УДК 57.001

А.О. МОРОЗ

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ЛЮДИНИ. ОГЛЯД СИСТЕМ

Анотація. *У статті розглянуті біометричні методи ідентифікації людини, їх розвиток та сучасне застосування. Наведені приклади розвитку біометричних систем та їх роль у світі інформаційних технологій.*
Ключові слова: *біометричні технології, біометричні системи, ідентифікація.*

Аннотация. *В статье рассмотрены биометрические методы идентификации человека, их развитие и применение в современном мире. Приведены примеры развития биометрических технологий и их роль в мире информационных технологий.*
Ключевые слова: *биометрические технологии, биометрические системы, идентификация.*

Abstract. *Biometric methods of identification of a person with their development and application in the modern world are considered. Examples of the development of biometric systems and their role in the universe of information technologies are given.*
Key words: *biometric technologies, biometric systems, identification.*

1. Вступ

Біометрія вже давно перейшла із розряду фантастики до розряду сучасних технологій, що набули нового, вужчого значення. Зараз під біометричними технологіями найчастіше розуміють автоматичні або автоматизовані методи розпізнавання особи людини за його біологічними характеристиками або проявами.

Найдавніші методи ідентифікації мали механічний характер, грунтувалися переважно на використанні певних технічних значень. Цей же принцип ліг в основу новітніх технологій з використанням пластикових бейджів, магнітних смарт-карток з електронним чи оптичним пристроєм запам'ятовування. В цих системах передбачений досить високий рівень захисту від підробок, копіювання і фальсифікації. Разом з тим технічним системам притаманна одна дуже суттєва вада: орієнтування на верифікацію самого предмета авторизації – картку, бейдж, посвідчення, а не на саму персону-власника. Система контролю доступу в даному разі відстежує проходження карток без підтвердження ідентичності персони, що скористалась ними. Іншими словами, картка може бути загублена, викрадена, передана і використана іншою особою.

Системи, які грунтуються на спеціальних знаннях, а саме на паролях та секретних кодах, намагаються виключити ці недоліки. Разом з картками вони значно підвищують рівень безпеки. Проте паролі забуваються, записуються на аркушах паперу, передаються по телефону і викрадаються через підглядування за допомогою прихованих відеокамер, клавіатурних шпигунів тощо. Але нові технологічні рішення розвиваються за тими ж законами, що і все людське суспільство. Спіраль прогресу вивела на нові можливості використання архаїчного методу авторизації за допомогою пальця, прикладеного до документа. Це і привело до появи сучасної технології біометрії. Єдиним напрямом для беззаперечної ідентифікації особи є автоматичне визначення її особистих характеристик, які називаються біометричними. Відповідно до цього з'явилась і нова технологія ідентифікації – біометрична. В основі її лежить розуміння, що архаїчний відбиток пальця може бути тим самим, практично неповторним, об'єктом, за яким повністю ідентифікується персона. Недарма в дуже важливих моментах для посвідчення особи, наприклад, під час голосування в парламенті Туреччини, використовується біометрична система ідентифікації з автоматичною перевіркою відбитка пальця.

ISSN 1028-9763. Математичні машини і системи, 2011, № 1

Діяльність приватних фірм, урядових організацій і лабораторій, що займаються питаннями біометрії, координується Біометричним Консорціумом BIOAPI Consortium [1]. Провідними виробниками біометричних систем є: Biolink Technologies [2], Bioscrypt [3], Precise Biometrics [4], Neurotechnology [5], Digitalpersona [6], Identix [7] та ін.

Відповідно на ринок виходить все більше продуктів, які використовують біометричні технології, починаючи з usb-накопичувачів зі сканером відбитків пальців і закінчуючи корпоративними системами обліку робочого часу і контролю доступу.

Прикладами таких систем можуть бути автоматизована дактилоскопічна ідентифікаційна система по слідах і відбитках пальців і долонь «АДІС Папілон» [8] (Росія), система обліку робочого часу і контролю доступу по відбитках пальців BioTime [9] (Росія), Next Generation Identification (NGI) [10] глобальна система ідентифікації, що розробляється ФБР.

