КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

V. Romanov, I. Galelyuka, P. Klochan

TECHNOLOGIES FOR PERSON AUTHENTICATION BY USING BIOMETRIC CHARACTERISTICS

It is analyzed the state in the field of standardization on biometrics and described fundamentals of biometric technologies of person authentication by using person biometric characteristics.
Key words: biometric, biometric authentication, biometric technology.

Проанализировано состояние стандартизации в области биометрии и рассмотрены основы биометрических технологий, которые предназначены для аутентификации личности на основе использования биометрических характеристик личности.
Ключевые слова: биометрия, биометрическая аутентификация, биометрическая технология.

Проаналізовано стан стандартизації в області біометрії та розглянуто основи біометричних технологій, які призначені для аутентифікації особи на основі використання біометричних характеристик людини.
Ключові слова: біометрія, біометрична аутентифікація, біометрична технологія.

УДК 381.3

В.О. РОМАНОВ, І.Б. ГАЛЕЛЮКА,
П.С. КЛОЧАН

ТЕХНОЛОГІЇ АУТЕНТИФІКАЦІЇ ОСОБИ ЗА БІОМЕТРИЧНИМИ ХАРАКТЕРИСТИКАМИ

Вступ. Євросоюзом на даний час вже прийняті заходи по впровадженню до 2012 року паспортів з біометричними даними для громадян країн Шенгенської зони. На сьогоднішній день у паспортах громадян 34 країн вказуються біометричні дані.

Рішення про перехід до біометричної ідентифікації особи в Україні передбачені Державною цільовою програмою по організації і реконструкції державного кордону, причому ці заходи мають бути завершені до 2015 року. Дослідна експлуатація засобів біометричного контролю у тестовому режимі вже сьогодні відбувається в аеропорту "Бориспіль". В Україні біометричні технології ідентифікації особи ще не здобули широкого розповсюдження. Але така ситуація не може довго продовжуватися, оскільки Україна має спільний державний кордон з п'ятьма країнами – членами Європейського Союзу.

Враховуючи практику розвинутих країн, Верховна рада 14 квітня 2009 року прийняла зміни до закону "Про правовий статус іноземців і осіб без громадянства", які передбачають збір біометричних даних іноземців при видачі віз всіма консульствами і дипломатичними представництвами України, а також прикордонниками при перетині вказаними особами державного кордону. Ця процедура мала бути введена з 1 січня 2010 року. Слід зазначити, що в травні 2009 року Президент України повернув закон у Верховну Раду для повторного розгляду, мотивуючи це тим, що в Україні на той час були відсутні законодавчі гарантії захисту персональних біометричних

даних від несанкціонованого доступу при їх автоматичній обробці [1].

Загальна частина. Біометрія (Biometrics) – технологія ідентифікації особи, яка використовує фізіологічні параметри суб'єкта (код ДНК, відбитки пальців, райдужну оболонку ока, зображення обличчя, тембр голосу і т. п.). Біометричні технології активно використовуються в багатьох областях, які пов'язані зі захистом доступу до конфіденційної інформації, до матеріальних цінностей, при перетині державного кордону і т. п.

Стандарти в області біометрії розробляються підкомітетом SC 37 "Біометрія" Технічного комітету ISO/IEC JTC 1 "Інформаційні технології". У роботі підкомітету приймає участь 26 країн, серед яких є і Україна. Ще 10 країн беруть участь у роботі підкомітету як спостерігачі. Підкомітетом "Біометрія" розроблено 39 стандартів [2]. Слід зазначити, що розроблені на даний час стандарти [3] охоплюють такі напрями біометрії:

1) біометричний прикладний програмний інтерфейс (БіоППІ) та біометричний графічний інтерфейс користувача;

2) специфікація елементів та форматів біометричних даних;

3) процедури дій органу реєстрації у сфері біометрії та специфікацію формату провідної організації;

4) статистичні та динамічні біометричні параметри: дані та шаблон відбитка пальця, зображення обличчя, радужна оболонка ока, характеристики підпису, спектральні та контурні дані рисунка відбитка пальця, зображення сосудів і геометричні дані силуету кисті;

5) експлуатаційні випробування, випробування на відповідність та протоколи випробувань у біометрії;

6) біометричні профілі, процедури контролю доступу для працівників аеропортів, біометрична верифікація та ідентифікація особи моряків;

7) протоколи взаємодії при використанні біометричного прикладного програмного інтерфейсу;

8) фіксація відбитків десяти пальців з використанням біометричного прикладного програмного інтерфейсу.

