

ПОКАЗНИКИ FRR І FAR ЯК КРИТЕРІЇ ОЦІНЮВАННЯ НАДІЙНОСТІ БІОМЕТРИЧНИХ МЕТОДІВ

В умовах зростаючих загроз інформаційній безпеці, зокрема несанкціонованого доступу до критичних об'єктів, сучасні організації стоять перед викликом вибору і впровадження надійних рішень ідентифікації особистості. Біометричні технології створюють низку важливих переваг, серед яких висока точність і швидкість, водночас, вибір найбільш прийнятної біометричної рішення для конкретної організації чи виконання певної функції є нелегким завданням і потребує ретельного оцінювання різних методів біометрії.

Встановлено, що основними критеріями оцінювання біометричних методів є універсальність, унікальність, постійність, вимірюваність, доступність, зручність і простота використання, ймовірність фальсифікації, вартість встановлення та експлуатації технології тощо. У контексті інформаційної безпеки важливим чинником вибору біометричного рішення є його надійність, основними критеріями оцінювання якої є показники хибних відмов FRR і хибних допусків FAR.

Дослідження показало, що чим менше значення обох показників, тим вища надійність біометричного методу: низький рівень FRR вказує на більш надійну та зручну біометричну систему, а низький показник FAR – на вищий рівень її безпеки. Водночас, провадження надійної біометричної системи з низькими показниками FAR і FRR є більш дорогавартісним. З'ясовано, що біометричні методи мають суттєві відмінності за обома показниками.

У результаті порівняння найпопулярніших біометричних методів (на основі відбитків пальців, геометрії обличчя та руки, голосу; райдужної оболонки ока) за такими факторами як FRR і FAR, ймовірність фальсифікації, стабільність, чутливість до середовища, швидкість роботи, простота і вартість встановлено, що найкращі показники мають методи ідентифікації за райдужною оболонкою ока, 3D розпізнавання обличчя і відбитками пальців.

Ключові слова: методи біометричної ідентифікації, критерії оцінювання біометричних методів, показник хибних відмов FRR, показник хибних доступів FAR.

Вступ

На сучасному етапі біометричні технології ідентифікації особистості отримали значне поширення в різних сферах життєдіяльності людини. Як свідчить статистика, у 2024 році 28% респондентів відали перевагу використанню біометричних технологій для входу в онлайн-облікові записи, програми та смарт-пристрої, в той час як, наприклад, складні паролі, відомі тільки власнику, обрали 17% опитаних, а одноразові паролі, що надсилаються на мобільні пристрої – 13%, решта варіантів отримали підтримку 8% осіб і нижче [1].

Серед найбільш відомих прикладів використання біометрії варто згадати ID-картки й паспорти із вбудованими зразками відбитків пальців; технології автентифікації користувачів смартфонів: за відбитками пальців, наприклад, Touch ID і Face ID від iPhone, голосом, наприклад, Google Pixel 8 Pro, сканування райдужної оболонки ока - Galaxy S8, S9, Note8 і Note9 (хоча в наступних моделях від такої функції відмовилися); платіжні системи з голосовою біометрією, наприклад від компанії PCI Pal; безготівкова оплата за допомогою методу сканування рисунку вен людини; біометричні системи контролю доступу в аеропортах на основі сканування обличчя, зокрема розробка відомої японської корпорації NEC; ідентифікація зловмисників та розкриття злочинів за допомогою різних біометричних методів тощо.

Формулювання проблеми

Незважаючи на багато переваг біометричних технологій, серед яких висока точність, швидкість і відсутність потреби носити з собою додаткові засоби для ідентифікації, сьогодні досить гостро стоїть питання оцінювання й вибору найбільш прийнятної методу для конкретної організації чи виконання певної функції. Ключову роль у цьому процесі відіграють показники надійності біометричних технологій: FRR (показник хибних відмов) і FAR (показник хибних допусків).

