УДК 621.391

ДО ПИТАННЯ ОЦІНКИ ЕФЕКТИВНОСТІ БІОМЕТРИЧНИХ СИСТЕМ

М.О. ПАСТУШЕНКО,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

М.С. ПАСТУШЕНКО, М.О. ПЕТРАЧЕНКО
Харківський національний університет радіоелектроніки

Abstract *– The current scientific task of quantitative assessment of the effectiveness of existing and developing biometric systems is considered. Known works on the comparative analysis of biometric systems, as a rule, discuss their characteristics and principles of operation. However, there is no data on the quantitative assessment of the effectiveness of biometric systems, of which there are quite a few on the market. In the proposed work, an attempt is made to eliminate this shortcoming. The development is based on a systematic approach, namely the efficiency/cost criterion. When evaluating efficiency, the main characteristics of biometric systems are used - errors of the first and second kind, the estimates of which are given and analyzed in the scientific literature. At the same time, it is possible to take into account various consequences caused by errors of the first and second kind. For this, a special coefficient is introduced. For the first time, a quantitative comparative analysis of biometric systems used in modern access control and management systems, namely dactyloscopy, 2D and 3D facial geometry, and voice, was carried out. According to the results of research, dactyloscopy (fingerprints) turned out to be the most effective. The 2D face geometry, which is quite widely used in mod-ern access control and management systems, has the worst performance indicators ac-cording to the developed criterion. In order to increase the efficiency of voice systems, it is proposed to reduce the probability of false recognition by an order of magnitude, for example, due to accounting for the phase data of the processed signals. The developed criterion is characterized by simplicity, correctness, physical clarity, completeness of accounting of the main characteristics of reliability and reliability, and can also be used to assess the current state of known biometric systems, as well as to determine the main directions of their improvement. The obtained results can be used both at the stage of development and selection of biometric systems.*

Анотація – Розглядається актуальне наукове завдання кількісної оцінки ефективності існуючих та розроблюваних біометричних систем. У відомих роботах щодо порівняльного аналізу біометричних систем, як правило, обговорюються їх характеристики та принципи роботи. Однак, відсутні дані кількісної оцінки ефективності біометричних систем, яких на ринку досить багато. У запропонованій роботі зроблено спробу усунути цей недолік. В основу розробки покладено системний підхід, а саме критерій ефективність/вартість. При оцінці ефективності використовуються основні характеристики біометричних систем - помилки першого і другого роду, оцінки яких наводяться та аналізуються у науковій літературі. При цьому є можливість урахування різних наслідків, зумовлених помилками першого та другого роду. Для цього запроваджується спеціальний коефіцієнт. Вперше проведено кількісний порівняльний аналіз біометричних систем, які використовуються в сучасних системах контролю та управління доступом, а саме дактилоскопія, геометрія обличчя 2D та 3D, голос. За результатами досліджень найефективнішою виявилася дактилоскопія (відбитки пальців). Найгірші показники ефективності за розробленим критерієм має геометрія обличчя 2D, яка досить широко використовується в сучасних системах контролю та управління доступом. Для підвищення ефективності голосових систем запропоновано знизити на порядок ймовірність помилкового розпізнавання, наприклад, за рахунок обліку фазових даних сигналів, що обробляються. Розроблений критерій відрізняється простотою, коректністю, фізичною ясністю, повнотою обліку основних характеристик надійності та достовірністю, а також може бути використаний для оцінки поточного становища відомих біометричних систем, а й визначити основні напрями їх удосконалення. Отримані результати можуть бути використані як на етапі розробки, так і вибору біометричних систем.

Вступ

Відправною точкою широкого використання біометричних засобів у системах контролю та управління доступом (СКУД) можна вважати подію 9/11, яка пов'язана з терористичними актами 11 вересня 2001 року (іменовані як 9/11). Рішення про запровадження біопаспортів було ухвалено ще у травні 2003 р. на зустрічі міністрів внутрішніх справ країн Великої Вісімки (G8).

Планувалося, що в проїзні документи буде додано мікрочіп, що містить біометричні дані, які перевірятимуться при прикордонному контролі: дані, записані в паспорті, будуть порівнюватися з даними людини, що перетинає кордон, автоматично спеціальним програмно-апаратним комплексом. Стандарти в галузі біометричних паспортів, обрала обличчя як основу біометрики та розробила вимоги до її якості з електронною цифровою фотографією (двовимірною або тривимірною), що задовольняє стандарту. При перетині кордону фотографія на чіпі в паспорті звіряється з особою людини, яка перетинає кордон, і при їх збігу з певним ступенем точності видається дозвіл на в'їзд.