Під фіксацією мається на увазі процес отримання біометричного зразка від особи, що взаємодіє з біометричною системою для реєстрації або ідентифікації своєї особистості. До біометричного зразка можна віднести не тільки інформацію, яку отримано з сенсора, але і ту, яку отримуємо після обробки.

Робота по гармонізації міжнародних стандартів з біометричної ідентифікації особи на даний час виконується відповідним Національним підкомітетом України, яким на початок 2010 року підготовлено до впровадження в дію стандарти, які стосуються тільки біометричних інтерфейсів, форматів біометричних даних, зображення обличчя, зображення відбитка пальця, процедур дій органу реєстрації у сфері біометрії, специфікації формату провідної організації, експлуатаційних випробувань та відповідних протоколів.

Слід зауважити, що діяльність відповідного міжнародного підкомітету ISO/IEC направлена на стандартизацію усіх областей біометрії. Узагальнена модель взаємозв'язку стандартизованих областей біометрії показана на рис. 1.

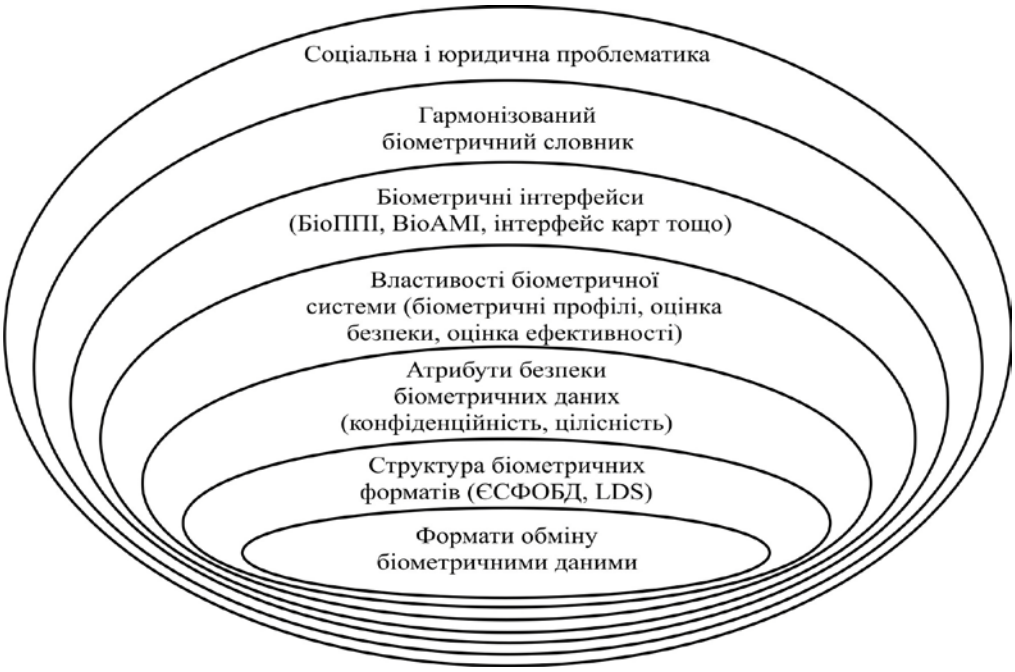

РИС. 1. Узагальнена модель взаємозв'язку стандартизованих областей біометрії

Біометричні дані, які містять у собі біометричну характеристику особи і відповідають стандартизованим форматам обміну біометричними даними, представляють собою ядро біометричної сумісності. Такі структури біометричних форматів, які визначені в ISO/IEC 19785-1 [4] як єдина система форматів обміну біометричними даними (ЄСФОБД), служать обгорткою навколо біометричних даних. Оскільки біометричні дані є таємними даними й об'єктом атак, то вони підлягають захисту й в середовищах обміну цими даними має використовуватись криптографічний захист. Біометричні властивості профілів, оцінки безпеки й ефективності відіграють важливу роль при реалізації біометричних систем різного типу. Біометричні інтерфейси є необхідними засобами для покращення інтеграції і використання різноманітних біометричних компонентів, у тому числі тих, які створені різними виробниками. Гармонізований словник біометричних термінів, який на даний час знаходиться у постійному розвитку, рекомендується використовувати при створенні та реалізації всіх біометричних технологій. Створення і впровадження прикладних рішень з використанням біометричної верифікації або ідентифікації визначаються соціальними і юридичними вимогами і, відповідно, мають місце в контексті зазначених вимог.

Біометричні технології. Як правило, при класифікації біометричних технологій виділяють дві групи систем за типом біометричних параметрів, що використовуються. Перша група використовує статичні біометричні параметри: від-

битки пальців, геометрію руки, зображення обличчя, райдужна оболонка ока і т. п. Друга група використовує динамічні параметри: динаміку відтворення підпису або рукописного ключового слова, тембр голосу і т. п.

