УДК 004.93
DOI: 10.31733/2078-3566-2019-3-29-32

Гребенюк А. М. ©
кандидат технічних наук,
доцент

Краснобрижий І. В.©
кандидат юридичних наук

Мирошниченко В. О.©
кандидат технічних наук,
доцент

(Дніпропетровський державний університет внутрішніх справ)

ЕФЕКТИВНІСТЬ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ ТА ОСОБЛИВОСТІ ЇХ ВИКОРИСТАННЯ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

Розглянуто основні напрямки розвитку біометричних технологій, зроблено спроби знаходження найбільш ефективних біометричних систем, які реально існують у різних країнах світу і використовуються на практиці різними установами і організаціями, у тому числі правоохоронними органами. Розглянуто також особливості використання кожної біометричної системи, виходячи із зовнішніх чинників, таких як кількість одночасно ідентифікованих об'єктів, стан зовнішнього середовища, пропускна здатність інформаційно-телекомунікаційному обладнання.

Ключові слова: *СКУД, верифікація, ПІН-код, Proximity-картки, RFID, ID-картки, ідентифікація, біометрія, IP-камери, Web-камери, графічні процесори, відеопоток.*

Постановка проблеми. На сьогодні, у зв'язку з великою кількістю населення у містах, збільшеною мобільністю кожної окремої особи, розвитком інформаційно-телекомунікаційних систем, збільшенням потужності електронно-обчислювальних машин, які можуть бути використані для протиправних діянь, активізацією різноманітних антисоціальних угруповань, питання автоматизації ідентифікації конкретної особи стає дуже гостро. Ідентифікація особи потрібна не тільки для пошуку антисоціальних елементів, але і для оптимізації та спрощення життєвих функцій людини. Проблема ідентифікації особи, особливо в автоматичному режимі та режимі онлайн, постійно вимагає пошуку найбільш ефективних програмно-апаратних комплексів вирішення цієї задачі і знаходження критеріїв, за якими буде ідентифіковано особу. Зараз існує багато критеріїв, за якими може бути розпізнана конкретна особа, але ідентифікація за деякими критеріями дає неприйнятні помилки. Тому ідентифікація особи за її біометричними ознаками повинна виконуватись комплексно, або за тими ознаками, які дадуть нам прийнятні результати. У вирішення проблеми ідентифікації за біометричними ознаками повинна бути включена і фінансова складова. Біометричні системи, які призначені для розпізнавання особи, повинні бути як ефективними, так і найбільш доступними для організацій і установ як державного, так і приватного сектора.

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. Проблеми використання біометричних технологій для захисту інформації розглядалися у публікаціях як у відкритих, так і закритих літературних джерелах, зокрема, таких учених: Заха-

© Гребенюк А.М., 2019
ORCID iD: https://orcid.org/0000-0002-6529-683X
k_inf@dduvs.in.ua

© Краснобрижий І.В., 2019
ORCID iD: https://orcid.org/0000-0001-9943-4666
k_inf@dduvs.in.ua

© Мирошниченко В. О., 2019
ORCID iD: https://orcid.org/0000-0002-7508-737X
k_inf@dduvs.in.ua

ров В.П., Зачек О.І., Рудешко В.І., Барсуков В.С., Козирєв С.П., Корченко А.О., Мацьків Н.С., Гречишкіна О.М., Кухарєв Г. А., Дубчак О.В., Підгайна К.І., Брюхомицький Ю.А., Казарин М.Н., Іванов А.І., Урсуленко І.В., Полєнніков М.О., Пономаренко Л. В. та ін. [1-3]. Важливість наукового здобутку та внеску в теорію і практику інформаційної безпеки згаданих учених важко переоцінити.

Мета даної статті полягає у знаходженні найбільш перспективних напрямків розвитку біометричних технологій і ефективних існуючих біометричних систем, виходячи з їх ефективності, цінової складової, складності налагодження та обслуговування цих біометричних систем.

