provision «About operative search activity», efficiency of application of that comes true not to a full degree.

Key words: *operative search activity, a crime is a process activity, protocol, results of hordes, legalization of materials.*

Стаття надійшла 24 лютого 2014 р.

УДК 340.64

Т. Я. Гнідець

БІОМЕТРІЯ: СИЛЬНІ ТА СЛАБКІ СТОРОНИ

Розглянуто поняття біометрії, її режими, класи, основні види біометричних систем, відомості про сильні сторони біометрії, її застосування у сфері безпеки суспільства та держави, обліку робочого часу, контролю за доступом та за впровадження паспортно-візових режимів. Наведено й деякі недоліки, виокремлені противниками цих систем. Описано процес упровадження біометричних систем у різні сфери життя суспільства та держави у провідних країнах світу.

Ключові слова: *біометрія, ідентифікація, верифікація, відбитки пальців, райдужна оболонка, ідентифікація обличчя, ідентифікація за голосом, охоронна система.*

Постановка проблеми. Віднедавна дедалі більше уваги привертає біометрія як одна з новітніх інформаційних технологій, що визначає розвиток засобів і систем ідентифікації і верифікації громадян, які з високою точністю можна використовувати в різних системах контролю і управління доступом для забезпечення безпеки у державній і приватній сферах.

Сьогодні громадяни України не повною мірою володіють інформацією щодо біометричних систем контролю та захисту. Причина цього – низький рівень дослідження та розвитку цієї галузі технологій, небажання впроваджувати біометричні пристрої серед представників підприємств, установ, організацій державної та приватної форми власності. Як наслідок – високий рівень злочинності та малоосвіченість громадян у цьому питанні.

Стан дослідження. Наукові досягнення в галузі біометрії належать таким ученим, як Ф. Гальтон, К. Пірсон, Р. Фішер, І. Романовський, А. А. Сапегін, Ю. А. Філіпченко, С. С. Четверіков та ін.

Мета статті – виклад основних понять щодо використання сучасних біометричних технологій, насамперед положень про можливості існуючих біометричних систем захисту і контролю, а також відомостей про біометричні банки даних, які ефективно працюють за кордоном.

Виклад основних положень. Уявіть собі будинок, де відчиняються двері, після того, як відеокамера ідентифікує ваше обличчя, доступ до комп'ютера стає можливим після сканування відбитку пальця, а ваш сейф відкриється тільки після сканування райдужної оболонки ока. Це все здається фантастикою фільму? Помиляєтесь, це незабаром може стати можливим. Всі ці засоби ідентифікації можуть бути встановлені у вашому будинку, офісі чи автомобілі. Біометричні технології (ідентифікація за відбитком пальця, обличчя, долоні, райдужної оболонки ока та голосу) застосовуються в провідних країнах світу, позаяк біометричний код є унікальним для кожної людини, він не може бути забутим, загубленим чи викраденим. Тому розглянемо всі сильні та слабкі сторони біометричних технологій.

Найперше визначимо, що таке біометрія, окреслимо її види та основні принципи.

Біометрія – це система розпізнавання людей за однією чи декількома фізичними, або поведінковими рисами. У сфері інформаційних технологій біометричні дані використовуються як форми управління ідентифікаторами доступу і контролю доступу [1]. Як самостійна дисципліна, біометрія виникла в кінці 19 століття в результаті робіт Ф. Гальтона, що зробив великий внесок у створення кореляційного і регресійного аналізу, та К. Пірсона – засновника найбільшої біометричної школи. Також значну роль у поширенні і вдосконаленні біометрії виконали Р. Фішер, І. Романовський, А. А. Сапегин, Ю. А. Філіпченко, С. С. Четверіков та ін. [2].

Біометричні дані можна розділити на два основні класи:

– фізіологічні (статичні) – стосуються форми тіла. Це розпізнавання особи за відбитками пальців рук, за ДНК, формою долоні руки, сітківкою ока, запахом/ароматом;

– поведінкові (динамічні) пов'язані з поведінкою людини. Наприклад, хода і голос. Для цього класу біометрії часом використовується термін «behaviometrics».