Усі біометричні технології характеризуються однаковою базовою моделлю. Спочатку необхідно створити первинний реєстраційний шаблон користувача. Ця операція здійснюється шляхом збору кількох зразків за допомогою будь-якого біометричного сенсора. Далі зі зразків добуваються характерні ознаки й отримані результати об'єднуються згідно певного алгоритму в шаблон. Процес створення даного первинного шаблона називається реєстрацією (або фіксацією). Алгоритми, які використовуються для створення шаблонів, можуть бути запатентовані за бажанням розробника. Первинний шаблон зберігається прикладною програмою як контрольний шаблон. Також можна зберігати цей шаблон за допомогою спеціальних засобів у відповідному модулі архіву біометричного прикладного програмного інтерфейсу.

Отже, кожного разу, коли необхідно аутентифікувати користувача, з сенсора отримують "живі" зразки (або зразок), обробляють їх для подання в придатній для використання формі та зіставляють із раніше зареєстрованим контрольним шаблоном. Таку форму біометричної аутентифікації називають верифікацією, оскільки проводиться перевірка того, чи є користувач тим, ким він себе називає (тобто перевіряється заявлена особистість). У стандартах термін "біометрична верифікація" визначається як автоматизований процес оцінювання твердження про те, що поданий біометричний зразок (зразки) та вже збережений біометричний шаблон належать одному й тому самому джерелу біометричної інформації.

Крім того, біометричні технології використовують іншу форму аутентифікації, яка називається ідентифікацією. При ідентифікації користувачу не потрібно заявляти свою особистість. У даному випадку оброблені "живі" зразки користувача порівнюються з базою контрольних шаблонів і приймається рішення про те, який з них має найбільший ступінь схожості. Залежно від отриманого результату може бути ухвалене рішення про ідентичність користувача та особи, шаблон якої має найбільший ступінь схожості з урахування порогу ступеня схожості. В біометричних стандартах термін "біометрична ідентифікація" визначається як процес порівняння поданих біометричних даних з усіма шаблонами в базі даних (схема "один до декількох") з метою визначення відповідності та, якщо відповідність визначено, ідентифікації відповідної особи.

Можлива архітектурна реалізації вищенаведеної базової моделі зображена на рис. 2. Стадії, зазначені над блоком "Постачальник біометричної служби", відповідають елементарним функціям інтерфейсу верхнього рівня: отримання зразка, обробка та зіставлення. Різні стадії операцій верифікації та ідентифікації показані у блоці, позначеному як "постачальник біометричний служби". Під постачальником біометричної служби розуміється компонент прикладної програми, який здійснює біометричні операції за допомогою певного інтерфейсу або шляхом безпосереднього керування одним або декількома модулями біометричного прикладного програмного інтерфейсу, або з використанням наперед визначених функцій.