Кожна країна має право посилити прикордонний контроль, додавши ще один або два біометричні параметри, наприклад відбиток пальця або райдужку ока. Проте вони є не обов'язковими.

Бурхливий розвиток і досить широке використання біометричних систем у різних сферах людської діяльності, в тому числі і в сучасних телекомунікаційних системах, висуває на перший план надійність їхнього функціонування. В основу роботи біометричних систем покладено методи теорії перевірки статистичних гіпотез у математичній статистиці, які дуже широко та ефективно використовуються у ряді сучасних технічних систем. Надійність таких систем характеризується помилками першого та другого роду.

Поняття надійності, як правило, поділяють на три великі аспекти [1, 2]. Перший, зазвичай, обговорюють виробники біометричного устаткування. Йдеться про імовірнісний характер виробленої біометричними системами автентифікації (ідентифікації). Тому всі біометричні системи характеризуються параметрами: FAR (False Acceptance Rate, хибне розпізнавання) та FRR (False Rejection Rate, хибна відмова).

Ряд авторів [3-6] як оптимальний варіант вибору значень зазначених помилок пропонують використовувати порівняльну характеристику EER (Equal Error Rate, рівний коефіцієнт помилок). Ця характеристика визначає точку, де величини FRR і FAR рівні. Як показано в [1], це твердження не справедливе, оскільки наслідки помилок першого і другого роду суттєво відрізняються. Наприклад, у сучасних радарах систем попередження про ракетний напад умовна ймовірність помилкової тривоги (помилка першого роду) перебувати на рівні 10^{-12} і нижче. При цьому вимоги до помилок другого роду не такі жорсткі.

Другий аспект (не)надійності біометричних систем фірмами виробниками старанно замовчується. Йдеться про захищеність систем від свідомого обману, про способи симулювати об'єкт біометричного сканування. Відомі способи обману біометричних систем контролю доступу по відбитку пальця. Наприклад, досліди японського криптографа Цутому Мацумото. Фахівцям у галузі біометрії всі ці факти були давно відомі, проте результати подібних досліджень свідомо замовчуються. Вихід зі становища не простий, він вимагає залучення складніших у використанні і дорожчих методів біометрії (а краще – багатофункціональну автентифікацію), що відразу ставить під удар саму ідею повсюдного поширення біометричних технологій. Прийнятного рі-

шення на даний момент можна досягти комбінованої перевіркою - зчитуванням декількох параметрів, наприклад відбитка пальця і голосу, використанням біометричного контролю разом зі смарткартами тощо.

Нарешті, третім аспектом проблеми надійності є питання безпеки зібраної біометричної інформації. Більшість біометричних систем уразливі для злому за допомогою перехоплення, збереження та подальшого відтворення даних. Наскільки це можливо, залежить від методу передачі біометричної інформації по мережі. Однак це ще півбіди. Найгірше те, що будь-який біокод, на відміну від безособового коду-паролю, практично завжди несе в собі набагато більше інформації, ніж це потрібно для перевірки доступу. Навіть малюнок райдужної оболонки ока, не кажучи вже про ДНК код, може повідомити фахівця важливу інформацію про стан індивідуума, його вроджених або набутих властивостях, у тому числі хворобах. А ця інформація, очевидно, є надто інтимною, щоб давати доступ до неї не тільки своєму лікарю. Можливі зловживання очевидні кожному – від дискримінації прийому працювати до прямого шантажу.

Разом з тим, у сучасних біометричних системах для розпізнавання особистості використовуються різні фізіологічні та поведінкові характеристики особи, такі як, відбитки пальців, райдужна та сітчаста оболонки ока, голос, ручний підпис, геометрія руки, малюнок вен на руці тощо. Відомі роботи з порівняльного аналізу біометричних систем [3-7] не дають відповіді, яка з систем краща. Як правило, аналіз закінчується наведенням характеристик та розглядом принципів роботи аналізованих систем. Тому актуальним є наукове завдання розробки критерію для порівняльного аналізу, бажано кількісного, аналізованих біометричних систем.

У статті розглядатимемо лише ті біометричні ознаки, які застосовуються в СКУД або в близьких їм завданнях. А саме, основна увага буде приділена біометричним системам, які використовують як ознаки геометрію обличчя, відбитки пальців та голос. Такий вибір обумовлений також поширеністю вказаних систем. Наприклад, відбитки пальців займають приблизно 60% ринку біометричних систем; геометрія особи відповідно до 20%; голос – до 10%.