Виклад основного матеріалу. У нашій країні, як і за кордоном, системи контролю і управління доступом (СКУД) включають у себе різні технічні засоби: пристрої контактної і безконтактної ідентифікації, системи відеоспостереження та відеоаналізу, виконавчі пристрої (шлагбауми, турнікети та ін.), мережеве та серверне обладнання, спеціалізоване й інтеграційне програмне забезпечення, персоніфіковані Proximity-карти (і деякі інші рішення, засновані на технології RFID), які можуть працювати як самостійно, так і в поєднанні з додатковими методами, наприклад, з персональними ідентифікаційними номерами (ПІН-кодами). Ця технологія добре відпрацьована, вона має цілу низку переваг: порівняно невисоку вартість, наявність на ринку великого вибору обладнання, програмного забезпечення та підрядників із впровадження та обслуговування. Разом з тим технологія RFID не позбавлена недоліків, перш за все пов'язаних з необхідністю носити із собою ідентифікаційну картку, яку можна забути, втратити, передати іншій людині (з умислом чи без) або скопіювати. Тому в даний час актуальним є пошук нових підходів, які при невисокій вартості і максимальному використанні вже створеної інфраструктури допомагали б уникнути зазначених вище недоліків, кардинально підвищити загальну надійність системи, впроваджувати різні додаткові функції і сервіси, зробити СКУД зручнішим як для служби безпеки, так і для користувачів.

Один з найбільш перспективних шляхів вирішення вищезазначених проблем пов'язаний із застосуванням біометрії. Як відомо, на ринку пропонуються різні біометричні системи ідентифікації для СКУД. Це і сканери відбитків пальців або райдужної оболонки ока, і зчитування венозного малюнка на долонях, і навіть ідентифікація за голосом. Однак, на думку багатьох експертів, найкращі перспективи стати галузевим стандартом у СКУД має технологія біометричної ідентифікації за обличчям. Так, за оцінками дослідників Markets and Markets ринок розпізнавання осіб зростає в середньому на 15,3 % на рік і збільшиться з 3,4 млрд. дол. у 2016 році до 6,8 млрд. дол. у 2021 році. Одним з головних чинників його зростання є саме біометричні системи ідентифікації і контролю доступу. За прогнозами, ці технології будуть затребувані як державними органами, так і бізнес-спільнотою.

Сучасні реалізації технологій розпізнавання осіб (у тому числі хмарні рішення, «розпізнавання як сервіс») роблять їх доступними і рентабельними навіть для невеликих торгових точок, не кажучи вже про великі територіально-розподілені підприємства. Адже, і це, мабуть, найголовніше, кращі алгоритми розпізнавання осіб, засновані на нейронних мережах, досягли практично 100 % точності роботи, наприклад, алгоритми розпізнавання NIST і Megaface, допускають помилкове спрацьовування (пропускають «чужого») не більше ніж в одному випадку на один мільйон. Це дає можливість використовувати біометрію за обличчям в якості основної, і в багатьох випадках єдиної, технології аутентифікації у СКУД.

Біометричні системи мають ряд переваг перед традиційними ID- картами: вони забезпечують високу достовірність розпізнавання, їх неможливо обдурити, скопіювати або вкрасти ідентифікатор, їх легко інтегрувати з існуючим охоронним обладнанням. Вони працюють дистанційно і дуже швидко. Усі події фіксуються і зберігаються в архіві.

Важливою перевагою застосування технології ідентифікації за обличчям є можливість максимально задіяти вже існуючу інфраструктуру. Багато стандартних пристроїв СКУД вже містять вбудовану камеру. Тому при виборі біометричної СКУД потрібно звернути увагу на можливість використання різних типів камер. В ідеалі, система розпізнавання осіб повинна працювати з IP-, web-камерами, із вбудованими камерами мобільних пристроїв і зі спеціалізованими камерами розпізнавання осіб. Алгоритм розпізнавання повинен вміти справлятися із зображеннями, які отримуються навіть з найпростіших камер, які, як правило, і вбудовуються у пристрої контролю доступу. Якість «картинки», яку вони видають, має бути достатньою для побудови біометрично-

го шаблону і подальшої його перевірки у базі даних. У цьому випадку, все, що потрібно зробити – це встановити на сервері відповідне програмне забезпечення – і біометрична СКУД готова до роботи.

Сучасні алгоритми розпізнавання працюють на різних обчислювальних платформах. Там, де необхідна велика продуктивність, наприклад, на складних територіально-розподілених об'єктах, таких як аеропорти, транспортно-пересадочні вузли і т. ін., використовуються графічні процесори (GPU). Сучасна відеокарта класу NVIDIA Tesla дозволяє будувати більше 250 біометричних шаблонів на секунду (побудова шаблонів є найбільш ресурсномісткою операцією в біометричній ідентифікації). Таким чином, застосування GPU дозволяє обійтися однією відеокартою там, де потрібна була б ціла серверна стойка.