Біометрична система може працювати в двох режимах:

1) верифікації – порівняння біометричних шаблонів. Так перевіряється, чи людина та, за кого себе видає [1]. Іншими словами, верифікація задає питання: «Ви той, за кого себе видаєте»?

Відповідь на це питання будь-яка біометрична система надає в режимі верифікації, порівнюючи одного з одним. Користувач вводить своє ім'я, пароль або пін-код, пред'являє електронну картку або іншим способом оголошує системі, хто він. Її завдання в цьому випадку – перевірити правдивість отриманої інформації, тобто звірити відповідність вимірюваної біометричної характеристики записаному раніше шаблону заявленого індивідуума [3];

2) ідентифікації – порівняння одного з багатьма: після «захоплення» біометричних даних триває з'єднання з біометричної базою даних для визначення особистості. Ідентифікація особистості успішна, якщо біометричний зразок уже є в базі даних [1]. Іншими словами ідентифікація відповідає на питання: «Хто ви»?

Відповідаючи на нього, будь-яка біометрична система працює в режимі ідентифікації, порівнюючи одного з багатьма. У цьому випадку користувач «пред'являє біометрики» сканеру (сканер зображення обличчя, сканер райдужної оболонки ока, пред'являє відбиток пальця), і завдання алгоритму – прийняти рішення, чи належить користувач до відомих індивідуумів. Якщо так, то хто він? У цьому випадку вимірюється біометрична характеристика, порівнюється з базою раніше записаних шаблонів усіх «відомих» системі людей [3].

Ідентифікація в будь-якій біометричній системі охоплює чотири стадії:

1. Запис – фізичний або поведінковий зразок запам'ятовується системою.

2. Виділення – унікальна інформація виділяється з зразка і створюється біометричний зразок.

3. Порівняння – збережений зразок порівнюється з представленим.

4. Збіг/незбіг – система вирішує, збігаються зразки чи ні [4].

Основні види біометричних систем:

1. Відбитки пальців. У кожної людини відбитки пальців унікальні за малюнком, навіть у близнюків відбитки пальців різні. Це одна з найбільш популярних технологій, яка застосовується для забезпечення безпечного доступу до комп'ютера чи автомобіля. Завдяки цій системі користувачам більше не потрібно набирати паролі чи носити ключі, доступ забезпечується дотиком до сканера. Також під час застосування цієї технології зникне необхідність у «відкатуванні пальців» працівниками ОВС, потрібно буде тільки приставити пальці руки до сканера, і біометрична система відповість, чи відбитки пальців

рук були виявлені на місці події. В цієї технології найбільша кількість прихильників у світі, і саме тому вона найбільш вживана. Сильна сторона цього способу – в всесвітньому схваленні, зручності та надійності.

2. Ідентифікація обличчя. Ідентифікація особи за обличчям може бути здійснена різними способами, наприклад, фіксація обличчя в зоні видимості, використання звичайної відеокамери, або за допомогою теплового малюнка обличчя. Впізнання освітленого обличчя полягає в розпізнанні певних рис. Використовуючи велику кількість камер, система аналізує риси отриманого зображення, які не змінюються упродовж життя, незважаючи на поверхневі характеристики, такі як вираз обличчя чи стан волосся. Деякі системи розпізнання обличчя потребують стаціонарного положення для того, щоб отримати найбільш правдиве зображення, але поряд з цим є і системи, які працюють у режимі реального часу і розпізнають обличчя автоматично. Цей спосіб ідентифікації є одним із найкращих, оскільки найбільш схожий до того, як люди впізнають одне одного.