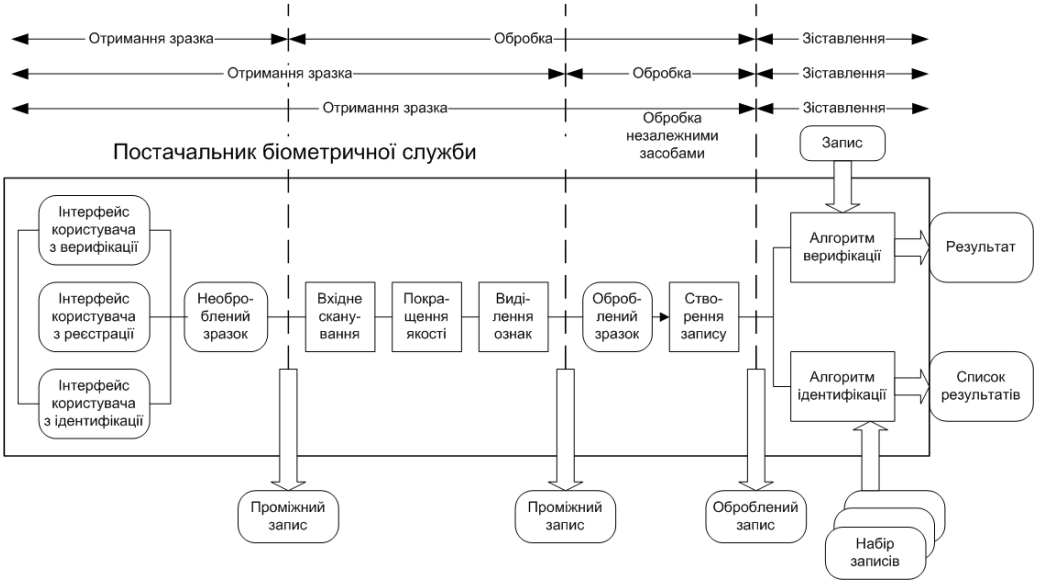

РИС. 2. Можлива архітектурна реалізація базової моделі

Поняття біометричної системи. Під біометричною системою розуміється автоматизована система, здатна знімати з сенсорів дані про користувача, обробляти отримані дані, добувати дані ознак з оброблених даних, порівнювати добуті ознаки з даними одного або більше біометричних шаблонів, визначати ступінь їх збігу та відображати успішність верифікації або ідентифікації особистості.

Дати визначення та відобразити узагальнену біометричну систему досить складно, оскільки слід врахувати різноманітні біометричні застосування і технології. Але, тим не менш, можливо виділити загальні елементи, які характерні будь-якій біометричній системі. Біометричні зразки здобувають з об'єкта за допомогою сенсорів. Вихідні дані з сенсора передаються на обробку даних, при якій добувають відмінні, але обов'язково повторювані ознаки зразка, і відкидають всі інші дані. Виділені в такий спосіб ознаки можуть бути збережені в базі даних у вигляді "шаблона" або піддані порівнянню з окремим шаблоном, декількома шаблонами або всіма шаблонами, що зберігаються в базі даних. Метою цього порівняння є визначення ступеня збігу, на підставі якого приймається рішення про визнання особи за результатами зіставлення ознак зразка і шаблонів.

Інформаційні потоки в узагальненій біометричні системі та її структурні компоненти подані на рис. 3. Система складається з підсистем фіксації даних, обробки сигналів, зберігання, зіставлення й ухвалення рішення. Схема ілюструє процеси реєстрації, верифікації й ідентифікації. Слід відмітити, що елементи, надані в даній концептуальній моделі, можуть бути відсутні або не відповідати безпосередньо фізичним компонентам у реальній біометричній системі.

