УДК 343.982.323

Г.С. Веретун, *завідувач сектору Харківського науково-дослідного експертно-криміналістичного центру МВС України*
Д.В. Чернонос, *головний судовий експерт Харківського науково-дослідного експертно-криміналістичного центру МВС України*

ДАКТИЛОСКОПІЧНА ВЕРИФІКАЦІЯ В СИСТЕМАХ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ: ПРОБЛЕМНІ ПИТАННЯ

Розглянуто питання надійності ідентифікації особи в системах контролю управління доступом, запобігання можливості копіювання зразків відбитків пальців рук і використання їх іншими особами для отримання несанкціонованого доступу, окреслено технічні проблеми реєстрації зразків відбитків пальців рук для подальшої їх ідентифікації.

Ключові слова: ідентифікація особи, верифікація особи, системи контролю та управління доступом.

Рассмотрены вопросы надежности идентификации личности в системах контроля управления доступом, предупреждения возможности копирования образцов отпечатков пальцев рук и использования их другими лицами для получения несанкционированного доступа, определены технические проблемы регистрации образцов отпечатков пальцев рук для дальнейшей их идентификации.

This work contains the question about reliability of verification of the personality in access control systems, about possibility of sample copy fingerprints and using it by others for unsanctioned access, about technical problems of registration of fingerprints for their further identification.

Нині в Україні дедалі більшої актуальності набуває проблема біометричної ідентифікації людини, яка ґрунтується на аналізі індивідуальних характеристик особистості.

Біометричні технології, насамперед дактилоскопічні, застосовують у криміналістиці починаючи з XIX століття, а з кінця минулого століття з розвитком технічного прогресу з'явилася можливість формалізувати алгоритми розпізнавання людини за її зовнішнім виглядом або особливостями поведінки, застосовуючи для цього автоматизовані системи.

Сьогодні біометричні технології переживають період бурхливого розвитку в усьому світі. Багато в чому цей розвиток пов'язаний з рішеннями урядів провідних держав застосовувати їх під час виготовлення паспортно-візових документів, що спонукало спрямувати в цю сферу великі фінансові та матеріальні ресурси. Наявний великий інтерес суспільства до застосування цих технологій і в інших сферах.

Суспільні відносини, пов'язані зі збиранням, накопиченням, захистом, зберіганням, обліком, використанням і поширенням інформації Єдиного державного демографічного реєстру, а також оформленням, видачею, обміном, пересиланням, вилученням, поверненням державі, визнанням недійсними та знищенням передбачених Законом України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» документів регулюються Конституцією України, міжнародними договорами України, зазначеним Законом, а також прийнятими на їх виконання нормативно-правовими актами у сферах, де використовують відповідні документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи.

Згідно із зазначеним Законом:

– ідентифікація особи — це встановлення особи шляхом порівняння наданих даних (параметрів), у тому числі біометричних, з наявною інформацією про особу в реєстрах, картотеках, базах даних тощо;

– верифікація — порівняння даних (параметрів), у тому числі біометричних, для встановлення тотожності особи документам або інформації з Реєстру для підтвердження їх ідентичності;

– біометричні дані — сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та суттєво відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри — відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук);

– біометричні параметри — вимірювальні фізичні характеристики або особистісні поведінкові риси, що використовуються для ідентифікації (впізнання) особи або верифікації наданої ідентифікаційної інформації про особу [1].

Дослідженню питань щодо надійності ідентифікації особи в системах контролю управління доступом до ідентифікаційної інформації приділили увагу у своїх працях А. Вакуленко, А. Юхин, Н. Мазниченко, В. Ворона, В. Тихонов, О. Гинце та інші. Проте питання організації та експлуатації систем контролю і управління доступом до ідентифікаційної інформації, які постійно вдосконалюються з розвитком науково-технічного прогресу, залишаються доволі актуальними та потребують додаткового дослідження, що і становить мету цієї статті.

Нині питання ідентифікації особи є доволі актуальним для вирішення завдань безпеки транспортних, державних і міждержавних систем паспортних, візових, митних, міграційних служб, під час контролю пропусків і перевірки документів. Важливе значення також має питання ідентифікації осіб у місцях їх масового скупчення. Застосування для цього звичайних методів контролю сьогодні явно недостатньо, лише за допомогою біометричних технологій можна вирішити сучасні завдання ідентифікації особи [2].