3. Ідентифікація за голосом використовує акустичні особливості розмови, які певною мірою є унікальними. Ці акустичні зразки відображають і анатомію (наприклад, розмір і форму горла, рота), і вироблені звички (манера розмови, гучність голосу). Перетворення цих зразків у голосові моделі надало цьому способу ідентифікації назву «поведінкова біометрія». Поведінкова біометрія розбиває кожне слово на декілька сегментів. Голосовий зразок зберігається в вигляді математичного коду.

4. Ідентифікація за райдужною оболонкою ока. Цей спосіб ідентифікації заснований на аналізі райдужної оболонки ока, що навколо зіниці. Зразки райдужної оболонки ока створюються з допомогою відеосистем. Такі системи можуть ідентифікувати особу, навіть якщо вона буде в окулярах чи лінзах. Ця система ідентифікації також дуже зручна у використанні і не потребує особистого контакту зі сканером. Ідентифікація за райдужною оболонкою ока застосовується упродовж декількох років і довела свою зручність і надійність.

5. Геометрична побудова руки і пальців. Цей спосіб ідентифікації доволі відомий, тому що використовується 20 років. Щоб ідентифікувати особу, системі достатньо виміряти фізичні характеристики пальців або руки: довжину, ширину, товщину. Цікавою характеристикою означеної технології є малий обсяг біометричного зразка, необхідного для ідентифікації (декілька байтів).

6. Ідентифікація за підписом. Ця технологія використовує аналіз динамічності підпису для ідентифікації людини. Технологія заснована на зміні швидкості, тиску і нахилу в момент підпису [4].

Тепер можемо зазначити про сильні сторони біометрії.

Переваги біометричних систем безпеки очевидні: унікальні людські якості хороші тим, що їх складно підробити, залишити фальшивий відбиток пальця за допомогою власного, або зробити райдужну оболонку свого ока схожою на чиюсь. На відміну від паперових ідентифікаторів (паспорт, водійські права, посвідчення особи), від пароля або персонального ідентифікаційного номера (ПІН), біометричні характеристики не можуть бути забуті або втрачені, через свою унікальність вони використовуються для запобігання крадіжці або шахрайству. Деякі люди вміють імітувати голоси, а в Голівуді навчилися гримувати людей так, що вони стають вражаюче схожі на інших, але це вимагає особливих навичок.

Застосування біометрії в сучасному світі може значно спростити наше життя. Не буде потрібно більше носити з собою пластикові карточки, запам'ятовувати паролі, чи брати перепустки на роботу. Паролем, кодом і перепусткою будемо ми ж.

Нині експерти вирізняють такі основні напрями застосування біометричних технологій [5, ст. 149]:

– безпека суспільства та держави;

– впровадження масштабних проектів створення паспортно-візових, фінансових і транспортних ідентифікаційних систем;

– облік робочого часу;

– контролю за доступом;

– захист інформації.

Наведемо приклади, як біометричні системи застосовуються на практиці у провідних країнах світу.

У Великій Британії компанія «Philips» створила кавову машину, яка сканує відбитки пальців користувачів. «Різні люди готують каву порізному, – пояснює Вів'єн Палмір, яка працює у «Philips». Тепер достатньо піднести до сенсора палець, машина «впізнає» його і приготує ваше звичне капучино, латте чи американо. Цим ми можемо переконатися, що речі, які нам здавалися і без того простими, можуть стати ще простішими.

З допомогою біометрії можна вирішувати і складніші завдання. Під час президентських виборів у Венесуелі, 7 жовтня 2006 року, за допомогою біометричних автоматичних комплексів, які сканували відбитки пальців виборців, перемогу Уго Чавеса оголосили за кілька хвилин після закінчення голосування. Відтак бюлетені підраховували вручну.

Результат повністю збігся з «електронним». Також у багатьох європейських країнах і США на прикордонних пунктах встановлено обладнання, яке зчитує інформацію з мікрочипа за кілька секунд, на відміну від перевірки паперового документа. Тому власники біометричних закордонних паспортів користуються спеціальними коридорами [6]. І це ще не всі способи застосування біометрії для зручності людини.