Голосові системи включені до переліку аналізованих з низки причин. У першу чергу, це переваги, які не притаманні іншим системам: простота, зручність, економічність, можливість реалізації процедур автентифікації дистанційно та ін. Крім цього, голосові системи можуть бути вдосконалені, наприклад, за рахунок використання фазових даних [8-10] . Очевидно, тому нині найбільший український банк Приват запроваджує голосову автентифікацію.

Мета статті – розробити критерій та виконати порівняльний кількісний аналіз обраних біометричних систем.

I. Аналіз характеристик біометричних систем та розробка критерію

У першу чергу проаналізуємо основні параметри розглянутих систем, які характеризують їхню надійність. Основні характеристики аналізованих систем представлені

в табл. 1. Тут слід зауважити, що, як правило, виробники систем, які розглядаються, приховують як основні характеристики, так і вартість обладнання. Узагальнивши дані, які представлені в роботах [2-7], та доступну інформацію із мережі Інтернет були отримані величини, розміщені в табл. 1. Тобто вони відображають порядок величин, не претендуючи на точність.

Таблиця 1. Основні характеристики біометричних систем

№ з/п	Використана ознака	FAR, %	FRR, %	Фальсифікація	Поширеність	Вартість, USD
1	Відбитки пальців	0,001	0,6	Можлива	Висока	від 500
2	Геометрія обличчя 2D	0,1	2,5	Можлива	Висока	від 1000
3	Геометрія обличчя 3D	0,0005	0,1	Проблемати-чна	Середня	від 10000
4	Голос	0.01	3	Проблемати-чна	Середня	від 50

Як додаткові характеристики біометричних систем розглядають такі:

- час ідентифікації – скільки часу знадобиться для коректного збору біометричних даних та їх розпізнавання;

- зручність збору біометричної інформації: наприклад, аналіз крові або поту дозволить точно ідентифікувати людину, проте процедура взяття цих біологічних рідин потребує спеціального обладнання та додаткового часу;

- широта охоплення: наприклад, пропускна здатність Big Data системи біометрії на основі відеоаналітики потоку людей в режимі онлайн значно вища, ніж при скануванні пальців, долонь, очей або інших частин тіла кожної людини окремо;

- спосіб збору біоданих – поки контактні способи точніше, ніж безконтактні, але перші вимагають більше часу та відрізняються меншою пропускною здатністю;

- стійкість до завад, що означає низькі показники FRR та FAR, у зв'язку з наявністю завад у матеріалах реєстрації або низькою якістю представлених даних;

- необхідна інфраструктура – Big Data засоби для зберігання біометричних шаблонів (наприклад, HBase Apache Hadoop або інші NoSQL – системи управління базами даних), фреймворки аналітичної обробки за допомогою алгоритмів Machine Learning (Apache Spark, Flink), а також сенсори та інші інтелектуальні пристрої інтернету речей (Internet of Things, IoT), які будуть збирати та передавати оцифровані біометричні дані для їх звіряння з шаблонами в базі. Іноді вся ця інфраструктура може уміститися в рамках одного смартфона, а для великих біометричних систем типу індійського AADHAAR потрібні масштабні розподілені рішення на основі високонадійних кластерів;

- контекст програми, що включають місце та особливості використання системи біометрії, наприклад, відеокамери вуличного спостереження, контроль в аеропортах, пропускні пункти на режимних об'єктах, онлайн-банкінг, телемедицина тощо.

Розглянуті характеристики враховуються по-різному й часто використовують експертні оцінки.

Проблема формулювання кількісного критерію до оцінюваних систем є виключно складною, і часто не може бути вирішена на основі строго формальних обґрунтувань і методів розрахунку. Важливе значення при цьому має той факт, що для вибору найкращих рішень достатньо мати критерій оцінки порівняльної цінності окремих альтернатив і не обов'язково давати адекватний абсолютний вимір величини вартості, корисності чи ефективності. Звернімо увагу на відомий критерій «ефективність/вартість».

Критерій ефективність/вартість у найбільш розгорнутій формі є ґрунтовне і кошторисне дослідження, здійснення якого доцільно, перш за все, при розробці великих заходів, пов'язаних зі значними одноразовими і поточними витратами. Разом з тим, загальна методологія аналізу «ефективність/вартість» в принципі робить його досить універсальним інструментом обґрунтування рішень з управління, які можна бути використати для вирішення економічних, технічних та соціальних проблем різного масштабу.

Відомо, що економічна оцінка систем ґрунтується на трьох ключових параметрах: вартість, ефективність та час. Якщо з вартістю все гранично ясно, а саме, існують орієнтовні оцінки вартості біометричних систем (див. табл. 1), то з ефективністю виникають проблеми. Можливим є підхід до оцінки ефективності, коли її пов'язують із середнім ризиком (див. наприклад, [1]). Однак, у цьому випадку, крім оцінок надійності FAR і FRR, необхідно задати апріорні ймовірності помилкових рішень і їхню вартість. Останнє не завжди зручне.