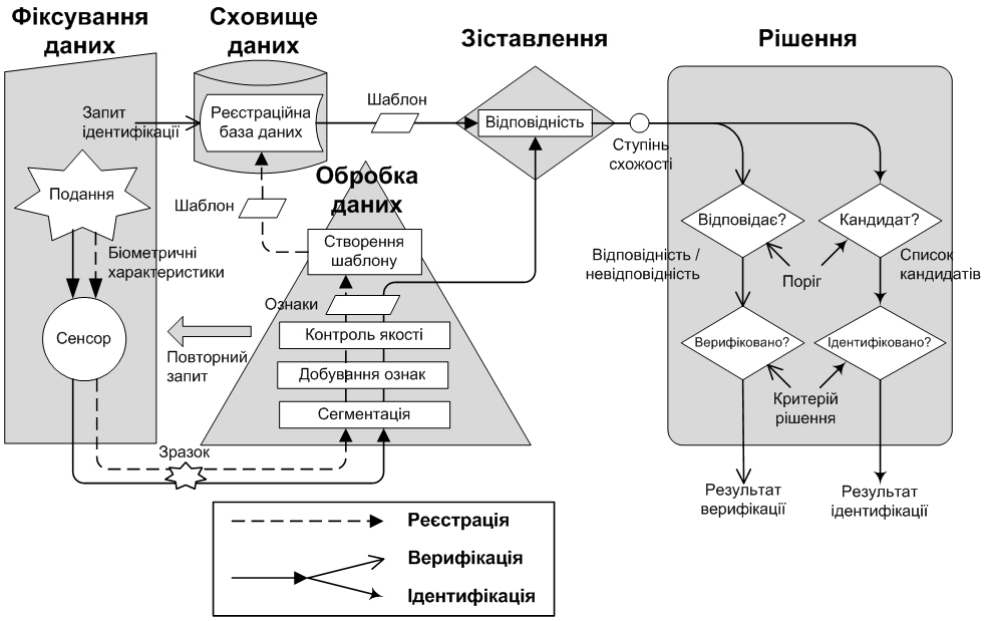

РИС. 3. Концептуальна схема узагальненої біометричної системи

Підсистема фіксації даних збирає зображення або сигнали біометричних характеристик суб'єкта, які надані біометричному сенсору, та видає це зображення або сигнал у вигляді біометричного зразка.

Підсистема передавання даних (не зображена на схемі, оскільки може бути відсутня в біометричній системі у явному вигляді) забезпечує обмін зразками, ознаками та шаблонами між різними підсистемами. Ці зразки, ознаки та шаблони можна передавати використовуючи стандартні формати обміну біометричними даними. Біометричний зразок можна ущільнити та/або зашифрувати перед передаванням та розгорнути та/або дешифрувати перед використанням. Також він може бути змінений у процесі передавання через шум у каналах передачі або через втрати в процесі ущільнення та розширення. Рекомендується використовувати криптографічні методи, що захищають аутентичність, цілісність та конфіденційність біометричних даних, що передаються та зберігаються.

Підсистема обробки сигналів виділяє відмітні ознаки з біометричного зразка. Це можливо шляхом виділення сигналу біометричних характеристик суб’єкта з отриманого зразка (сегментації), добування ознак та контролю якості, який забезпечуватиме відмітність та повторюваність добутих ознак. Якщо підсистема контролю якості відхилить отриманий зразок (зразки), керування

може бути повернуто підсистемі фіксації даних для збору додаткового зразка (зразків).

Можна визначити кілька рівнів обробки біометричних даних:

- здобуті дані: необроблені дані отримані з сенсора;
- проміжні дані: дані, оброблені після отримання з сенсора, але у формі непридатній для зіставлення – на такі дані посилаються, як на дані зображень або поведінки;
- оброблені дані: дані у формі придатній для зіставлення – на ці дані посилаються, як на дані ознак.