«Козирем» біометричних систем є їх здатність забезпечувати безпеку охоронюваного об'єкта. Доволі складно обманути біометричний пристрій. Саме тому біометричним системам одразу ж знайшли застосування в фінансовій, воєнній і промисловій сферах. Ними розпочали обладнувати аеропорти, банки, воєнні і промислові будівлі, закриті стратегічні об'єкти.

Один із швейцарських банків розпочав використовувати біометричну систему контролю доступу, засновану на тривимірній технології розпізнавання обличчя і райдужної оболонки ока, яка повністю виключила ризик втрати, крадіжки чи несанкціонованого доступу до використання ключів. Сканери райдужної оболонки були встановлені для обмеження доступу в сховище. Біометрична система контролю доступу, заснована на тривимірній технології сканування обличчя і райдужної оболонки ока, може працювати без ідентифікаційних карток, PIN-кодів і забезпечує найвищий рівень безпеки [7].

Використання біометрії в банкоматах і терміналах оплати допоможе суттєво знизити рівень шахрайства під час зняття грошей з рахунку.

Будь-яка територія, де забезпечується пропускний режим, неможлива без контрольно-пропускних пунктів (КПП). Найбільш простим способом забезпечувати пропускний режим було використання контролера-охоронця. Та для забезпечення вищого рівня безпеки на КПП застосовується система контролю і управління доступом, яка забезпечує більш якісний рівень роботи КПП, а також різко знижує рівень впливу «людського чинника» охоронця на пропускний режим, наприклад, втоми, розсіяності, сонливості [8].

Японські вчені створили водійське крісло з 360 датчиками тиску, яке на 98% розпізнає свого власника. Система реагує на вагу, розподіл маси тіла, який у кожної людини унікальний. Якщо водій гладшає, програма одразу про це повідомить [6].

У Диснейленді біометричним розпізнаванням відбитків пальців перевіряють, що один квиток використовується кожен раз однією і тією ж людиною [1].

Розрізняти користувачів комп'ютерів за рисами обличчя запропонувала компанія «XID Technologies». Мета – захистити конфіден-

ційну інформацію користувачів. До комп'ютера підключають вебкамеру і фіксують усіх, хто за нього сідає. Після цього програма порівнює зображення з тими, що занесені в її базу даних як дозволені. Упізнати справжнього господаря комп'ютера програма може незалежно від того, в окулярах він чи ні, відростив чи зголив вуса [6].

Стратегічний актив будь-якої компанії – це її працівники та їх робочий час. Реальний облік робочого часу дозволяє якісно вирішувати питання, що є основною діяльністю будь-якої організації. З допомогою біометричних пристроїв контролю робочого часу компанії зможуть вирішити такі питання, як реєстрація приходу і виходу персоналу, здійснення обліку робочого часу кожного працівника, формування звітності перебування працівника на роботі, можливість інформування начальства про присутність персоналу в режимі «онлайн», а також подолання одвічної проблеми карткових систем контролю робочого часу, коли один працівник збирає картки інших співробітників і одночасно реєструє особистий та прихід своїх колег [5, с. 179].

Попри всю користь і розвиток біометричних систем, у них є і недоліки.

Одним із них є те, що у випадку, коли злодії не можуть отримати доступ до охоронюваної власності, існує можливість вистежування і замаху на носія біометричних ідентифікаторів з метою отримання доступу. Якщо що-небудь захищено біометричним пристроєм, власникові може бути завдано незворотної шкоди. Наприклад, 2005 р. малайзійські викрадачі відрізали палець власнику Мерседес-Бенц S-класу за спроби вкрасти його авто [1].

Також перевагою паролів над біометрією є можливість їх зміни. Якщо пароль був вкрадений або загублений, його можна скасувати і замінити новою версією. Це стає неможливим у випадку з деякими варіантами біометрії. Якщо параметри якоїсь особи були вкрадені з бази даних, то їх не можна скасувати або видати нові. Біометричні дані з можливістю відміни є шляхом, який повинен охоплювати можливість скасування та заміни біометрії [1].

