УДК 65.012.8:343.982.34

В. П. Захаров,
О. І. Зачек

ТЕНДЕНЦІЇ ВИКОРИСТАННЯ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ, ЯКІ НЕ ВХОДЯТЬ ДО «ТРЬОХ ВЕЛИКИХ БІОМЕТРИК»

Розглянуто сучасні тенденції використання в системах захисту інформації біометричних технологій, які не входять до «трьох великих біометрик», а саме: ідентифікації за ДНК, за зображенням кисті руки, за малюнком вен долоні або пальця руки, за термограмою обличчя, за формами вушних раковин, за запахом, за голосом, за підписом, за клавіатурним почерком, шляхом аналізу біоелектричної активності мозку та надано пропозиції щодо їх використання в правоохоронних органах України.

Ключові слова: *біометрія, методи біометричної автентифікації, ідентифікація за ДНК, ідентифікація за зображенням кисті руки, ідентифікація за малюнком вен долоні або пальця руки, ідентифікація за термограмою обличчя, ідентифікація за формами вушних раковин, ідентифікація за запахом, ідентифікація за голосом, ідентифікація за підписом, ідентифікація за клавіатурним почерком, ідентифікація шляхом аналізу біоелектричної активності мозку, системи контролю та управління доступом.*

Постановка проблеми. Нині розробки в галузі захисту інформації є надзвичайно актуальними, оскільки злочинці намагаються заволодіти інформацією за допомогою сучасних високих технологій. Адже всі знають, що хто володіє інформацією, той володіє світом. А якщо злочинці заволодіють інформацією, яка використовується в діяльності правоохоронних органів, то вони зможуть значно ефективніше провадити свою протиправну діяльність.

Також актуальними є розробки в галузі систем управління доступом, які використовуються в комплексних системах захисту інформації, як важлива складова.

Найсучаснішим напрямом розробок у перелічених галузях є використання біометричних технологій. Біометричні технології мають низку переваг порівняно з традиційними методами ідентифікації осіб із метою надання їм права доступу до інформації. Є біометричні методики, які використовуються вже традиційно, а є такі, які досі вважаються екзотичними. Але не слід забувати, що нещодавно будь-які біометричні технології вважалися екзотикою.

До 11 вересня 2001 року біометричні системи доступу використовувалися в основному тільки для захисту військових секретів та найважливішої комерційної інформації [1]. Але після теракту в Нью-Йорку ситуація різко змінилася. Наприклад, серед громадян США всього 10% підтримувало ідею біометричної паспортизації до 11 вересня 2001 року і вже понад 75% – після теракту, коли відстеження потенційно небезпечних особистостей стало найважливішим завданням [2]. Нині попит на системи, які використовують біометричні технології, значно зріс, збільшилась кількість галузей їх використання та вдосконалилися технології. Відбулося зниження вартості елементів таких систем, що позитивно впливає на подальший розвиток біометричних технологій. Наприклад, нещодавно вартість дактилоскопічних систем становила 2000–5000 доларів США, а після створення мініатюрного мікроелектронного дактилосканера вартість біометричного захисту комп'ютерів знижена до 50–100 доларів США [2]. Тому в майбутньому варто очікувати запровадження в практичну діяльність новітніх біометричних технологій, навіть таких, які нині є незвичними та перебувають у зародковому стані.

Нині потрібно проводити розробки в галузі використання таких методик. Необхідно визначити, які з цих технологій є найпридатнішими для застосування в правоохоронних органах і з погляду надійності, і економічної доступності.

Стан дослідження. Проблемам використання біометричних технологій для захисту інформації присвячено достатньо публікацій і у відкритих, і закритих літературних джерелах, зокрема таких учених: В. П. Захаров, В. І. Рудешко, В. С. Барсуков, Г. Двоєносова, М. Двоєносова, С. П. Козирєв, А. О. Корченко, Н. С. Мацьків, О. М. Гречишкіна, Г. А. Кухарєв, О. В. Дубчак, К. І. Підгайна, Ю. А. Брюхомицький, М. Н. Казарин, А. І. Іванов, І. В. Урсуленко, М. О. Полєнніков, М. Попов, Н. Вороніна, А. Прохоров, Ю. Семко, Л. В. Пономаренко.