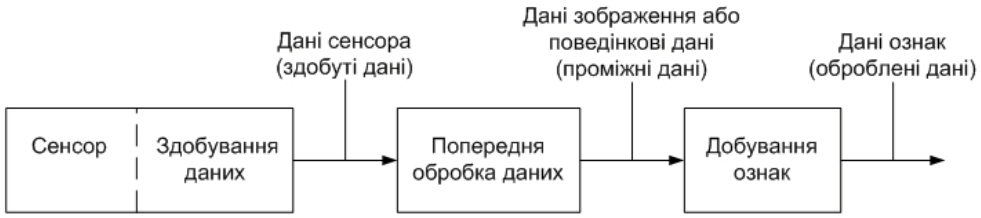

РИС. 4. Послідовність обробки біометричних даних

У випадку реєстрації, підсистема обробки сигналів створює шаблон із добутих біометричних ознак.

Підсистема зберігання даних містить реєстраційну базу, яка служить для зберігання шаблонів. Кожний шаблон пов'язаний з певною інформацією про суб’єкт реєстрації. Слід зазначити, що перед збереженням у реєстраційній базі даних, формат шаблонів може бути змінений відповідно до формату обміну біометричними даними. Шаблони можуть бути збережені в пристрої біометричної фіксації, на переносному носії (наприклад, смарт-карті), локально – на персональному комп'ютері або локальному сервері, або в централізованій базі даних.

Підсистема зіставлення даних порівнює біометричні дані з даними одного або декількох шаблонів та передає інформацію про ступінь схожості до підсистеми ухвалення рішень. Ступінь схожості визначає ступінь відповідності ознак шаблонам, з якими проводилося порівнювання. При верифікації один визначений запит суб’єкта реєстрації ініціює один розрахунок ступеня схожості. У випадку ідентифікації декілька або всі шаблони можуть бути порівняні з ознаками, вихідний ступінь схожості буде отриманий для кожного порівняння.

Підсистема ухвалення рішення використовує ступені схожості, створені однією або більше спробами, для надання вихідного рішення щодо запиту верифікації або ідентифікації.

У випадку верифікації, порівняння ознак та шаблону вважається успішним, якщо ступінь схожості перевищує встановлене граничне значення. Підтвер-

дження реєстрації суб'єкта може бути ухвалене у відповідності з правилами прийняття рішень, які можуть вимагати або допускати кілька спроб верифікації.

У випадку ідентифікації зареєстрований шаблон є потенційним кандидатом для суб'єкта, коли ступінь схожості перевищує встановлене граничне значення. Правила ухвалення рішень можуть дозволити або вимагати декількох спроб перед ухваленням рішення про ідентифікацію.

Підсистема керування (не зображена на схемі) керує у повній мірі правилами, реалізацією і використанням біометричної системи відповідно до узаконених, юрисдикційних і соціальних обмежень та вимог.

Біометрична система може взаємодіяти або не взаємодіяти із зовнішніми прикладними програмами або системами через прикладний програмний інтерфейс, апаратний інтерфейс або інтерфейс протоколів (не зображені на схемі).

Висновки. Проведений аналіз стану стандартизації в області біометрії у світі та Україні свідчить про те, що наша держава робить тільки перші кроки по впровадженню біометричних технологій аутентифікації особи при перетині державного кордону і керування доступом до таємної інформації та матеріальних цінностей на основі біометричних характеристик людини. Слід звернути увагу, що підкомітетом SC 37 "Біометрія" Технічного комітету ISO/IEC JTC 1 "Інформаційні технології" вже розроблено і введено в дію 39 стандартів в області біометрії та відповідних технологій. Жодний з цих стандартів не впроваджений в Україні. Ситуацію виправляє те, що на початок 2010 року Національним технічним комітетом підготовлено першу групу біометричних стандартів, які гармонізовано з міжнародними відповідниками.

1. *Президент* вернув у ВР закон "Про внесення змін в статтю 25 Закону України "Про правовий доступ іноземців і осіб без громадянства", 08.05.2009. – http://www.president.gov.ua/news/13724.html.
2. http://www.iso.org.
3. *Романов В., Галелюка И., Клочан П.* Биометрическая идентификация личности: современное состояние и перспективы развития в Украине // Электронные компоненты и системы. – 2010. – № 5. – С. 16 – 20.
4. *ISO/IEC* 19785-1:2006 Information technology. – Common Biometric Exchange Formats Framework – Part 1: Data element specification.

Отримано 12.04.2010