Доцільно зауважити, що умови сканування щоразу трішки відрізняються, а частини тіла, які підлягають скануванню, та поведінкові рефлекси особи також не зовсім постійні, тому можна говорити про неточне збігання зі зразком, а лише про ступінь подібності з еталоном. Тому всі біометричні системи характеризуються параметрами «можливість невизнання свого» (тобто вірогідність невпізнання зареєстрованої особи), та «можливістю визнання своїм чужого» (тобто є вірогідність, що проникне несанкціонований користувач) [9].

Ще одною проблемою є те, що надійність систем фірмами-виробниками старанно замовчується. Йдеться про захищеність систем від свідомого їх обману і способи симулювати об'єкт біометричного сканування. Наприклад, японський криптограф Цутумо Мацумото і група його студентів з університету Йокогами (непрофесійні зламачі) продемонстрували, як з допомогою підручних засобів можна обманути практично будь-яку з таких систем. Японські студенти перевірили 12 комерційних скануючих систем і кожну з них змогли обманути в 4 випадках з п'яти. Притому, що Мацумото зміг виготовити відбиток не тільки з дозволу власника, а й без його відома [9].

Відбитки пальців можна зняти з будь-якої гладкої поверхні, навіть зі сканера, з допомогою графітового порошку або желатину. Сканери райдужної оболонки також обманути не складно, достатньо використати фотографію райдужної оболонки особи, виконану з великим розширенням, або нанести проекцію райдужної оболонки на лінзу. Але, щоб виявити обман, нові пристрої реєструють «ознаки життя», а саме – пульсацію судин [10].

Є декілька видів шахрайського використання муляжів у біометричних системах [5, с. 223]:

– для доступу до конкретного електронного ресурсу або реального об'єкта;

– з метою компрометації конкретної особи, біометричну характеристику якої копіює муляж;

– анулювання операцій, учасники якої верифікувались за допомогою віддаленого доступу до біометричної системи.

Не потрібно забувати і про хакерів, які з допомогою комп'ютерних мереж здатні зламати сервер бази даних біометричних кодів. А біометричний код може чимало розповісти про індивіда – від його вроджених особливостей до хвороб.

Противниками впровадження біометричних систем, зокрема біометричних паспортів, є духовенство. Запровадження біометричних паспортів, на їхню думку, – це «знак на правій руці, або на чолі», знак антихриста [11].

Висновки. Розвиток біометрії є пріоритетною ланкою розвитку сучасних технологій. Найважливіше свідчення успіху біометричних систем – це її прийняття користувачами в розвинених країнах світу, таких як США, ФРН, Велика Британія, Франція та ін. Щоб біометричні системи були прийняті українським суспільством, необхідно врахувати такі три фактори: по-перше, пристрій не повинен викликати в користувача почуття дискомфорту; по-друге, біометричний пристрій має

бути простим у використанні; по-третє, біометричний пристрій повинен функціонувати надійно, чітко та точно. Проте жоден пристрій не може бути абсолютно досконалим, і біометричні системи – не виняток, вони також можуть помилятися, але потрібно зважати на те, що за подальшого розвитку біометрії її слабкі сторони будуть усуватися, а сильні – примножуватися. Наведено достатньо прикладів для того, щоб зрозуміти сильні та слабкі сторони біометричних систем, відтак вважаємо, що за біометрією – майбутнє. Також розвиток біометричних систем в Україні – це ще один із способів рухатися в ногу з часом. Біометрія дасть змогу почуватися безпечніше, тому що її основне завдання – боротьба зі злочинністю, тероризмом, способом збереження особистої інформації, підвищення комфорту громадян.