Метою дослідження є встановити сутність показників FRR і FAR для біометричних технологій, з'ясувати середні значення FAR і FRR для найбільш популярних методів біометричної ідентифікації та запропонувати рекомендації щодо їх використання.

Аналіз літератури

У ході підготовки статті було розглянуто низку публікацій закордонних дослідників, які займалися питаннями безпеки і точності біометричних систем [2], в тому числі на основі відбитків пальців [3] і визначення геометрії обличчя [4, 5], вивчали різні біометричні технології як інструменти безпеки і провели аналіз їхніх характеристик, в тому числі за FRR і FAR [6], досліджували особливості різних методів біометричної ідентифікації, їх переваги й недоліки [7], здійснили оцінювання біометричних систем за різними показниками, в тому числі FRR і FAR [8, 9].

Аналіз вітчизняної літератури за темою дослідження показав, що низка публікацій присвячена проблемам біометричних технологій, зокрема аналізу основних методів біометричної автентифікації [10, 11], порівнянню методів біометричної автентифікації [12-14], формулюванню критеріїв вибору біометричних систем [15] тощо.

Також при підготовці статті було розглянуто публікації компаній-розробників біометричних продуктів [16-18], аналіз яких показав використання провайдером біометричних рішень науково обґрунтованих підходів до розробки своїх продуктів.

Основна частина

Сучасні системи безпеки в багатьох випадках базуються на багатофакторній ідентифікації, одним із видом якої є біометричні методи, які використовують поведінкові або фізіологічні характеристики людини для перевірки її особи.

На сьогодні у практиці інформаційної безпеки використовують близько 20 видів біометричних методів, які базуються на розпізнаванні фізіологічних ознак (відбитки пальців, геометрія обличчя, райдужна оболонка й сітківка ока, голос, візерунок вен на долоні або пальці, серцебиття, ДНК, запах тощо) або поведінкових характеристик людини (хода, підпис, стиль натискання клавіш клавіатури комп'ютера). Серед перелічених технологій є більш поширені й такі, що тільки розвиваються.

В умовах наявності великої кількості альтернативних методів біометричної ідентифікації для організацій, які прагнуть забезпечити ефективні ідентифікацію й управління доступом, актуальною залишається проблема вибору найбільш прийняттого варіанту.

Загальними критеріями оцінювання й вибору біометричного методу є (рис. 1):

Критерії оцінювання й вибору біометричних методів	
Універсальність	Надійність
Унікальність	Вимірюваність
Постійність	Залежність від зовнішніх умов
Швидкість	Можливість безконтактної перевірки на ходу
Прийнятність: доступність, зручність, простота використання	Ймовірність фальсифікації
Легкість запам'ятовування і навчання правилам використання	Вартість встановлення та експлуатації

Рис. 1. Критерії оцінювання й вибору біометричних методів

- універсальність: характеристика притаманна кожній особі;
- унікальність: риса характерна окремій особі максимально відрізняється від аналогічних рис інших осіб;
- постійність: дана ознака характерна індивіду впродовж усього життя;
- вимірюваність: ознаку можна виміряти в кількісних показниках;
- прийнятність: можливості використання є доступними, зручними і простими для користувачів [7, 8].

Оцінюючи біометричні методи, також беруть до уваги швидкість процесу перевірки, можливість безконтактної перевірки на ходу, легкість запам'ятовування і навчання користування системою, залежність від зовнішніх умов, наприклад освітленості, ймовірність фальсифікації (введення системи в оману з використанням шахрайських методів), вартість встановлення та експлуатації технології [13, 14].

Слід відзначити, що серйозною проблемою біометричних технологій є їхня недостатня надійність, під якою розумітимемо властивість інформаційної або технічної системи зберігати протягом встановленого часу значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування [19]. Одним із параметрів надійності біометричної ідентифікації є ймовірність відмов і хибних спрацювань біометричної системи. Помилка першого типу FRR (False Rejection Rate) означає хибну відмову в доступі легітимному користувачу і називається помилковим негативним результатом. Помилка другого типу FAR (False Acceptance Rate) передбачає надання хибного доступу неавторизованому користувачу і називається помилковим позитивним результатом.