Нині існують різні способи і методи біометричної ідентифікації, але вони базуються в основному на вимірюванні фізіологічних властивостей, а також особливостях поведінки особи. Серед них такі напрямки, як розпізнавання за геометрією руки і пальців, венозною структурою, райдужною оболонкою, внутрішньою структурою дна ока, рисами обличчя, відбитками пальців. Відомі спроби використання для цих цілей зовнішньої форми вуха, структури долоней і навіть запаху людського тіла, хоча результати практичного застосування останнього невідомі [11].

До високоефективних, з точки зору вірогідності, методів можна віднести ідентифікацію за аналізом ДНК людини. Досі не існувало таких технологічних рішень, які уможливили б її ширше використання. Устаткування для ДНК- тесту надто дороге: біохімічна лабораторія. Хоча на хвилі боротьби з тероризмом і криміналом кількість таких лабораторій в Європі та Північній Америці значно зростає.

Події 11 вересня 2001 року значно змінили відношення до біометрії в світі. Практично відразу після 11 вересня 2001 року при Міжнародній організації по стандартах (ISO) був створений підкомітет Sc37 з біометрії, покликаний оперативно розробити і затвердити єдині міжнародні стандарти використання, обміну і зберігання біометричних даних. Аналогічні комітети створені в багатьох національних органах зі стандартів. Одним із перших з'явився комітет М1 при Американському національному інституті стандартів (ANSI), аналогічний підкомітет ПК7 створений у Федеральному агентстві з технічного регулювання і метрології Росії.

З січня 2004 року в США розпочалася програма US-Visit. Всі прибулі були зобов’язані проходити процедуру біометричної ідентифікації особи, тепер таку саму процедуру їм доведеться проходити і при виїзді з США.

В ЄС та Росії готуються до введення електронних паспортів, що містять біометричну інформацію. Планується також введення єдиного європейського посвідчення для водія з біометричною інформацією. Аналогічні програми почалися в багатьох країнах Азії.

Швидкість операції розпізнавання або ідентифікації в сучасних біометричних системах навіть за наявності тисяч користувачів (доступ персоналу до великих підприємств, аеропортів, атомних станцій) вимірюється секундами, тобто відповідає запитам виробничого режиму. Відомо, що найпершими користувачами систем біометричної ідентифікації були організації з високим рівнем безпеки: банки, арсенали, паспортні системи.

Деякі інформаційні джерела (приміром, Р. Браделін. Швейцарія "Що значить біометрія") наводять приклади використання біометричних систем. Повідомляється, скажімо, про центр з виготовлення і продажу ювелірних виробів, де персоналу 5500 чоловік і понад 7000 відвідувачів. Там облаштовано 30 пунктів доступу і всі пункти прийому клієнтів пристроями біометрії на відбиток пальця в комплексі з бейджами, що були встановлені раніше. В багатьох міжнародних аеропортах, наприклад, у Празі, крім персоналу, біометричну перевірку за відбитками пальців проходять всі водії автотранспорту, що заїжджають на те-

риторію. Багато банківських закладів у Європі, особливо в Швейцарії, для доступу клієнтів до депозитних сейфів встановили біометричні системи на відбитках пальців або розпізнавання по обличчю. Це дає змогу клієнтам користуватись депозитними сейфами без присутності клерків банку. Одна з найбільших систем супермаркетів в Австралії з 450 вихідними терміналами і персоналом 7500 чоловік оснащена біометричною системою з відбитками пальців. Це дає змогу уникнути порушень режиму безпеки, шахрайства, а також забезпечити повний контроль використання робочого часу персоналу.

Можливості використання біометричних систем у службах прикордонного контролю, паспортах, ідентифікаційних картках, посвідченнях водіїв прискориться з введенням єдиних міжнародних стандартів. Хоча деякі країни ефективно використовують біометричні системи за внутрішніми стандартами. В Південно-Африканській Республіці, Іспанії, Колумбії біометрію за відбитками пальців упроваджено в системах соціальних виплат і державних пенсійних фондах. Це зменшило ризики і суми несанкціонованих виплат, які завдавали відчутні збитки державі.

