КІЛЬКІСНА ОЦІНКА ЕФЕКТИВНОСТІ БІОМЕТРИЧНИХ СИСТЕМ

Пастушенко М.С., Шабохін М.О.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна

E-mail: mykola.pastushenko@nure.ua,
mykyta.shabokhin@nure.ua

Abstract

The rapid development and fairly wide use of biometric systems in various spheres of human activity, including in modern telecommunication systems, brings to the fore the reliability of their functioning. The work of biometric systems is based on the methods of the theory of testing statistical hypotheses in mathematical statistics, which are widely and effectively used in a number of modern technical systems. The reliability of such systems is characterized by errors of the first and second kind.

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.

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 1 і 2 роду суттєво відрізняються.

Другий аспект (не)надійності біометричних систем фірмами виробниками старанно замовчується. Йдеться про захищеність систем від свідомого обману, про способи симулювати об'єкт біометричного сканування.

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.

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 і т.д. .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 роботі 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 досліджень – розробка критерію та кількісний аналіз біометричних систем, які застосовуються у СКУД.

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 ефективності/вартості.

Критерій ефективність/вартість у найбільш розгорнутій формі є ґрунтовне і дороге 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, то з ефективністю виникають проблеми.

Можливий 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 їх вартість. Останнє не завжди зручне.

Тому в якості одного 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 більше має бути ефективність. В подальшому отриману оцінку ефективності будемо нормувати на вартість відповідної системи.

Результати досліджень свідчать, що 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 та приводить голосові системи у лідери СКУД.

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.

Література

1. *Пастушенко, О.М., Невлюдов, І.Ш. (2012),* "**Аналіз якісних показників біометричних систем автентифікації користувачів**", Електронне наукове фахове видання – журнал «Проблеми телекомунікацій», №.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, №, 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, № 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: наук.-техн. Журнал, Том 10. № 2, С. 233–239. URL: https://openarchive.nure.ua/server/api/core/bitstreams/b14aabcf-cc62-4f78-ba06-0325916bc491/content

5. *Безрук, В.М., Кобцева, В.М., Скорик, Ю.В.* (2019), "Сравнение методов биометрической аутентификации по совокупности показателей качества", Міжнародна науково-практична конференція High-Technologies in infocommunications 23-25 травня, Харків – Кам'янець-Подільський, Україна, С. 79-80. URL:http://openarchive.nure.ua/handle/document/10870

6. *Chastikova, V.A., Titova, A.A., Voylova, D.O.* (2022), "Analytical review of personal identification methods based on biometric characteristics", «Вестник АГУ». Вып. 1 (296). С. 92-112. DOI:10.53598/2410-3225-2022-1-296-92-112

7. *Li Stan. Z., Jain Anil. K.* (2015) Encyclopedia of Biometrics. Second Edition. Springer Science+Business Media. P. 1630. DOI: 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", Електронне наукове фахове видання – журнал «Проблеми телекомунікацій», № 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, 2019, 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, 2020, P. 1040-1053. URL: https://ceur-ws.org/Vol-2608/paper78.pdf.

.