Побіжно слід відзначити, що вітчизняні науковці розглядають зазначені показники для оцінювання якості [13, 14] або надійності біометричних систем [15], у той час як у публікаціях західних авторів їх переважно використовують як індикатори результативності (performance) біометричних технологій [8, 16].

Отже, показник помилкової відмови в доступі FRR визначається таким чином:

$$FRR = \frac{N_{FA}}{N_{IA}(IVA)} * 100\%,$$

де:

N_{FA} – кількість неавторизованих допусків;

N_{IA} – кількість спроб ідентифікації авторизованих користувачів;

N_{IVA} – кількість спроб перевірки неавторизованих користувачів;

Показник помилкового доступу FAR може бути визначений так:

$$FAR = \frac{N_{FR}}{N_{EIA}(EVA)} * 100\%,$$

де:

N_{FR} – кількість хибних відмов;

N_{EIA} – кількість спроб ідентифікації користувачів;

N_{EVA} – кількість користувачів в усіх спробах перевірки [2].

У таблиці 1 показано співвідношення між точністю та швидкістю обробки в біометричних системах при різних рівнях показників FRR і FAR [9].

Високий показник помилкових відмов у доступі FAR свідчить, що біометрична технологія хибно надає доступ більшості неавторизованих осіб. Натомість низький показник FAR означає, що хибний доступ надається дуже невеликій кількості користувачів, які не мають на це права. Зазвичай існує компроміс між цими двома помилками, який може вплинути на рівень точності і швидкість обробки в процесі верифікації, а також на загальні витрати.

Нижчий рівень FRR вказує на більш надійну та зручну біометричну систему. Нижчий показник FAR свідчить про вищий рівень безпеки. Закономірним є те, що біометричні системи з високими показниками FAR і FRR мають значно нижчу вартість. В ідеалі біометрична

система повинна мати дуже низькі FAR і FRR, щоб забезпечити високу якість ідентифікації користувачів. Однак це призведе до збільшення витрат на реалізацію і супровід системи.

Розглянемо співвідношення показників FAR і FRR на графіку (Рис. 2) [2].

Таблиця 1.

Співвідношення між точністю та швидкістю обробки в біометричних системах

Ймовірність хибного пропуску неавторизованого користувача, FAR	Ймовірність хибної відмови в доступі авторизованому користувачу, FRR		
		Низький FRR	Високий FRR
	Низький FAR	Висока точність пропуску законних користувачів і відмови порушникам. Нижча швидкість обробки й більші витрати на систему.	Висока точність запобігання доступу неавторизованих осіб. Нижча швидкість через велику кількість відмов законним користувачам.
	Високий FAR	Вища швидкість обробки, менше число відмов законним користувачам. Низька точність внаслідок надання доступу більшому числу порушників.	Висока швидкість обробки, але з дуже низькою точністю перевірки законних користувачів і відхилення порушників.

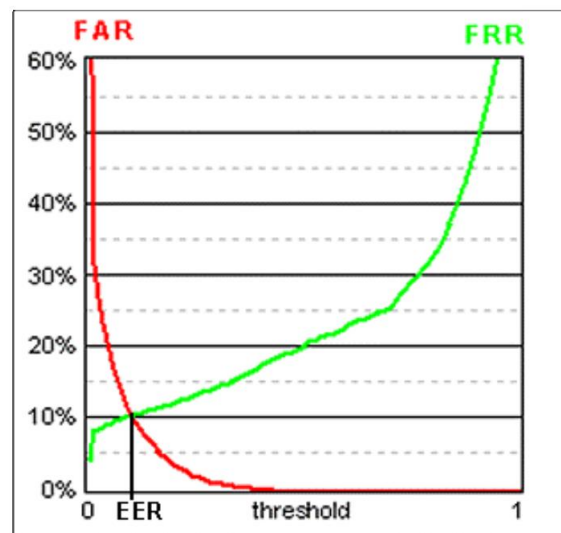


Рис. 2. Співвідношення показників FAR і FRR

Точка EER (Equal Error Rate) – показник однакової частоти помилок першого і другого типу, який представляє точку, де FAR і FRR мають однакові значення. Точка перетину є хорошим показником загальної надійності біометричного методу/пристрою. Показник нижче даної точки означає вищу надійність EER біометричної технології.