На українському ринку з'явилася пропозиція щодо біометричних пристроїв для унеможливлення доступу до комп'ютерних систем і мережевих ресурсів. Основані на методах ідентифікації за відбитками пальців, невеликих розмірів, зручні і прості в користуванні, ці системи унеможливлюють неавторизований доступ до комп'ютерних і мережевих ресурсів. Це може стати ефективним інструментом для інформаційних систем типу "клієнт-банк". Зразки таких рішень працюють у банках азіатського регіону та в Єгипті. Біометрія в комплексі із криптографічними засобами може бути встановлена в системах плебісциту чи голосування, в тому числі для забезпечення посвідчення персони і на різних рівнях передачі результатів плебісциту для подальшої обробки. При цьому база даних темплейтів біометричної системи знаходиться на різних рівнях в архітектурі мережі.

На сьогодні існує безліч методів біометричної аутентифікації, які поділяються на такі дві групи [12].

2. Статичні методи

Статичні методи біометричної аутентифікації грунтуються на фізіологічній (статичній) характеристиці людини, тобто унікальній характеристиці, даній їй від народження.

• Автоматичний face-контроль

Макіяж, вікові зміни, вживання міцних напоїв — всі ці чинники утрудняють ідентифікацію особи по обличчю. Навіть для експерта ідентифікація людини по фотографії десятирічної давності може виявитися дуже складним завданням. Біометричні технології дозволяють проводити face-контроль в автоматичному режимі, вони звіряють параметри обличчя об'єкта, який зафіксований камерою, з даними в базі. І достовірність такого аналізу складає 86–93%. Це значно більше за звичайні людські можливості. Проте проблема полягає в тому, що для здійснення цієї функції необхідне устаткування високої якості. Навіть для проведення візуальної ідентифікації особи відстань між центрами зіниць має бути еквівалентною 200 пікселям.

Сюди входять такі методи, як аутентифікація людини за формою обличчя, термограмою обличчя.

• За формою обличчя

У даному методі ідентифікації будується тривимірний образ обличчя людини. На обличчі виділяються контури брів, очей, носа, губ і т.д., обчислюється відстань між ними і будується не просто образ, а ще безліч його варіантів на випадки повороту особи, нахилу, зміни виразу. Кількість образів варіюється залежно від мети використання даного способу (для аутентифікації, верифікації, видаленого пошуку на великих територіях і т.д.).

• За термограмою обличчя

В основі даного способу аутентифікації лежить унікальність розподілу на обличчі артерій, що забезпечують кров'ю шкіру і виділяють тепло. Для здобуття термограми використовуються спеціальні камери інфрачервоного діапазону. На відміну від попереднього цей метод дозволяє розрізняти близнят.

• За відбитком пальця

В основі цього методу лежить унікальність для кожної людини малюнка папілярних узорів на пальцях. Відбиток, отриманий за допомогою спеціального сканера, перетворюється в цифровий код (згортку) і порівнюється з раніше введеним еталоном. Дана технологія є найрозповсюдженішою в порівнянні з іншими методами біометричної аутентифікації.

Наприклад, у Росії в МВС використовується система «АДІС-ПАПІЛОН», в якій містяться дактилоскопічні дані про десятки мільйонів осіб, що знаходяться на обліку в правоохоронних органах. Ця система здійснює автоматичну ідентифікацію затриманих.

• За формою долоні

Даний метод побудований на геометрії грона руки. За допомогою спеціального пристрою, що складається з камери і декількох підсвічуючих діодів (включаючись по черзі, вони дають різні проекції долоні), будується тривимірний образ грона руки, за яким формується згортка і розпізнається людина.

• За розташуванням вен на лицьовій стороні долоні

За допомогою інфрачервоної камери прочитується малюнок вен на лицьовій стороні долоні або грона руки. Отримана картинка обробляється, і за схемою розташування вен формується цифрова згортка. Ця технологія досить надійна. Основний її недолік полягає в тому, що якщо за відбитками пальців можна перевірити, чи не знаходиться людина в розшуку, чи має вона судимість, то для таких біометричних параметрів, як венозний малюнок, єдиної бази не існує.