Важливість наукового здобутку та внеску в теорію та практику інформаційної безпеки згаданих учених складно переоцінити. Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення й експлуатування біометричних систем захисту інформації є певні недоліки, які знижують ефективність їхнього функціонування.

Біометричні технології захисту інформації використовують різні параметри особи для її автентифікації. **Метою** цієї статті є розгляд сучасних тенденцій використання біометричних технологій, зокрема в системах захисту інформації правоохоронних органів України.

Виклад основних положень. Біометрію використовують для визначення права доступу осіб до інформації на основі їх ідентифікації за допомогою індивідуальних особливостей тіла.

З погляду поширеності біометричних методик виокремлюють «три великі біометрики»: ідентифікація за відбитками пальців, за геометрією обличчя та за райдужною оболонкою ока. Як вважають деякі автори, системи ідентифікації за відбитками пальців займають більшу частину ринку біометричних технологій, системи на основі технології розпізнавання за геометрією обличчя – 13–18%, а системи на основі ідентифікації за райдужною оболонкою ока – 6–9% [3]. І значно менше в системах захисту інформації використовуються такі методики, як ідентифікація за сітківкою ока, за ДНК, за зображенням кисті руки, за малюнком вен долоні або пальця руки, за термограмою обличчя, за формами вушних раковин, за запахом, за голосом, за підписом, за клавіатурним почерком та шляхом аналізу біоелектричної активності мозку.

Найнадійнішим із практично реалізованих методів вважається метод сканування сітківки ока. Тому він використовується в системах контролю доступу на особливо секретні об'єкти. Через низький рівень поширення таких систем незначною є вірогідність реалізації спроб зламу. Але недоліком є висока вартість систем із використанням цього методу.

Сполучення нуклеотидів у ланцюжок ДНК (дезоксирибозуклеїнова кислота) становить генетичний код будь-якої живої істоти [1]. Ідентифікація за ДНК здійснюється шляхом порівняння ДНК особи з ДНК контрольних зразків. Але нині ця методика використовується лише для ідентифікації особи в криміналістиці, а в системах захисту інформації вона поки що не застосовується внаслідок високої вартості та складності обладнання.

Ідентифікація за формою долоні або за геометрією кисті ґрунтується на побудові тривимірного зображення кисті руки. Для здійснення ідентифікації знімаються такі характеристики пальців чи долоні, як довжина, ширина, товщина та параметри поверхні шкіри. Загалом оцінюється понад 90 різних характеристик. Недоліком методу є зміни кисті руки впродовж життя, що спричиняє низьку надійність. Тому цей метод розглядається лише як доповнення до інших біометричних технологій [1]. Хоча є приклади його успішного використання в практичній діяльності. Одним із пристроїв, що використовує цю методику, є Handkey компанії Escape (США), який сканує внутрішню та бокову сторони долоні за допомогою вбудованої відеокамери із застосуванням алгоритмів стискання. Також є пристрій ID3D-R Handkey компанії

Recognition Systems (США) [2]. Декілька компаній, зокрема BioMet Partners, Palmetrics и BTG, розробляють пристрої, які можуть сканувати також інші параметри руки [4].

Розпізнавання за венами руки ґрунтується на використанні знімків зовнішньої та внутрішньої сторін руки. Оскільки гемоглобін крові поглинає інфрачервоне випромінювання, ступінь відбиття променів зменшується і вени стають видимими у вигляді чорних ліній. А малюнок вен у кожної людини є індивідуальним. Сканування можна здійснювати безконтактно. Ця технологія за надійністю прирівнюється до ідентифікації за райдужною оболонкою ока. Недоліком є вплив деяких хвороб, зокрема артриту. А перевагою є менш дороге обладнання за високої точності. Наприклад, обладнання є дешевшим, ніж для методів розпізнавання за геометрією обличчя чи за райдужною оболонкою. Розробками обладнання та програмного забезпечення займаються компанії Fujitsu, Veid Pte. Ltd., Hitachi VeinID [3].

Компанія «Hitachi» виготовляє систему «Finger Vein», яка використовує зображення малюнка вен будь-якого пальця особи, оскільки малюнок вен на пальці, як і на долоні, неможливо підробити. FRR цієї системи становить 0,01%, а FAR – 0,0001% [1].

