і технологій у сфері біометрії. Біометрична ідентифікація полягає у визначенні особи за її неповторними біологічними ознаками. Є понад десяток типів таких ознак, для кожного з яких розроблено спеціалізовані пристрої, що пра-

цюють за різними технічними принципами. Порівняно з традиційними методами автентифікації, біометричні технології мають низку переваг і їх дедалі частіше застосовують у комп'ютерних системах.

**Класифікація методів біометричної ідентифікації.** За способом взаємодії з ознаками, біометричні методи ідентифікації розділяють на статичні (використання ознак, що не змінюються протягом життя), динамічні (застосування ознак, що змінюються або генеруються під час дії) та комбіновані (використання комбінації обох типів).

*Статичні методи* використовують різноманітні прилади для зняття біометричної інформації і, в подальшому, на підставі різних математичних алгоритмів, обробляють цю інформацію, записуючи у вигляді цифрового унікального коду (спеціалісти називають його зліпок, або контрольний код) на різних інформаційних ресурсах. Відтак ці контрольні зліпки використовують для порівняння з іншими зліпками, застосовуючи ту саму технологію, що формувала контрольний зліпок.

*Динамічні методи* використовують алгоритми, які, в першу чергу, аналізують динамічні процеси або поведінку користувача, і також шифрують цю інформацію у вигляді деякого цифрового коду для подальшого порівняння з аналогічними процесами або поведінкою. Комбіновані методи біометричної ідентифікації (так звана багатофакторна автентифікація) поєднують кілька методів ідентифікації (зазвичай статичний і динамічний метод, а іноді кілька) для того, щоб збільшити достовірність ідентифікації та прискорити процес пошуку й оброблення результатів. Біометрична ідентифікація виконує дві основні функції.

1. Реєстрація. На цьому етапі за допомогою біометричного пристрою здійснюють зчитування кількох параметрів вибраної біометричної ознаки. На основі отриманих даних створюють цифровий шаблон (модель), який слугує унікальним представленням зареєстрованої особи.

2. Ідентифікація. Ця функція охоплює вимірювання контрольованої біометричної характеристики зчитувальним пристроєм, яке перетворюється на цифровий код.

Подальші порівняння коду виконують:

а) з *єдиним шаблоном*: у цьому випадку шаблон обирають за наперед відомим номером або кодом у базі даних. Результат порівняння відображається на екрані пристрою, що ініціює запит. Ця процедура відома як *верифікація* або порівняння "один до одного", а отриманий результат вказує на ймовірність того, що порівнювані шаблони належать одній особі;

б) з *усіма зареєстрованими шаблонами*: у цьому випадку результатом є список кількох найбільш схожих шаблонів (із вказуванням ступеня схожості). Після цього застосовується математичний критерій для ухвалення рішення щодо ідентичності шаблонів. Ця процедура відома як автентифікація або порівняння "один до багатьох". Є два основні показники, які використовують для порівняння якості методів і технологій біометричної ідентифікації – це FAR (False Acceptance Rate, або частота помилкових спрацювань) та FRR (False Rejection Rate, або частота відмов у спрацюванні). Іншими критеріями, яким має відповідати будь-який біометричний метод, є такі.

1. **Універсальність.** Кожна людина повинна мати ту біометричну характеристику, яка потрібна для конкретного біометричного методу.

2. **Унікальність (розрізнованість).** На відміну від автентифікації за допомогою паролів чи цифрових ключів, біометричні технології завжди мають деяку ймовірність схожості між біологічними характеристиками. Унікальність визначається як мінімальне значення ймовірності помилкового розпізнавання (False Acceptance Rate), що вказує на ймовірність того, що система помилково визначить "чужого" як "свого".

3. **Перманентність.** Біометрична характеристика має залишатися незмінною із часом (біометричний шаблон не повинен старіти). Це оцінюють за допомогою залежності False Rejection Rate від часу між тестами на одній і тій самій групі індивідів.

Важливою частиною використання певного методу біометричної ідентифікації є технологія та розмір цифрового коду (зліпка) користувача. Це разюче впливає на вибір практичного використання тієї або іншої технології. Особливо це важливо, коли термін прийняття рішення щодо автентичності особи короткий. Тому

науковці рухаються для оптимізації методів ідентифікації в таких напрямках (Jain, Ross, & Prabhakar, 2004; Jain, Flynn, & Ross, 2007):

- математичні алгоритми, які мінімізують сам цифровий код (зліпок);
- оптимізація зберігання й оброблення інформації (розподілені процеси, алгоритми пошуку тощо);
- ефективне кодування зліпка щодо достовірності, мінімізації, неможливості підробки.

Використання математичних методів багатокритеріального аналізу, методів вагових коефіцієнтів та експертних систем дозволяють розширити математичний апарат і розвинути нові можливості використання методів біометричної ідентифікації та технологій на їхній базі. До найбільш поширених нині методів біометричної ідентифікації належать такі: статичні – за відбитками пальців, обличчям, райдужною оболонкою ока, сітківкою ока, геометрією долоні, рисунком вен долоні, рисунком вен пальця, ДНК, на основі характеристик вуха; динамічні – за голосом, за рукописним почерком, за клавіатурним почерком, за ходом особи. Критерії використання деяких технологій біометричної ідентифікації наведено в табл. 1.