• За сітківкою ока

Це спосіб ідентифікації по малюнку кровоносних судин очного дна. Для того, щоб цей малюнок став видний, людині потрібно поглянути на видалену світлову крапку, і очне дно, що таким чином підсвічується, сканується спеціальною камерою.

• За радужною оболонкою ока

Малюнок радужної оболонки ока також є унікальною харатеристикою людини. Причому для її сканування досить портативної камери із спеціалізованим програмним забезпеченням, що дозволяє захоплювати зображення частини лиця, з якого виділяється зображення ока, з якого, у свою чергу, виділяється малюнок веселкової оболонки, за яким і будується цифровий код для ідентифікації людини.

При використанні цієї технології об'єкта необхідно позиціонувати свою особу для реєстрації якісного зображення веселкової оболонки очей, що, звичайно, не завжди зручно. Наприклад, при face-контролі подібних вимог не існує. Людина йде по коридору, в той момент, коли вона попаде в зону найкращого бачення, камера робить контрольний знімок. При ідентифікації особи за зображенням обличчя і радужної оболонки ока необхідно враховувати також і зовнішні умови. Залежно від фону і рівня освітленості вірогідність розпізнавання міняється. Тому в ідеалі треба помістити людину в стандартизовані умови, наприклад, в ізольовану кабіну.

• За ДНК

Переваги даного способу очевидні, проте використовувані в даний час методи здобуття і обробки ДНК працюють настільки довго, що такі системи використовуються лише для спеціалізованих експертиз.

• Інші методи

У даній статті описані лише найпоширеніші методи. Існують ще такі унікальні способи, як ідентифікація за підігтьовим шаром шкіри, за об'ємом вказаних для сканування пальців, формою вуха, запахом тіла тощо [12].

3. Динамічні методи

Динамічні методи біометричної аутентифікації грунтуються на поведінковій (динамічній) характеристиці людини, тобто побудовані на особливостях, характерних для підсвідомих рухів у процесі відтворення якої-небудь дії.

Розглянемо методи аутентифікації цієї групи.

• За почерком

Як правило, для цього виду ідентифікації людини використовується його розпис (інколи написання кодового слова). Цифровий код індентифікації формується залежно від необхідної міри захисту і наявності устаткування (графічний планшет, екран карманного комп'ютера Palm і т.д.) двох типів:

1. За самим розписом, тобто для ідентифікації використовується просто міра збігу двох картинок.

2. За розписом і динамічними характеристиками написання, тобто для ідентифікації будується згортка, в яку входить інформація по безпосередньому підпису, тимчасовим характеристикам нанесення розпису і статистичним характеристикам динаміки натиску на поверхню.

• За клавіатурним почерком

Метод у цілому аналогічний описаному, але замість розпису використовується кодове слово (коли для цього використовується особистий пароль користувача, таку аутентифікацію називають двофакторною) і не потрібно жодного спеціального устаткування, окрім стандартної клавіатури. Основною характеристикою, за якою будується згортка для ідентифікації, є динаміка набору кодового слова.

• За голосом

Одна із старих технологій, у даний час її розвиток прискорився, оскільки передбачається її широке використання в побудові «інтелектуальних будівель». Існує досить багато способів побудови ідентифікації за голосом, як правило, це різні поєднання частотних і статистичних характеристик голосу.

У Росії в МГТУ імені Н.Е. Баумана розроблений програмний продукт, який за 15-секундним звучанням фрази дозволяє ідентифікувати людину з досить високою вірогідністю.

• Інші методи

Для даної групи методів також описані лише найпоширеніші методи. Існують такі унікальні способи, як ідентифікація за рухом губ при відтворенні кодового слова, за динамікою повороту ключа в дверному замку і т.д.

Загальною характеристикою, яку використовують для порівняння різних методів і способів біометричної ідентифікації, є статистичні показники: помилка першого роду (не пустити в систему «свого») і помилка другого роду (пустити в систему чужого).