Слід відзначити, що різні біометричні методи мають суттєві відмінності в показниках хибних відмов і допусків. Більшість сучасних біометричних систем мають відсоток хибних відмов легітимним користувачам (FRR) від 0,1% (законному користувачеві в середньому буде відхилено один раз із тисячі) до 20% (законному користувачеві буде відхилено в середньому один раз із п'яти).

Показник помилкового доступу (FAR) коливається в середньому від 0,01% (один хибний дозвіл неавторизованому користувачу на 100 спроб ідентифікації) до 100 хибних спрацьовувань на 10 мільйонів спроб (0,00001%) [9].

Оскільки кожна біометрична система передбачає певний баланс між показниками FAR і FRR, для вибору економічно ефективного варіанту біометричного застосування необхідно

враховувати конкретні вимоги до кожної технології. Коли йдеться про системи з великою кількістю користувачів (платіжні системи, обробка важливих конфіденційних даних), доцільно орієнтуватися на низькі коефіцієнти FAR: від 0,0000001% і менше [18]. Натомість у випадку, наприклад, використання біометрії для розблокування корпоративного смартфона, який не містить критичних даних, низький FRR є прийнятним, оскільки користувач віддає перевагу швидкості на противагу безпеці.

Прийнятним для біометричної системи є показник хибних відмов FRR приблизно 0,01%, оскільки такий відсоток можна пом'якшити в результаті проведення додаткових спроб перевірки. У разі необхідності перевірки великого потоку користувачів показник FRR необхідно покращувати до 0,001 - 0,0001%, щоб уникнути черг.

Таким чином, можна зробити висновок, що помилка надання хибного допуску FAR є більш критичною у контексті забезпечення інформаційної безпеки, а помилка хибної відмови в доступі FRR насамперед призводить до зменшення зручності використання біометричної системи для користувачів.

Як свідчить статистика за 2022 рік [20], найбільш популярними серед користувачів методами біометричної ідентифікації є: сканування відбитків пальців (44% опитаних); розпізнавання обличчя (26%); визначення голосу (5%); сканування райдужної оболонки ока і геометрії руки (по 2%). Опитування від Statista 2024 року [1] також підтверджують лідируючі позиції технологій сканування відбитків пальців і розпізнавання обличчя.

На основі дослідження [14], у рамках якого методом аналізу ієрархій встановлено середні значення показників FAR та FRR для різних біометричних систем, а також напрацювань [7-9] здійснено порівняння перелічених вище біометричних методів за сукупністю факторів: показниками хибних допусків і хибних відмов, фальсифікація, стабільність, чутливість до середовища, швидкість роботи, простота, вартість (табл.2).

Таблиця 2.

Порівняння біометричних методів за сукупністю факторів

Біометрична ознака	FAR, %	FRR, %	Фальсифікація	Стабільність	Чутливість до середовища	Швидкість роботи	Простота	Вартість, \$
Відбиток пальця	0,001	0,6	Можлива	Низька	Висока	Висока	Середня	Низька від 60 до 600
Геометрія обличчя 2D	0,1	2,5	Можлива	Низька	Висока	Середня	Висока	Низька
Геометрія обличчя 3D	0,0005	0,1	Проблематична	Висока	Низька	Низька	Середня	Висока до 45000
Райдужка ока	0,00001	0,016	Неможлива	Висока	Середня	Висока	Висока	Середня від 500 до 6000
Голос	1	1	Можлива	Низька	Середня	Висока	Висока	Низька

У даному контексті найвищі показники надійності зручності показали методи ідентифікації за райдужною оболонкою ока, 3D розпізнавання обличчя та відбитками пальців. У найближчому майбутньому саме ці біометричні методи можуть стати найбільш прийнятними рішеннями для подолання загроз у сфері інформаційної безпеки.