Термографічна картина обличчя, отримана за допомогою інфрачервоної камери, залежить від густини кісток, жиру та кровоносних судин, і є суто індивідуальною ознакою. Точність цього методу є дуже високою та дає змогу розрізняти навіть близнюків. Цей метод не залежить від застосування косметики, макіяжу, пластичної хірургії та дозволяє провадити розпізнання негласно [5].

Оскільки форми вушних раковин є індивідуальними, то вони теж дають змогу ідентифікувати особу. Навіть недорога Web-камера дозволяє з високою надійністю здійснювати ідентифікацію [5]. Але відомостей про виробництво приладів для такої ідентифікації немає.

Давно відомою є здатність собак розпізнавати людей за запахом. Нині здійснюються розробки «електронного носа», який містить системи відбору проб запахів та їх підготовки, матриці сенсорів, які сприйматимуть запахи, та процесора для обробки сигналів матриці сенсорів. Але ці розробки недосконалі, тому їх практично ще не реалізовують [5].

Перелічені методи належать до статичних, що використовують фізіологічні параметри людини, які не змінюються в часі. Крім них, є динамічні методи, які ґрунтуються на індивідуальних поведінкових особливостях людини.

До них належать голосова ідентифікація, ідентифікація за підписом, за клавіатурним почерком, за біоелектричною активністю

мозку. Але ці технології не забезпечують високої точності та надійності ідентифікації.

Одним із методів, які дають змогу розпізнавати особу на відстані та негласно, є голосова ідентифікація. Перевагами є невисока ціна означеного методу, оскільки потрібні лише мікрофон та звукова карта, яка є тепер у кожному комп'ютері, та відсутність психологічного дискомфорту під час ідентифікації [6]. Під час ідентифікації за голосом аналізуються висота тону, модуляція, інтонація тощо. Але надійність та точність цього методу не є високими, оскільки голос може залежати від стану здоров'я та поведінкових чинників [7]. Одним із розробників технологій розпізнавання особи за голосом є російське товариство з обмеженою відповідальністю «Центр мовних технологій» [1].

Одним із найбільш звичних для нас методів ідентифікації особи є її підпис. Якщо підпис як графічне зображення можна підробити, то поведінку руки особи під час підпису скопіювати неможливо. Біометричний метод ідентифікації людини за підписом ґрунтується на аналізі швидкості руху руки, сили тиску та тривалості виконання етапів підпису. Людина імітує свій звичний підпис, а прилад знімає параметри руху та звіряє з наявними в базі даних. Але цей метод не можна використовувати в системах контролю доступу, він має перспективи в тих галузях, де підписуються важливі документи, наприклад, у банківській сфері [7]. В галузі розпізнавання підпису було видано сотні патентів фірмам «IBM», «NCR», «VISA», «Adapteck» [1].

Метод ідентифікації за клавіатурним почерком схожий на ідентифікацію за підписом, але тут використовується введення кодового слова на стандартній клавіатурі комп'ютера. Основною характеристикою є динаміка набору кодового слова [7]. Перевагою є використання звичайного комп'ютера. Такий метод нині не є поширеним, але розробки в цій галузі здійснюються. Наприклад, компанія «BioPassword Inc.» розробила програму перевірки особистості користувача комп'ютера за ритмічними характеристиками набору тексту [1].

Ідентифікація шляхом аналізу біоелектричної активності мозку ґрунтується на електроенцефалографії. За допомогою шапочки з електродами система здійснює моніторинг електричної активності мозку, передає дані на комп'ютер і формує цифровий портрет електричної активності мозку особи. Під час ідентифікації знята енцефалограма порівнюється з еталонною. Але низка фахівців вважає, що така ідентифікація не набуде практичного використання через свою непрактичність [1].

Найбільша ефективність захисту інформації досягається шляхом комбінації різних методів ідентифікації. Наприклад НПФ «Кристал» (Росія) виготовляє систему захисту інформації «Рубіж», де комбіновано

використовуються голосова ідентифікація, ідентифікація за динамікою підпису та за персональним кодом ключа «Touch memory» [2].

Висновки. Нині в системах захисту інформації правоохоронних органів України не використовуються перелічені методи ідентифікації особи. Розглянувши переваги та недоліки, а також існуючі практичні реалізації цих методів, можна констатувати, що для практичного використання в правоохоронних органах України сьогодні можна рекомендувати ідентифікацію за геометрією кисті, за венами руки та пальців і за голосом. Ці методи не потребують дорогого обладнання та програмного забезпечення, які, крім того, є у продажу. Також доцільною є розробка такого обладнання й програмного забезпечення в Україні, оскільки науковий та промисловий потенціал нашої держави це дозволяє.