1. [Електронний ресурс]. – Режим доступу: http://znaimo.com.ua

2. [Електронний ресурс]. – Режим доступу: http://vseslova.com.ua›word/Біометрія-11220u

3. [Електронний ресурс]. – Режим доступу: http://tmb.org.ua/new/index.php/i-i/4-/138-2011-12-13-17-44-10.html

4. [Електронний ресурс]. – Режим доступу: http://www.gs1ru.org/technologies/biometrics/

5. 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.

6. [Електронний ресурс]. – Режим доступу: http://www.gazeta.ua/articles/opinions-journal/_biometriya/461546»>Gazeta.ua

7. [Електронний ресурс]. – Режим доступу: http://www.secuteck.ru/articles2/sys_ogr_dost/biometriya_na_strazhe_1

8. [Електронний ресурс]. – Режим доступу: http://www.bnti.ru/showart.asp?lvl=04.09.&aid=208

9. [Електронний ресурс]. – Режим доступу: http://www.bellabs.ru/SBiometry

10. [Електронний ресурс]. – Режим доступу: http://www.ccc.ru/magazine/depot/03_08/read.html?0502.htm

11. [Електронний ресурс]. – Режим доступу: http://inlegal.com.ua/raznoe/edynyi-derzhavnyi-demografichnyi-reestr-abo-pravova-biometriya.html

Гнидец Т. Я. Биометрия: сильные и слабые стороны

Рассмотрено понятие биометрии, ее режимы, классы, основные виды биометрических систем, сведения о некоторых сильных сторонах биометрии, ее применение в сфере безопасности общества и государства, учета рабочего времени, контроля доступа и при внедрении паспортно-визовых режимов. Приведены и некоторые недостатки, выделены противниками данных систем. Описан процесс внедрения биометрических систем в различные сферы жизни общества и государства ведущих стран мира.

Ключевые слова: *биометрия, идентификация, верификация, отпечатки пальцев, радужная оболочка, идентификация лица, идентификация по голосу, охранная система.*

Gnidets T. Y. Biometrics: strengths and weaknesses

The article considers the issues of biometry, its regulations, categories and main types of biometrical systems, such as scanning by the fingerprints, eye retina, form of face, voice, hand geometry, person's signature. It also contains some information about such strong sides of biometry, its application in the sphere of the society and state security, duly performance record, control for the access, protection of information and introduction passport and visa requirements, besides, the article also considers some drawbacks of biometrical systems which were singled out by its opponents, which includes the risk of attack on the bearer of biometric identifiers, impossibility of changing biometrical codes, lack of some biometric systems with the possibility of their breaking, and industrious suppression of the devices drawbacks by the producing companies. Special place was given to the description of the process of the biometric systems introduction into different spheres of everyday life of state and society in certain countries of the world.

When writing the article, the author's objective was to expound main issues as to the use of modern biometrical technologies, and, first of all, about existing of biometrical systems of protection and control as well as information about biometrical databases efficiently operating abroad.

In his article the author comes to the conclusion that the development of biometry is a top branch of modern technologies development. Therefore, in order for the biometric systems to be approved by the Ukrainian society, it is necessary to take into account the following three factors: first of all, the device should not produce the sense of discomfort; secondly, the biometric device should be user-friendly; thirdly, biometric device should operate reliably and accurately

Key words: *biometrics, identification, verification, fingerprints, iris, face identification, voice identification, security system.*

Стаття надійшла 25 грудня 2013 р.

УДК 343.123.12: 343.37

Н. Л. Гула

ПРАВОПОРУШЕННЯ, ЯКІ ВЧИНЯЮТЬСЯ У СФЕРІ ЦІЛЬОВИХ СПЕЦІАЛІЗОВАНИХ ДЕРЖАВНИХ ФОНДІВ

З'ясовано основні види правопорушень, які скоюються у сфері цільових спеціалізованих державних фондів. Зазначено, що посягання на бюджетні кошти, спрямовані на соціальну підтримку населення, охоплюють більше 20% злочинів, учинених у бюджетній сфері. Акцентовано на способах учинення