Популярність біометричних систем контролю та управління доступом зумовлена об'єктивною потребою організації сучасної грамотно побудованої системи безпеки. При цьому завдяки інтенсивному розвитку мультимедійних, цифрових технологій (і, як наслідок, їх здешевленню) у практику постійно впроваджуються нові підходи до ідентифікації особи [3].

Сьогодні структура біометричних ідентифікаторів у різних системах контролю та управління доступом на світовому ринку за способом ідентифікації ідентифікованих об'єктів виглядає так [4]:

– сканування відбитка пальця руки — 34 %;
– сканування райдужної оболонки ока — 34 %;
– геометрія руки — 25 %;
– розпізнання обличчя — 15 %;
– верифікація голосу — 11 %;
– верифікація підпису — 3 %.

Трапляються також комбіновані біометричні ідентифікації та порівняно нові біометричні об'єкти (наприклад, клавіатурний почерк, розпізнавання людини за розташуванням вен в організмі тощо).

Сканування відбитків пальців рук набуло значного поширення завдяки унікальності папілярних узорів пальців. Сканери, які використовують відбитки пальців рук, можуть виконувати функції електронного замка. Їх встановлюють на вході у приміщення, до якого дозволено доступ лише чітко визначеному колу осіб. Спеціальними сканерами сьогодні оснащено деякі моделі сейфів. Тривають дискусії про запровадження цієї технології у банківському секторі з метою запобігання діям шахраїв, зокрема шляхом внесення інформації про відбитки пальців рук власника у спеціальний чип на кредитній картці.

Дуже поширеними також стали сканери, що здійснюють контроль за доступом до комп'ютерів, які підключають, зокрема, через USB-інтерфейс. У багатьох ноутбуках такі сканери вбудовано безпосередньо у лицьову панель. Існують також маніпулятори та клавіатури із вбудованими сканерами відбитків пальців рук.

Досліджуючи питання застосування систем контролю та управління доступом, заснованих на скануванні відбитків пальців рук, слід нагадати, що між дактилоскопіюванням та скануванням є суттєва різниця: під час сканування відбитків пальців рук зберігається не повне зображення папілярного узору, як при дактилоскопіюванні, а лише інформація про окремі характерні точки папілярного узору. Тож відновити повний образ відбитка пальця руки за збереженою інформацією і, відповідно, використати його неможливо.

У криміналістиці дактилоскопію використовують для ідентифікації особи за відбитками пальців рук. А коли йдеться про застосування цифрових сканерів для створення систем безпеки, то мають на увазі верифікацію особи. Під час ідентифікації особи за відбитками пальців рук встановлюють, кому саме вони належать. Для цього відбиток пальця ідентифікованої особи порівнюють з відбитками з бази даних стосовно їх збігу. Тобто ідентифікація дає змогу відповісти на запитання, ким є людина, яку ідентифікують (хто вона). Верифікація означає порівняння відсканованого відбитка з одним або кількома шаблонними відбитками пальців рук з метою встановлення того, чи є певна особа саме тією, за кого себе видає.

У дактилоскопічних зчитувачах для систем контролю та управління доступом використовують такі сканери для папілярних узорів пальців рук [5]:

– оптичні контактні (Frustrated Total Internal Reflection), засновані на одній із найстаріших та найпоширеніших технологій. При цьому отримання образу відтиску пальця руки (темплейта) пов'язане з певними труднощами і має певні недоліки, а саме: якість образу залежить від навколишнього освітлення, можливі викривлення на межах образу, сканер можна «обдурити» за допомогою муляжів або фотографій;

– ємнісні або кремнієві (Capa-citive Scanners, Capacitive Sweep Scanners), отримання темплейта в яких засноване на ефекті зміни ємності pn-переходу напівпровід-

никового пристрою під час дотику виступів (гребенів) папілярного узору пальця руки до кремнієвої матриці (виступи тиснуть на матрицю і формується зображення);

– сканери, які генерують електромагнітне поле. У таких пристроях датчик випромінює слабкий електромагнітний сигнал, який проходить через виступи і борозенки відтиску пальця руки, і відповідно до зміни цього сигналу формується темплейт. Цей метод сканування дозволяє проглядати папілярний узор пальця руки під шаром омертвілих клітин.