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

2. Барсуков В. С. Біоключ – шлях до безпеки / В. С. Барсуков [Електронний ресурс]. – Режим доступу: http://kvartir-remont.com.ua/biokljuch-shljah-do-bezpeki.

3. Современные биометрические методы идентификации. [Електронний ресурс]. – Режим доступу: http://habrahabr.ru/post/

4. Попов М. Биометрические системы безопасности / М. Попов [Электронный ресурс]. – Режим доступа: http://www.bre.ru/security/12571.html.

5. Воронина Н. Биометрические пароли / Н. Воронина, А. Прохоров, Ю. Семко [Электронный ресурс]. – Режим доступа: http://www.compress.ru/article.aspx?id= 10058 &iid=419

6. Пономаренко Л. В. Система захисту від несанкціонованого доступу на основі голосової автентифікації: дисертація канд. наук: 05.13.21 – 2009. [Електронний ресурс]. – Режим доступу: http://www.lib.ua-ru.net/diss/cont/355488.html.

7. Шаров В. Биометрические методы компьютерной безопасности / В. Шаров [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles/detail.php?ID=6719

Захаров В. П., Зачек О. И. Тенденции использования в деятельности правоохранительных органов биометрических технологий, не входящих в «три большие биометрики»

Рассмотрено современные тенденции использования в системах защиты информации биометрических технологий, которые не входят в «три большие биометрики», а именно: идентификация по ДНК, по изображению кисти руки, по рисунку вен ладони или пальца руки, по термограмме лица, по форме ушных раковин, по запаху, по голосу, по подписи, по клавиатурному

почерку, путём анализа биоэлектрической активности мозга и даются предложения по их использованию в правоохранительных органах Украины.

Ключевые слова: *биометрия, методы биометрической аутентификации, идентификация по ДНК, идентификация по изображению кисти руки, идентификация по рисунку вен ладони или пальца руки, идентификация по термограмме лица, идентификация по форме ушных раковин, идентификация по запаху, идентификация по голосу, идентификация по подписи, идентификация по клавиатурному почерку, идентификация путём анализа биоэлектрической активности мозга, системы контроля и управления доступом.*

Zakharov V. P., Zachek A. I. Trends of Application of Biometric Technologies that are not Part of the «Three Major Biometrics» in Activity of Law Enforcement Bodies

The article deals with the modern trends of application of biometric technologies that are not part of the «three major biometrics» in the systems of information protection. Some biometric techniques are applied traditionally and some are still considered exotic. «Three major biometrics» are distinguished, in terms of prevalence of biometric techniques, namely, by fingerprint identification, geometry of the face and iris. Such techniques are applied in the information security systems to much lesser extent in addition to «three major biometrics». The identification is carried out by retina, DNA, the geometry of the hand, vein pattern palm or fingers, facial thermogram, forms of ears, smell, voice, signature, handwriting keyboard, analysis of the bioelectrical activity of the brain.

The introduction of the advanced biometric technology is a matter of the near future. It is necessary to determine which of these technologies are the most suitable for application in law enforcement bodies in terms of reliability and in terms of economic affordability. Having considered the advantages and disadvantages, and existing practical implementation of these technologies, we concluded that the identification carried out by the geometry of the hand, vein pattern palm or fingers, and by the voice can be recommend for practical application in law enforcement bodies of Ukraine.

The identification carried out by the geometry of the hand is based on the construction of three-dimensional image of the hand. The examples of the successful application of this method exist, inspite of very high reliability. The identification carried out by pattern of vein palm or fingers for reliability is comparable with identification by the iris, but requires less expensive equipment. Voice identification can recognize a person distantly and secretly. The advantages of this method is low cost and lack of psychological discomfort during authentication.

Key words: *biometrics, biometric methods of authentication, DNA identification, image of the hand identification, vein pattern palm or fingers identification, facial thermogram identification, ears forms identification, smell identification, voice identification, signature identification, handwriting keyboard identification, identification by analyzing the bioelectrical activity of the brain, control systems and access management.*

Стаття надійшла 2 березня 2015 р.