Для підвищення рівня надійності біометричних технологій у випадках необхідності перевірки користувачів для отримання доступу до секретних об'єктів, об'єктів критичної інфраструктури або виконання завдань державного чи міждержавного масштабу, де є потреба

в ідентифікації за величезними базами даних з мільйонами записів, доцільно використовувати прийоми для ускладнення системи, наприклад, перевірку обох очей або кількох пальців замість одного, використання результатів 2D і 3D сканування обличчя одночасно, впровадження комбінованих систем, наприклад сканування пальця і райдужної оболонки ока. а також поєднання біометричних методів з іншими методами ідентифікації.

Висновки і рекомендації

Безумовно, вибір методу біометричної ідентифікації в першу чергу залежить від вимог до нього з боку організації, оскільки кожен з варіантів має свої переваги й недоліки. Порівняння біометричних методів за сукупністю розглянутих вище факторів дає підстави для прийняття обґрунтованого рішення щодо впровадження найбільш прийнятної біометричної технології або їх поєднання.

Дослідження показало, що важливу роль при виборі біометричного методу відіграє критерій надійності, основними параметрами якої є показники хибної відмови FRR і хибного доступу FAR. Встановлено, що в ідеалі біометрична система повинна мати дуже низькі відсотки FAR і FRR, щоб забезпечити високу надійність ідентифікації. В реальності існує компроміс між цими двома показниками, який відображає рівень надійності й точності, з одного боку, та зручність використання і швидкість процесу біометричної верифікації, з іншого, а також свідчить про загальні витрати на впровадження й експлуатацію біометричної системи.

Низькі показники FAR показують на високий рівень надійності, а, отже, й безпеки біометричного методу, а низький рівень FRR вказує на більш швидку й зручну для користувача біометричну систему. Водночас, низькі відсотки обох показників є ознаками значної вартості реалізації і супроводу системи.

Слід відзначити, що різні біометричні методи мають суттєві відмінності в показниках хибних відмов і допусків. Більшість сучасних біометричних систем мають відсоток FRR від 0,1% до 20%, а рівень FAR коливається в середньому від 0,01% до 0,00001%.

Порівняльний аналіз найбільш популярних за статистикою біометричних методів (на основі відбитків пальців, геометрії обличчя та руки, голосу; райдужної оболонки ока) за такими факторами як FRR і FAR, ймовірність фальсифікації, стабільність, чутливість до середовища, швидкість роботи, простота і вартість показав, що найкращі показники мають методи ідентифікації за райдужною оболонкою ока, тривимірним розпізнаванням обличчя і відбитками пальців.

Підсумовуючи, слід зауважити, що підвищити рівень надійності біометричних систем можна шляхом їх ускладнення, впровадження комбінованих біометричних систем, а також поєднання біометричних методів з іншими методами ідентифікації. Крім цього такі системи мають бути надійно захищені від несанкціонованого доступу до біометричних даних користувачів.

