УДК 004.93'1

Коваль Л.Г.
Вінницький національний технічний університет

Злепко С.М.
Вінницький національний технічний університет

Новіцький Г.М.
Вінницький національний технічний університет

Крекотень Є.Г.
Вінницький національний технічний університет

МЕТОДИ І ТЕХНОЛОГІЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЗА РЕЗУЛЬТАТАМИ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

У статті проведено аналіз методів біометричної ідентифікації та технологій їх реалізації. Підтверджено актуальність наявної проблеми ідентифікації і аутентифікації особистості і визначено її як одну з пріоритетних. Наведено переваги, недоліки та основні характеристики біометричних ідентифікаційних технологій методів біометричної ідентифікації, що дозволило класифікувати їх.

Ключові слова: *ДНК, відбиток пальця, райдужна оболонка, біометрична ідентифікація.*

Вступ. Біометрична ідентифікація – це спосіб ідентифікації особистості за окремими специфічними біометричними ознаками (ідентифікаторами), які властиві конкретній людині.

Біометричні технології базуються на біометрії, вимірюванні унікальних характеристик окремо взятої людини. До них належать унікальні ознаки, отримані нею з народження (ДНК, відбитки пальців, райдужна оболонка ока) або характеристики, придбані згодом або ж здатні змінюватися з віком або в результаті зовнішнього впливу (почерк, голос або хода) [1].

Біометричні технології застосовуються в багатьох областях, пов'язаних із забезпеченням безпеки доступу до інформації й матеріальних об'єктів, а також у завданнях унікальної ідентифікації особистості. Застосування біометричних технологій різноманітні: доступ до робочих місць і мережних ресурсів, захист інформації, забезпечення доступу до певних ресурсів і безпека. Ведення електронного бізнесу й електронних урядових справ можливе тільки після дотримання певних процедур з ідентифікації особистості. Біометричні технології використовуються в області безпеки банківських обігів, інвестування тощо, а також роздрібній торгівлі, охороні правопорядку, питаннях охорони здоров'я, а також у сфері соціальних послуг.

За останні два десятиліття біометричні технології зробили великий крок уперед. Багато в чому цьому сприяло поширення мікропроцесорних технологій. Використання в системах контролю й управління доступом (СКУД) біометричних сканерів практично не ускладнює систему безпеки, і їх вартість для деяких біометричних методів дуже низька. Навіть більше, близько третини ноутбуків та смартфонів випускаються зараз із вбудованою системою зчитування відбитка пальців, а за наявності в ноутбуці відеокамери на ньому можна встановити систему розпізнавання людини за геометрією обличчя.

Сучасний стан. Інформація, яка міститься в кількох біометричних параметрах, може бути інтегрована за допомогою різних методів на різних рівнях і в різному контексті. Прийнято поєднувати в один клас мультимодальні та багатофакторні рішення. У мультимодальних системах ідентифікатори одного типу (наприклад, відбитки пальців) обробляються за допомогою різноманітних алгоритмів з метою підвищення надійності ідентифікації. У багатофакторних системах разом з біометричними використовуються також і інші ідентифікатори (Pin-код, пароль, смарт-карта тощо). Основною метою багатофакторних систем є прискорення процесу ідентифікації та/або надання можливості розпізнавання без звертання до централізованої бази даних ідентифікаторів. Першими роботами з мультибіометричної ідентифікації вважають експерименти 1976–1978 рр. із застосування логічних класифікаторів для іденти-

фікації за кількома біометричними характеристиками [21].

Існує безліч різних джерел інформації, які можуть бути використані для розширення можливостей біометричної системи. Сьогодні виділяють такі методи інтеграції:

– різні біометричні характеристики (зображення обличчя і відбиток пальця);

– множинні біометричні характеристики (відбитки різних пальців, райдужна оболонка лівого і правого ока);

– різні способи отримання біометричних зразків (зображення обличчя у видимому та інфрачервоному діапазоні);

– різні сканери (дві фотокамери);

– кілька зразків однієї біометричної характеристики;

– кілька алгоритмів порівняння біометричних зразків [22].

Незалежно від методу має місце сильна або слабка двостороння інтеграція інформації з різних джерел. У першому випадку вихідні сигнали від різних біометричних сенсорів можуть бути використані для створення сукупності більш точних та інформативних вхідних сигналів. У другому – зв'язок між вхідними сигналами (наприклад, обличчя і відбитку пальця) буде досить слабким або взагалі відсутнім. У цьому випадку інтеграція відбувається на рівні автономних сенсорів, і кожен пристрій незалежно від інших оцінює біометричний зразок. Властивості і шаблони, які виділені однією біометричною системою, неприйнятні для іншої, тоді як значення персональних біометричних параметрів піддаються інтеграції. У системах ідентифікації особистості інтеграція кількох біометричних характеристик відбувається або на рівні ухвалення рішення або на рівні обчислень [21].