Сортувати і порівнювати описані вище біометричні методи за свідченнями помилок першого роду дуже складно, оскільки вони є різними для одних і тих же методів у зв’язку з залежністю від устаткування, на якому вони реалізовані.

За показниками помилок другого роду загальне сортування методів біометричної аутентифікації виглядає приблизно так (від кращих до гірших):

• ДНК.
• Радужна оболонка ока, сітківка ока.
• Відбиток пальця, термограма обличчя, форма долоні.
• Форма обличчя, розміщення вен на долоні та кисті руки.
• Розпис.
• Клавіатурний почерк.
• Голос.

У даний час активно розвивається технологія розпізнавання особи за підписом. Вона заснована на тому факті, що, якщо у людини хороша асоціативна пам'ять, вона може скопіювати чужий підпис, але повторити динаміку виконання неможливо.

Існує біометрична технологія ідентифікації особи по роботі на клавіатурі. Спеціальна система фіксує швидкість, силу, особливість натиснення клавіш. І якщо параметри, закладені як ключ до доступу, і параметри миттєвого користувача не збігаються, система повинна блокувати комп'ютер. У світі вже розроблена технологія, яка фіксує розташування користувача відносно екрану: якщо об'єкт випадає з поля зору, то екран відключається, якщо система фіксує другий об'єкт напроти екрану, то він також відключається.

Одним із основних завдань, які стоять перед «біометричним» суспільством, є ефективне використання біометричних технологій при вирішенні різних практичних завдань.

Для vip-персон зручно використовувати технологію ідентифікації особи за геометрією руки. В даному випадку об'єкту необов'язково навіть класти руку на сканер. В інфрачервоному світлі автоматично знімаються параметри і відбувається ідентифікація.

Враховуючи все вищезазначене, ми дійшли до такого висновку: біометрія й основані на її принципах системи стали ефективним засобом забезпечення всіх видів власності, захисту від шахрайства, фальсифікації та криміналу. Їх подальше впровадження в різні галузі є актуальним завданням, адже це забезпечить створення зручних і надійних інструментів як для державного сектору, індустріальних і комерційних структур, так і для окремих громадян. Біометрія, при нашому бажанні, стане надійним захистом.

Подальший прогноз не викликає особливих сумнівів відносно біометричної паспортизації населення.

Які ж глобальні зміни чекають світ у 2010–2020 роках?

1. Практично все населення землі матиме біометричні посвідчення особи. Уся інформація буде зберігається в державних базах даних, об'єднаних у глобальну міжнародну ідентифікаційну систему.

2. Реальністю стане не лише ідентифікація особи, але й ідентифікація думок і намірів. При пересіченні кордонів держави або при доступі на певні об'єкти чоловік проходить автоматичне психофізіологічне тестування протягом реального часу (не більше 10 секунд) на предмет представлення небезпеки для цієї держави або об'єкта.

Україна

Згідно з рекомендаціями Міжнародної організації цивільної авіації (ICAO) до 1 квітня 2010 року 189 держав-членів цієї організації (серед яких і Україна) зобов’язалися забезпечити своїх громадян так званими біометричними закордонними паспортами. Це машинозчитувані електронні ІД-документи, в які імплантовано RFID-чіп (RFID – радіочастотна ідентифікація). В чіп записуються біометричні характеристики власника закордонного паспорта: відбитки пальців, сітківка ока, геометрія руки та ін., в залежності від вимог законодавства тієї чи іншої країни (конкретний біометричний параметр визначається законодавчо).

У зв’язку з прийняттям Верховною Радою від 23 лютого 2007 року Постанови «Про внесення змін до Постанови Верховної Ради «Про затвердження положень про паспорт громадянина України і свідоцтво про народження»» найближчим часом Україна розпочне виробництво закордонних паспортів нового зразка.

Вищевказаною Постановою Верховної Ради також прийнято «Положення про паспорт громадянина України для виїзду за кордон». Положення передбачає, що додаткова інформація, зокрема, біометрична, про власника закордонного паспорта, зміст якої визначається чинним законодавством, може зберігатися на безконтактному електронному носієві, вмонтованому в документ.