Основними характеристиками будь-якого біометричного зчитувача є коефіцієнти надійності або вірогідності помилок першого та другого роду. Помилка першого роду (FRR — False Rejection Rate) — це вірогідність хибної відмови у доступі. Помилка другого роду (FAR — False Acceptance Rate) — це вірогідність хибного доступу, коли система помилково впізнає чужого як свого. Крім того, біометричні системи іноді характеризуються коефіцієнтом рівної вірогідності помилок першого та другого роду (EER — Equal Error Rates), що є точкою збігу вірогідностей FRR та FAR. Зрозуміло, що надійна система повинна мати якнайнижчий рівень EER. Під час вибору біометричних систем слід керуватися значенням EER (FRR та FAR) та можливістю взаємного регулювання рівнів FAR та FRR, а також конкретними завданнями, які має вирішувати система контролю та управління доступом, часом ідентифікації особи зчитувачем, сумісністю зчитувачів та контролерів інформації.

Таким чином, біометричний процес гарантує виявлення системою істинності особи, яку перевіряють, з певним рівнем надійності, тобто він не гарантує, що ідентифікований об'єкт є точною копією наявних зразків, а свідчить про те, що вірогідність відповідності особи тій, за яку вона себе видає, становить X % [4, с. 60]. Хоча виробники систем контролю та управління доступом, зокрема у дактилоскопічному сегменті, заявляють про невеликі похибки системи (коефіцієнт першого роду становить не більше ніж 0,1 %, другого роду — не більше ніж 0,0001 %), вона не може повною мірою забезпечити ідентифікацію людини [3, с. 131; 4, с. 63].

Важливим питанням з погляду надійності дактилоскопічної ідентифікації за відбитками пальців рук у системах управління та контролю доступу є питання про можливість їх копіювання і використання іншими особами для отримання несанкціонованого доступу.

Як одну із можливостей обману термінала спеціалісти називають використання штучної кисті руки з відповідними відбитками пальців (або «вилучення оригіналу» у законного володільця). Деякі автори у свої працях наводять способи боротьби з такими проявами фальсифікації шляхом поміщення до термінального обладнання інфрачервоного детектора, який здатний фіксувати теплове випромінювання від руки (пальця руки), та фотоплетізмографа, який дозволяє оцінити стан судинної системи людини [4, с. 64].

Так, у 2002 році аспірант національного університету Йокогами Цутомо Мацумото опублікував результати своїх експериментів, під час яких він з матеріалів, придбаних у звичайному магазині, спромігся сфальсифікувати узор пальця руки та обманути дактилоскопічні сканери різних систем доступу. З відома власника фальсифікованого папілярного узору пальця руки він виготовив желатиновий (можна гумовий) ковпачок, який надягнув на палець фальсифікатора (зрозуміло, що за бажанням можна негласно використати відбиток пальця руки, отриманий за допомогою традиційної криміналістичної техніки (з посуду чи з гладкої поверхні меблів), а

потім використати його у протиправних цілях). Муляж, який виготовив і використав Ц. Мацумото, настільки непомітний, що міг застосовуватися у присутності співробітників охорони, які нічого не підозрювали. Перевагою муляжу, який надягався на палець, було й те, що він дозволяв також обманути прилади, забезпечені додатковими засобами захисту від доступу, наприклад, датчиками тепла. Ц. Мацумото стверджує, що йому вдалося ввести в оману дев'ять з одинадцяти різних систем зчитування дактилоскопічної інформації [6]. Отже, питанням безпеки від технічних обманів системи слід приділяти важливе значення.

На окрему увагу заслуговують і питання верифікації осіб системами контролю та управління доступом з великими обсягами вміщених до них баз даних, роботі яких пред'являють доволі високі вимоги щодо мінімізації помилок. У цьому випадку реєстрація відбитків пальців рук має бути навіть якіснішою, ніж в автоматизованих дактилоскопічних інформаційних системах (далі — АДІС), насамперед за рахунок вищого рівня автоматизації прийняття системою рішень. Якщо в АДІС остаточне рішення завжди приймає експерт, який аналізує результати пошуків і здатний скорегувати помилки системи, зазвичай спричинені низькою якістю первинних зображень (зображення з дактилокарт, виконаних типографською фарбою та іншими барвниками, відбитки рук з місця події), то для більшості дактилоскопічних систем контролю втручання оператора для коригування помилок, зумовлених низькою якістю реєстрації дактилоскопічної ознаки, зводить нанівець впровадження подібних систем [7].