Кількість помилок у системах біометричної ідентифікації визначається точністю, з якою внутрішній біометричний пристрій зіставлення зможе визначити, яка з гіпотез є дійсною. Вводячи біометричні зразки, можна будувати дві гіпотези: нульову та альтернативну.

Завдання визначення оптимального методу подібності можна звести до завдання оцінювання щільностей біометричних порівнянь. Але на етапі навчання мультибіометричної системи (визначення розподілів біометричних порівнянь) доступна лише досить обмежена інформація, яка використовується для оцінювання статистичних властивостей біометричних систем.

Це призводить до того, що по-перше, при використанні емпіричних частот як оцінок дійсних функцій розподілу спостерігають сильну залежність від навчальної вибірки й значну дисперсію результатів навчання.

По-друге, навіть при прийнятті певних припущень про динаміку помилок розпізнавання дисперсія прогнозу зі зменшенням рівня Коефіцієнту Невірного Допуску (КНД) росте неприйнятними темпами, що пояснюється нездатністю емпіричних щільностей до узагальнення на генеральну сукупність.

По-третє, слід враховувати, що інтеграцію технології застосовують для побудови систем ідентифікації з дуже низьким КНД, тому проблемою є верифікація результатів [22].

Для статистично залежних біометричних характеристик можна використовувати методи оцінювання щільностей розподілів, які оперують із багатомірним простором результатів порівнянь та залежно від рівня інтеграції біометричних технологій.

Найпоширенішим випадком інтеграції залежних технологій є використання кількох алгоритмів порівнянь із метою поліпшення якості розпізнавання й підвищення надійності системи ідентифікації. Отриманий комбінований алгоритм можна розглядати як нову одномодальну біометричну технологію, що усуває проблеми з верифікацією результатів завдяки тому, що навчання і випробування можна провести на доступних масивах за окремими біометричним характеристикам [11; 21].

Постановка проблеми. Недостатній рівень достовірності результатів ідентифікації зумовлений неадекватним вибором методу або комбінації методів, помилками під час формування апаратних засобів і низькою інформативністю обраних критеріїв і характеристик.

За принципом дії біометричні методи ідентифікації поділяються на статичні (за ознаками, даними людині з народження), динамічні (за ознаками, що набуті в процесі існування) та комбіновані (поєднання двох перших) [6].

Фізіологічні (статичні) методи біометричної ідентифікації:

– сканування райдужної оболонки ока;

– сканування сітківки ока;

– сканування рисунку вен долоні;

– геометрія кисті руки (відбитки пальців – дактилоскопія, розмір, довжина і ширина долонь);

– розпізнавання рис обличчя (контур, форма; розташування очей і носа);

– структура ДНК-сигнатури.

Поведінкові (динамічні) методи;

– аналіз підпису (форма букв, манера письма, натиск);

– аналіз тембру голосу;

– аналіз клавіатурного почерку тощо [4; 7].

За технологією реалізації, методи ідентифікації особистості бувають: оптоелектронні, напівпровідникові, ультразвукові, піроелектричні, електрооптичні, комбіновані, телевізійні та тепловізійні.

Найпоширенішими методами біометричної ідентифікації особистості є сканування райдужної оболонки і відбитків пальців, які разом становлять 2/3 від усього обсягу систем ідентифікації.

Більшість людей вважають, що в пам'яті комп'ютера зберігається зразок відбитка пальця, голосу людини або картинка райдужної оболонки його ока. Але в реальності в більшості сучасних систем це не так. У спеціальній базі даних зберігається цифровий код довжиною до 1 000 біт, який асоціюється з конкретною людиною, що має право доступу. Сканер або будь-який інший пристрій, який використовується в системі, зчитує певний біологічний параметр людини, потім обробляє отримане зображення або звук, перетворюючи їх на цифровий код. Саме цей ключ і порівнюється із вмістом спеціальної бази даних для ідентифікації особистості [5].

Біометрична ідентифікація за відбитками пальців. Дактилоскопія – найбільш розроблений на цей час біометричний метод ідентифікації особистості. Швидкому розвитку методу слугувало його широке використання в криміналістиці XX століття. Розпізнавання відбитка пальця базується на аналізі розподілу особливих точок (кінцевих точок і точок розгалуження папілярних ліній), розташування яких задається в декартовій системі координат [8].