Для невеликих підприємств увесь механізм ідентифікації може бути реалізований у хмарі (наприклад, система біометрії і відеоспостереження FaceMatica). Вбудовані камери передають у хмару зображення, а FaceMatica повертає результат ідентифікації. Використовувати цей сервіс можна через просте оформлення розсилання, не витрачаючи кошти на придбання програмного забезпечення та «заліза».

Цікаві результати можна отримати за допомогою вбудованих систем розпізнавання осіб. Наприклад, якщо в RFID чіп або в локальну базу даних пристрою розпізнавання записаний біометричний шаблон особи, то можна виконувати ідентифікацію та аутентифікацію в режимі офлайн, не обмінюючись даними і зображеннями із сервером. Таке рішення вже реалізовано на платформі NVIDIA Jetson і являє собою невеликий пристрій розміром з кредитну карту, яка може не тільки детектувати і розпізнати обличчя, але і визначити стать і вік людини, провести перевірку «живості» і взяти на себе управління виконавчими пристроями.

Тут доречно згадати одне з питань, яке найбільш часто виникає у зв'язку з біометричною ідентифікацією за обличчям: чи можна обдурити систему, пред'явивши їй фотографію або відеозапис? Для того щоб цього не сталося, система розпізнавання особи повинна включати механізм перевірки, так званий livenesscheck, який гарантує, що перед камерою знаходиться дійсно жива людина [4]. Тонкість полягає в механізмі реалізації цієї перевірки: більшість рішень вимагають від користувача виконання певних дій (наприклад, кивнути головою або повернути її вліво або вправо). Це не дуже зручно для користувача, тому доцільною є така система, яка виконує перевірку автоматично, не вимагаючи нічого від людини. Таку перевірку можна реалізувати за допомогою аналізу розподілу світла і тіней на обличчі (з урахуванням умов освітлення) – плоске зображення пройти цей тест не зможе.

Розгорнута в організації або у хмарі біометрична система може використовуватися не тільки в системах контролю доступу, але й для вирішення багатьох інших завдань. Наприклад, для ведення повного і достовірного обліку робочого часу персоналу, забезпечення превентивної безпеки об'єкта в режимі некооперативного дистанційного розпізнавання осіб, для контролю внутрішніх зон і виявлення присутності в них осіб без відповідних повноважень, аналізу потоків відвідувачів і збору різного роду статистики, запобігання проходу на об'єкт за підробленими документами.

Впровадження цієї технології затребуване в місцях масового перебування людей – в метро, аеропортах, вокзалах, транспортно-пересадочних вузлах, стадіонах, видовищних заходах і т.ін. Тобто там, де необхідно в реальному часі відстежувати пасажирів і персонал, що входить у термінали, обмежувати несанкціонований доступ у зони контролю і дистанційно виявляти в натовпі «небажаних» відвідувачів. Система автоматично, в режимі реального часу, порівнює зображення осіб з камери з однією або декількома базами даних. Технологічно – це найскладніше завдання, оскільки неможливо змусити кожну людину подивитися в камеру. Для таких систем краще використовувати спеціалізовані камери розпізнавання із вбудованим детектором, що дозволяє передавати для обробки не весь відеопотік, а тільки зображення осіб. Це знижує витрати і навантаження на мережу (що критично важливо, якщо мова йде про десятки одночасно працюючих камер), а самі зображення передаються з максимальною роздільною здатністю. Крім того, в порівнянні зі звичайними камерами відеоспостереження, вони краще працюють зі складним освітленням і ракурсом, здатні автоматично покращувати якість зображення.

Зараз є актуальною інтеграція СКУД на базі розпізнавання осіб з платіжно-пропускними терміналами, наприклад, на стадіонах. Вона дозволяє фіксувати на камеру всі події, починаючи з покупки квитка, при цьому особа покупця «прив'язується» до квитка в момент покупки, інша людина не зможе пройти по ньому на матч. Таким чином, виконуються вимоги верифікації (підтвердження особи) уболівальників, ведеться боротьба з квитковими спекулянтами. Якщо людина внесена до списків осіб, яким дос-

туп на стадіон заборонено, система її не пропустить, навіть якщо у неї є квиток.