Як відомо, зображення прокатного відбитка пальця руки є розгорткою узору папілярних ліній пальця руки у площині. Геометрична форма нігтьової фаланги пальця руки не збігається з ідеальною поверхнею обертання у формі циліндру, та й під час прокатки відбувається ковзання пальця по чутливій панелі з утворенням змазування зображення (чим повніше прокатують палець, тим більше вірогідність появи змазування).

Реєстрація дактилокарт у криміналістичних АДІС передбачає отримання відбитків усіх десяти нігтьових фаланг пальців обох рук, контрольних відтисків чотирьох та великого пальця кожної руки, відтисків долонь. Оскільки в АДІС пошуки здійснюють не лише за відбитками пальців, а й за слідами рук, вилученими з місць вчинення злочинів, а також за фрагментами папілярного узору, обраний дактилоскопічний сканер обов'язково має забезпечувати реєстрацію відбитків пальців рук «від нігтя до нігтя».

Дактилоскопічні системи контролю та управління доступом не завжди потребують реєстрації повного набору дактилоскопічних зображень (звичайно, йдеться лише про сканування папілярних узорів нігтьових фаланг пальців рук — від 1 до 10). Але для таких систем під час первинної реєстрації оптимальним є застосування приладу, здатного виконувати повну прокатку пальця руки. При цьому сканувати потрібно не відтиск (зображення папілярного узору, отримане завдяки плоскому торканню пальця до призми сканера), а повне зображення відбитка, отримане шляхом прокатки пальця по призмі приладу «від нігтя до нігтя». Це пояснюється тим, що максимально повна первинна реєстрація у базі даних дозволить під час подальших звернень до системи уникати помилок ідентифікації, зумовлених людським чинником (зокрема, через неправильне прикладання пальця до призми приладу (недостатній дотик, перекіс чи поворот пальця) або часткове пошкодження

шкіряного покрову пальця).

Підсумовуючи, слід зазначити, що неможливо скласти вичерпний перелік функцій, які повинна мати «ідеальна» система електронного дактилоскопіювання. Проте якісно розроблений програмний продукт зазвичай забезпечує гнучкість системи, що дозволяє адаптувати її до вимог певного замовника та виконання певного завдання.

Список використаної літератури

1. *Закон* України «Про єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» : станом на 6 груд. 2016 р. [Електронний ресурс] / Верховна Рада України. — Офіц. вид. — Режим доступу : http://zakon2.rada.gov.ua/laws/show/5492-17.

2. *Вакуленко А.* Биометрические методы идентификации личности: обыкновенный выбор / А. Вакуленко, А. Юхин // Мировой опыт применения биометрических решений в составе комплексных систем безопасности : сбор. науч. тр. 1 межд. науч.-прак. конф. — К. : Информация — Украина, 2006. — С. 79—82.

3. *Мазниченко Н.И.* Области применения и принципы построения биометрических систем идентификации личности / Н.И. Мазниченко // Вестник Национального технического университета «Харьковский политехнический інститут». Серия: Информатика и моделирование. — 2007. — № 19. — С. 132.

4. *Ворона В.А.* Системы контроля и управления доступом / В.А. Ворона, В.А. Тихонов. — М. : Горячая линия — Телеком, 2010 — 247с.

5. *Гинце А.А.* Дактилоскопические считыватели в СКУД [Электронный ресурс] / А.А. Гинце // Системы безопасности — 2010. — № 1 — С. 80—83. — Режим доступа : http://www.secuteck.ru/articles2/sys_ogr_dost/daktiloskopicheskie-schityvateli-v-skud/.

6. *Берд К.* Биометрия как она есть [Электронный ресурс] / К. Берд // Компьютерра. — 2002. — № 20 (45). — Режим доступа : http://www.kinet.ru/cterra/445/18034. html.

7. *Якушев Б.* Выбор дактилоскопического сканера для регистрации отпечатков в дактилоскопических идентификационных системах [Электронный ресурс] / Б. Якушев // Алгоритм безопасности. — 2008. — № 4. — С. 54—58. — Режим доступа : http://www.algoritm.org/arch/arch.php?id=35&a=620.