Тому як один з варіантів вирішення зазначеної проблеми можна запропонувати побудувати оцінку ефективності залежно від основних характеристик системи, а саме, величин FAR і FRR, які з певною мірою точності відомі для більшості біометричних систем. При цьому, як відомо, для біометричних систем наслідки помилкових рішень обумовлених FRR менш важкі. Тому вплив FRR доцільно враховувати з деяким коефіцієнтом. Природно припустити, що чим менше величини FAR і FRR, тим кращою має бути ефективність. Тому вираз для критерію «ефективність/вартість» представимо в наступному вигляді

$$K = \frac{\frac{1}{FAR} \times \frac{1}{k \times FRR}}{C}, \qquad (1)$$

де $k > 1$ – деякий коефіцієнт, що знижує вплив помилок FRR, які мають менш тяжкі наслідки; C – вартість відповідної системи.

Зробимо зауваження щодо вартості аналізованих систем. У табл. 1 і при оцінці величини критерію буде використовуватися оцінка вартості, яка включає ціну додаткового обладнання та програмних засобів. Таким чином, виключено вартість обчислювальних засобів, на яких реалізована біометрична система.

II. Аналіз результатів розрахунків

Результати розрахунків за формулою (1) представлені на рис. 1.

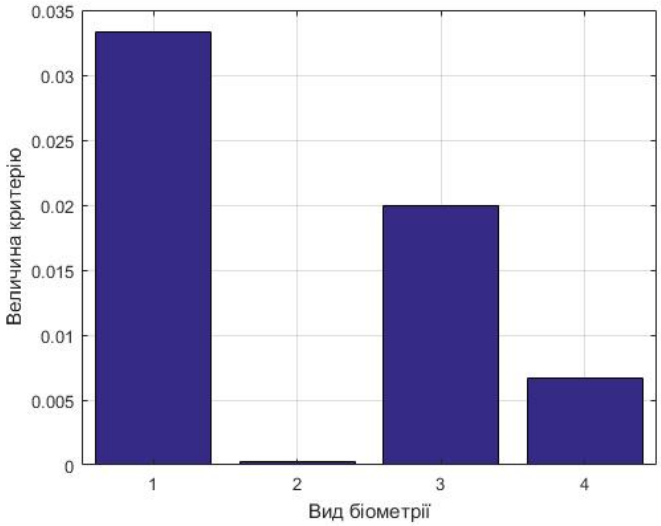

Рис. 1. Результати розрахунку критерію ефективність/вартість (поточний стан)

При цьому на рис. 1 коефіцієнт $k = 100$ і використовувалась наступна нумерація біометричних систем: 1 – відбитки пальців; 2 – геометрія обличчя 2D; 3 – геометрія обличчя 3D; 4 – голос. Результати несподівані. Основна система (геометрія обличчя 2D), з якою пов'язували свої надії країни G8 і яка широко використовується в системах доступу, має дуже низьке значення критерію «ефективність/вартість». Несподіваним є й те, що найефективнішою є дактилоскопія, яка широко використовується у сучасних СКУД. Введений критерій дає можливість визначити напрямок удосконалення голосових систем автентифікації. Наприклад, зниження FAR для цих систем на порядок змінює розстановку біометричних систем (див. рис. 2).

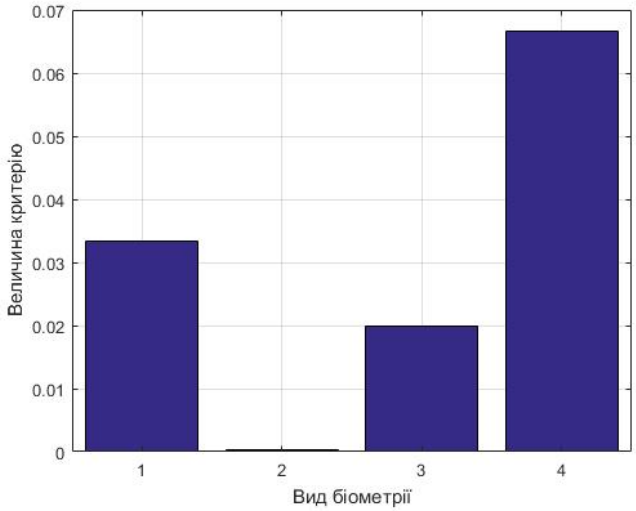

Рис. 2. Результати розрахунку критерію ефективність/вартість (при зниженні FAR голосових систем)

Такий варіант розвитку подій можливий. Обґрунтувати це можна тим, що можливості дактилоскопії та геометрії обличчя 3D вичерпані, про що свідчить аналіз наукових праць. У той же час, голосові системи своїх можливостей не вичерпали, оскільки досі обмежено використовуються фазові дані оброблюваних сигналів [8-10]. І з цим може бути пов'язане їх удосконалення.