Відповідно до вимог ICAO, обов’язковою інформацією для біометричної ідентифікації особи є зображення обличчя власника документа (форма людського обличчя має суто індівідуальні характеристики і у цифровому форматі записується на чіп). Інша біометрична

інформація в закордонному паспорті (відбитки пальців, сітківка ока, геометрія руки та ін.) використовується лише як факультативна. Тобто кожна країна використовує її на власний розсуд.

Україні залишилося лише визначитися, яка ж факультативна інформація відображатиметься в закордонному паспорті.

4. Висновки

Актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням числа об'єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу, а саме: криміналістика; системи контролю доступу; системи ідентифікації особи; системи електронної комерції; інформаційна безпека (доступ в мережу, вхід на ПК); облік робочого часу і реєстрація відвідувачів; системи голосування; проведення електронних платежів; аутентифікація на web-ресурсах; різні соціальні проекти, де потрібна ідентифікація людей; проекти цивільної ідентифікації (пересічення державних кордонів, видача віз на відвідини країни) і т.д.

Враховуючи, що більшість методів представляє собою комерційну таємницю, в даному випадку важко виділити кращий метод, оскільки порівнювати доцільно алгоритмічно-апаратний комплекс. Зараз проводяться розробки по зменшенню розмірів та ціни системи, збільшенню надійності роботи. Для систем, що вимагають особливі вимоги до безпеки, використовуватимуться мультимодальні біометрики. Використання біометричних засобів спрощує процедуру аутентифікації особи, а також піднімає надійність систем безпеки.

СПИСОК ЛІТЕРАТУРИ

1. BioAPI Consortium (Биометрический консорциум) [Електронний ресурс]. – Режим доступу: http://www.bioapi.org.
2. BioLink: защита информации, учет рабочего времени и контроль доступа средствами идентификации, сканерами отпечатков пальцев, голоса и лица, СКД, СКУД [Электронный ресурс]. – Режим доступа: http://www.biolink.ru.
3. Bioscrypt – enterprise access control [Електронний ресурс]. – Режим доступу: www.l1id.com/enterpriseaccess.
4. Precise Biometrics – World-leading provider of Match-on-Card, biometrics for smart cards [Електронний ресурс]. – Режим доступу: http://www.precisebiometrics.com.
5. Neurotechnology – Fingerprint, face and eye iris identification software, AI and mobile robotics research [Електронний ресурс]. – Режим доступу: http://www.neurotechnology.com.
6. DigitalPersona Fingerprint Identity Solutions for Identity Protection, Security and Compliance [Електронний ресурс]. – Режим доступу: http://www.digitalpersona.com.
7. Identix – Protecting and Securing Personal Identities and Assets [Електронний ресурс]. – Режим доступу: http://www.l1id.com/pages/17.
8. Автоматизированная дактилоскопическая информационно-поисковая система АДИС ПАПИЛОН [Электронный ресурс]. – Режим доступа: http://www.papillon.ru/rus/16/?PHPSESSID=8813bf02f4ee087c82abbad19a824515.
9. Система учета рабочего времени и контроля доступа по отпечаткам пальцев BioTime [Электронный ресурс]. – Режим доступа: http://www.biotime.ru.
10. Next Generation Identification (NGI) – Новое поколение идентификации [Электронный ресурс]. – Режим доступа: http://www.fbi.gov/hq/cjisd/ngi.htm.
11. Біометрія як універсальний спосіб ідентифікації людини [Електронний ресурс]. – Режим доступу: http://bablyukh.clan.su/publ/1-1-0-4.
12. Різник О. «Біокон» – система біометричної ідентифікації користувача комп'ютерної мережі / О. Різник, Д. Дзюба, А. Чернодуб // Системи підтримки прийняття рішень. Теорія і практика: зб. доп. наук.-прак. конф. з міжнар. участю. «СППР 2009». – Київ, 2009. – С. 189 – 193.

Стаття надійшла до редакції 12.01.2011