*Таблиця 1*

**Порівняння біометричних методів**

<b>Біометричні методи</b>	<b>FAR, %</b>	<b>FRR, %</b>	<b>Фальсифікація</b>	<b>Суворая автентифікація</b>	<b>Сталість</b>	<b>Швидкість автентифікації</b>	<b>Вартість реалізації</b>
Відбиток пальця	0,001	0,6	Можлива	Можлива	Низька	Висока	Низька
Розпізнавання обличчя 2D	0,1	2,5	Можлива	Ні	Низька	Середня	Середня

Закінчення табл. 1

Біометричні методи	FAR, %	FRR, %	Фальсифікація	Суворавтентифікація	Сталість	Швидкість автентифікації	Вартість реалізації
Розпізнавання обличчя 3D	0,0005	0,1	Проблематична	Ні	Висока	Низька	Висока
Радужна оболонка ока	0,00001	0,016	Неможлива	Можлива	Висока	Висока	Висока
Сітківка ока	0,0001	0,4	Неможлива	Можлива	Середня	Низька	Висока
Венозний малюнок долоні	0,00008	0,01	Неможлива	Можлива	Середня	Висока	Середня

### Дискусія і висновки

Інтенсивний розвиток біометричних технологій у XXI ст. дає змогу використовувати біометричні методи в різноманітних сферах суспільного життя і в прикладних інформаційних системах, які обслуговують ці сфери, зокрема:

- персоніфікована ідентифікація для доступу до операційних систем і локальних мереж, при підтвердженні особи користувачів комп'ютерних програм, де необхідно пройти процедуру авторизації;
- автентифікація під час доступу до вебресурсів;
- визначення конкретної фізичної особи в системах контролю доступом;
- облік робочого часу персоналу підприємств і установ;
- реєстрація та ідентифікація клієнтів;
- підтвердження особистості клієнтів під час здійснення електронних платежів;

- впровадження соціальних проєктів, що вимагають ідентифікаційних процедур (електронне урядування, біометричні системи голосування, благодійні акції тощо);

- ідентифікація або верифікація в різних державних і міжнародних проєктах, таких як оперативна перевірка осіб, контроль при перетинанні державних кордонів, видача віз тощо.

Для біометричної ідентифікації особи можна застосовувати тільки ті методи та технології, які можуть високодостовірно й однозначно ідентифікувати особу, тобто мають низькі показники FAR та FRR. Використання технологій біометричної ідентифікації з кількома методами біометрії підвищує надійність, достовірність ідентифікації та забезпечує *багатофакторну ідентифікацію*.

#### Список використаних джерел

Jain, A., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79, 80–105. <https://doi.org/10.1016/j.patrec.2016.01.002>

Jain, A., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1). <https://doi.org/10.1109/TCSVT.2003.818349>

Jain, A. K., Flynn, P., & Ross, A. A. (2007). *Handbook of biometrics*. Springer, Science & Business Media. <https://doi.org/10.1007/978-0-387-71041-9>

#### References

Jain, A., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79, 80–105. <https://doi.org/10.1016/j.patrec.2016.01.002>

Jain, A., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1). <https://doi.org/10.1109/TCSVT.2003.818349>

Jain, A. K., Flynn, P., & Ross, A. A. (2007). *Handbook of biometrics*. Springer, Science & Business Media. <https://doi.org/10.1007/978-0-387-71041-9>

**Отримано редакцією журналу / Received: 11.09.24**

**Прорецензовано / Revised: 23.09.24**

**Схвалено до друку / Accepted: 01.10.24**

Ievgen RIMEK, Director  
ORCID ID: 0009-0008-1934-7625  
e-mail: e.rimek@biosol.ua  
Limited Liability Company "Biosol Ukraine", Kyiv, Ukraine

Viacheslav KOLOMYTSEV, Deputy Director  
ORCID ID 0009-0003-9739-2636  
e-mail: v.kolomycev@biosol.ua  
Limited Liability Company "Biosol Ukraine", Kyiv, Ukraine

Artem RIMEK, Master of Arts  
ORCID ID: 0009-0007-7500-4267  
e-mail: a.rimek@biosol.ua  
Limited Liability Company "Biosol Ukraine", Kyiv, Ukraine

## THE USE OF INNOVATIVE BIOMETRIC TECHNOLOGIES IN APPLIED INFORMATION SYSTEMS

*The paper examines the main modern methods and technologies of biometric identification, their classification, and practical application in applied information systems in the context of current challenges and risks that can be addressed using biometric user identification. The key types of tasks considered are: a) access control to premises and critical zones; b) access to information resources, documents, databases, and applied information systems; c) user identification at the workplace or remotely and login to the operating system or applied information systems without the use of passwords or PIN codes to enhance protection against fraud, hacking attacks, and insider threats; d) the use of biometrics for identity verification in business processes.*

**Keywords:** *biometric methods, biometric technologies, person identification, protection of information systems, access control, information protection, information security.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.