Висновки

У роботі розглядається актуальне наукове завдання порівняльного кількісного аналізу ефективності відомих біометричних систем, які використовуються в системах контролю та управління доступом. Ефективність має враховувати основну мету системи – надійність її роботи. Тому при оцінці ефективності використовуються помилки першого і другого роду. При цьому є можливість враховувати різні наслідки цих помилок, що дає змогу зробити введений коефіцієнт. При цьому автори відмовилися від використання для оцінки ефективності показника середнього ризику. Зумовлено це тим, що потрібен більший набір вихідних даних, таких як, апріорні ймовірності та вартості помилкових рішень, оцінки значень яких досить ускладнені. Розроблений критерій відрізняється простотою, коректністю, фізичною ясністю, повнотою обліку основних характеристик і достовірністю, а також може бути використаний для оцінки поточного стану відомих біометричних систем, а також визначення основних напрямків їхнього удосконалення.

Отримані результати можна використовувати як етапі розробки, так і вибору біометричних систем. Подальші дослідження будуть орієнтовані на кількісний облік інших характеристик відомих біометричних систем.

Список літератури

1. *Пастушенко, О. М., Невлюдов, І. Ш.* (2012), "Аналіз якісних показників біометричних систем автентифікації користувачів", Проблеми телекомунікацій, No. 4(9), С. 96–103. **URL**: https://pt.nure.ua/wp-content/uploads/2020/01/124_pastushenko_biometric.pdf.

2. *Невлюдов, І. Ш., Пшеничних, С. В., Пастушенко, О. М.* (2012), "Аналіз тенденцій у розвітку систем автентифікації користувачів обчислювальних систем і мереж", Системи озброєння і військова техніка, No. 3, С. 193-196. **URL**: http://nbuv.gov.ua/UJRN/soivt_2012_3_48.

3. *Колесніков, К. В., Ободовський, Б. П.* (2017), "Види біометричної автентифікації та методи їх оценки", Штучний інтелект, No. 3-4, С. 61–69. **URL**: http://dspace.nbuv.gov.ua/handle/123456789/162340.

4. *Горбенко, І. Д., Олешко, І. В.* (2011), "Методи біометричної автентифікації для використання в паспортній системі", Прикладна радіоелектроніка, No. 10(2), С. 233–239. **URL**: https://openarchive.nure.ua/server/api/core/bitstreams/b14aabcf-cc62-4f78-ba06-0325916bc491/content.

5. *Bezruk, V., Skoryk, Y., Kobtseva, V.* (2022), Comparison of Methods of Biometric Authentication on the Total of Quality Indicators. Infocommunication and computer technologies, No. 1(01), P. 73–80. **DOI**: https://doi.org/10.36994/2788-5518-2021-01-01-05.

6. *Швець, В. А., Фесенко, А. А.* (2013), Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації, Безпека інформації, No. 19(2), С. 99–111. **DOI**: https://doi.org/10.18372/2225-5036.19.4882.

7. *Li, S. Z., Jain, A. K.* (2015) Encyclopedia of Biometrics, Second Edition, Springer Science+Business Media, 1630 p. **DOI**: https://doi.org/10.1007/978-1-4899-7488-4.

8. *Камені, Н. Г. Б., Пастушенко, М. С.* (2022), "Обгрунтування та вибір простору попередньої обробки голосового сигналу в системі автентифікації", Проблеми телекомунікацій, No. 1(30). С. 57–70. **DOI**: https://doi.org/10.30837/pt.2022.1.04.

9. *Pastushenko, M., Pastushenko, V., Pastushenko, O.* (2019), "Specifics of Receiving and Processing Phase Information in Voice Authentication Systems", Proceedings of the International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kyiv, Ukraine, 08-11 October, P. 621–624. **DOI**: https://doi.org/10.1109/PICST47496.2019.9061260.

10. *Pastushenko, M., Krasnozheniuk, Ya., Lemeshko, O.* (2020), "Analysis of voice signal phase data informativity of authentication system", Proceedings of the Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27-May 1, P. 1040–1053. **URL**: https://ceur-ws.org/Vol-2608/paper78.pdf.