Перелік посилань

1. Preferred ways to sign-in to online accounts, apps, and smart devices in selected countries in 2024. *Statista*. URL: <https://www.statista.com/statistics/1448883/preferred-security-authentication-methods-in-selected-countries/>
2. Milan Adámek, Miroslav Matýšek, Petr Neumann. Security of Biometric Systems 2015. URL: <https://www.sciencedirect.com/science/article/pii/S1877705815003823>
3. Wencheng Yang, Song Wang, Jiankun Hu, Zheng Guanglou. Security and Accuracy of Fingerprint-Based Biometrics: A Review 2019. URL: https://www.researchgate.net/publication/330711092_Security_and_Accuracy_of_Fingerprint-Based_Biometrics_A_Review
4. Manal Abdullah, Majda Wazzan, Sahar Busaeed. Optimizing Face Recognition Using PCA. 2012. URL: https://www.researchgate.net/publication/225279599_Optimizing_Face_Recognition_Using_PCA
5. Ziaul Haque Choudhury. Biometrics security based on face recognition. 2013. URL: <https://bsaulibrary.files.wordpress.com/2017/02/2013-biometrics-security-based-on-face-recognition.pdf>
6. Anil K. Jain, Arun Ross, S. Pankanti. Biometrics: a tool for information security. 2006. URL: https://www.researchgate.net/publication/3455239_Biometrics_a_tool_for_information_security_IEEE_Transactions_on_Forensic_Security

7. Reetu Awasthi, R.A.Ingolikar. A Study Of Biometrics Security System. 2013. URL: https://www.internationaljournalcorner.com/index.php/ijird_ojs/article/view/133344/92551
8. Mohamad El-Abed Christophe Charrier Christophe Rosenberger. Evaluation of Biometric Systems. 2012. URL: https://www.researchgate.net/publication/257365353_Evaluation_of_Biometric_Systems
9. Babita Gupta. Biometrics: Enhancing Security in Organizations. *IBM Center for The Business of Government*. 2008. URL: <https://www.businessofgovernment.org/sites/default/files/GuptaReport.pdf>
10. Олешко І. В. Порівняльний аналіз методів автентифікації з відбитку пальця. Харків: ХНУРЕ, 2011. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/9f8b266f-7783-43f0-9b46-dfacc92f7ee1/content>
11. Олешко І. В. Моделі та методи оцінки захищеності механізмів багатофакторної автентифікації від несанкціонованого доступу: Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук. Харків : ХНУРЕ, 2014. 126 с.
12. Бугаєнко Х. А., Горбенко І. Д. Аналіз трьох біометричних методів автентифікації особи: наук.-техн. журнал. Харків : ХНУРЕ, 2012. 266 с.
13. Безрук В.М., Кобцева В.М. Порівняння методів біометричної автентифікації за сукупними показниками якості. Харків: ХНУРЕ. URL: <https://openarchive.nure.ua/server/api/core/bitstreams/af6afb36-6ddd-425f-be72-c0dfdcd5efdc/content>
14. Скорик Ю., Безрук В. Вибір переважного методу біометричної автентифікації. *International Science Journal of Engineering & Agriculture*. 2023. № 2(4). С. 28-34.
15. Луцків А. М., Крутигорова О. І. Критерії вибору систем біометричної автентифікації. Тернопіль: ТНТУ ім. І. Пулюя, 2016. URL: https://elartu.tntu.edu.ua/bitstream/123456789/20215/2/ConfATMT_2016vII_Lutskiv_A_M-Selection_criteria_of_biometric_71-72.pdf
16. FAR and FRR: security level versus ease of use Recogtech. *Recogtech*. URL: <https://recogtech.com/en/insights-en/far-and-frr-security-level-versus-ease-of-use/>
17. False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics. *Bayometric*. URL: <https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/>
18. What you need to know about FRR and FAR. *Cursor Insight*. URL: <https://www.linkedin.com/pulse/what-you-need-know-frr-far-cursor-insight/>
19. ДСТУ 2860-94 Надійність техніки. Терміни та визначення. URL: https://dbn.co.ua/load/normativy/dstu/dstu_2860_94_nadijnist_tekhniki_termini_ta_viznachennja/5-1-0-1209
20. Eduardo Garcia. Has COVID-19 monitoring changed how UK consumers feel about sharing biometric data? *Capterra*. URL: <https://www.capterra.co.uk/blog/2715/covid-monitoring-and-biometric-data-uk-consumers>

Надійшла 02.02.2025