Висновок. Підсумовуючи викладене, можна зробити висновок, що нові рішення для систем контролю і управління доступом на базі біометричних технологій легко інтегруються в існуючу інфраструктуру, мають широкий функціонал, об'єднують апаратні засоби в єдину систему безпеки об'єкта. Біометрична ідентифікація осіб, безперечно, завоює в перспективі істотну частку ринку засобів ідентифікації, так як її застосування набагато зручніше і безпечніше, ніж використання традиційних карткових систем, а багато виробників СКУД вже починають вбудовувати у свої продукти розпізнавання осіб в якості однієї з базових функцій.

Бібліографічні посилання

1. Захаров В.П., Рудешко В.І. Використання біометричних технологій правоохоронними органами у XXI столітті: науково-практичний посібник. Львів: ЛьвДУВС, 2009. 440 с.

2. Пономаренко Л.В. Система захисту від несанкціонованого доступу на основі голосової автентифікації: дис. … канд. юрид. наук: 05.13.21. URL: http://www.lib.ua-ru.net/diss/cont/355488.html**.**

3. Зачек О.І. Можливості застосування біометричного методу ідентифікації за геометрією обличчя в системах відеоспостереження правоохоронних органів. *Науковий вісник Львівського державного університету внутрішніх справ: зб. Наук. праць.* 2014. № 1. С. 34 –351.

4. URL: http://www.biometric-solutions.com/liveness-check.html.

Надійшла до редакції 20.06.2019

References

1. Zakharov V.P., Rudeshko V.I. (2009) Vykorystannya biometrychnykh tekhnolohiy pravookhoronnymy orhanamy u XXI stolitti [The Use of Biometric Technologies by Law Enforcement Agencies in the 21st Century]: naukovo-praktychnyy posibnyk. L′viv: L′vDUVS [in Ukr.].

2. Ponomarenko L.V. Systema zakhystu vid nesanktsionovanoho dostupu na osnovi holosovoyi avtentyfikatsiyi [The system of protection against unauthorized access based on voice authentication]: dys. … kand. yuryd. nauk: 05.13.21. URL: http://www.lib.ua-ru.net/diss/cont/355488.html [in Ukr.].

3. Zachek O.I. (2014) Mozhlyvosti zastosuvannya biometrychnoho metodu identyfikatsiyi za heometriyeyu oblychchya v systemakh videosposterezhennya pravookhoronnykh orhaniv [Possibilities of application of biometric method of identification by face geometry in video surveillance systems of law enforcement agencies]. *Naukovyy visnyk L'vivs'koho derzhavnoho universytetu vnutrishnikh sprav*: zb. Nauk. prats′, 1, 34-351 [in Ukr.].

4. URL: http://www.biometric-solutions.com/liveness-check.html [in Engl.].

SUMMARY

Myroshnychenko V.O., Krasnobryzhyy I.V., Hrebenyuk A.M. The effectiveness of biometric technologies and features of their use in access control systems. Identification of a person is needed not only to search for antisocial elements, but also to optimize and simplify human life functions. The problem of identifying a person, especially in automatic and online mode, constantly requires finding the most effective software and hardware systems to solve this problem and finding the criteria by which the person will be identified. There are now many criteria by which a particular person can be identified, but identification by some criteria gives unacceptable errors. Therefore, the identification of a person by his/her biometric features must be performed in a comprehensive manner, or on the grounds that will give us acceptable results.

The article discusses the main directions of development of biometric technologies, in particular, methods of identification of a person by fingerprints, face geometry and iris. Attempts are being made to find the most effective biometric systems that actually exist in different countries of the world and are used in practice by various institutions and organizations, including law enforcement agencies. A comparison of these techniques based on FAR and FRR, according to which the most reliable is recognized by the iris of the eye. Other directions in recognition and identification systems are recognized as less reliable and it is preferable to use them in combination, for example, the use of recognition systems based on palm scans, papillary patterns and voice recognition systems; facial recognition systems and papillary line recognition systems; recognition systems for human gait and recognition systems for the face. It was concluded that recognition systems for human DNA are in the status of research and improvement (lack of efficiency in DNA analysis). It was determined that at a considerable distance identification is possible only by face geometry. The international experience of using such identification in video surveillance systems is considered. The features of the use of each biometric system are also considered on the basis of external factors, such as the number of simultaneously identified objects, the state of the external environment, and the capacity of information and telecommunications equipment.

New solutions for access control and management systems based on biometric technologies are easily integrated into existing infrastructure, have broad functionality, integrate hardware into a single facility security system.

Keywords*: access control system, verification, PIN code, Proximity-cards, RFID, ID-cards, identification, biometrics, IP-cameras, webcams, GPUs, video stream.*