Кожна людина має унікальний папілярний візерунок відбитків пальців, завдяки чому й можлива ідентифікація. Зазвичай алгоритми використовують характерні точки на відбитках пальців: закінчення лінії візерунка, розгалуження лінії, одиночні точки. Також залучається інформація про морфологічну структуру відбитка пальця: відносне положення замкнених ліній папілярного візерунка, аркових і спіральних ліній. Особливості папілярного візерунка перетворюються на унікальний код, який зберігає інформативність зображення відбитка в базі даних.

Існує два основних алгоритми порівняння отриманого коду з шаблоном із бази даних: за характерними точками і за рельєфом усієї поверхні пальця. У першому випадку виявляються характерні ділянки і запам'ятовується їхнє взаємне розташування. У другому – запам'ятовується вся «картина» в цілому. У сучасних системах використовується також комбінація обох алгоритмів, що підвищує рівень надійності системи.

Під час оцінювання надійності процедури ідентифікації за відбитками пальців постає питання про можливість їхнього копіювання й використання іншими особами для отримання несанкціонованого доступу. Одним із варіантів введення в оману терміналу фахівці називають виготовлення штучної кисті з нанесеними на неї відбитками пальців (або вилучення «оригіналу» в законного власника). Адекватним способом боротьби з такою фальсифікацією є використання інфрачервоного детектора, який дозволяє фіксувати теплове випромінювання від руки або пальця [8; 9].

Іншим способом підроблення є безпосереднє нанесення папілярного візерунка пальців закон-

Таблиця 1

Надійність та сфера застосування методів ідентифікації [11]

Метод	Носій біометричної інформації	Імовірність помилки	Надійність	Сфера застосування
Розпізнавання райдужної оболонки ока	Візерунок райдужки	1/1200000	Висока	Критичні до кількості помилок сервіси
Розпізнавання малюнка вен кисті руки	Візерунок вен	1/1100000	Висока	Критичні до кількості помилок сервіси
Дактилоскопія	Відбитки пальців	1/1000	Середня	Універсальна
Форма руки	Розмір, довжина й ширина долонь	1/700	Низька	Некритичні до кількості помилок сервіси
Розпізнавання обличчя	Контур, форма; розташування очей і носа	1/100	Низька	Некритичні до кількості помилок сервіси
Підпис	Форма букв, манера листа, натиск	1/100	Низька	Некритичні до кількості помилок сервіси
Розпізнавання голосу	Характеристики голосу	1/30	Низька	Телефонні сервери

ного користувача на руки зловмисника за допомогою спеціальних плівок. Однак у цьому випадку необхідно отримати якісні відбитки пальців законного користувача, причому саме тих пальців, які були зареєстровані системою [10].

Переваги методу:

1) висока достовірність (статистичні показники методу вищі за показники способів ідентифікації за обличчям, голосом, підписом);

2) низька вартість пристроїв, які сканують зображення відбитка пальця;

3) доволі проста процедура сканування відбитка.

Недоліки методу:

1) папілярний візерунок відбитка пальця дуже легко пошкоджується дрібними подряпинами, порізами;

2) недостатня захищеність від підроблення зображення відбитка [10; 11].

Біометрична ідентифікація за райдужною оболонкою і сітківкою ока. У 1994 р. Дж. Даугман у США запатентував метод розпізнавання особи за райдужною оболонкою ока, який використовує і дотепер.

Райдужна оболонка ока є унікальною характеристикою людини. Малюнок райдужки формується на восьмому місяці внутрішньоутробного розвитку, остаточно стабілізується у віці близько двох років і практично не змінюється протягом життя, окрім як в результаті сильних травм або складних патологій. Метод є одним з найточніших серед біометричних технологій [7; 11].

Система ідентифікації особистості за райдужною оболонкою логічно ділиться на дві частини: пристрій захоплення зображення, його первинного оброблення й передачі на обчислювач; обчислювач, який здійснює порівняння зображення із зображеннями в базі даних і передає команду про допуск виконавчому пристрою.

Розрізняють активні й пасивні системи розпізнавання. У системах першого типу користувач повинен сам налаштувати камеру, пересуваючи її для більш точного наведення. Пасивні системи є простішими у використанні, оскільки камера в них настроюється автоматично.

Варто зазначити, що райдужки правого і лівого ока за малюнком суттєво відрізняються.

Переваги методу:

1) статистична надійність;

2) захоплення зображення райдужної оболонки можна здійснювати на відстані від кількох сантиметрів до кількох метрів, при цьому фізичний контакт людини з пристроями не відбувається;

3) райдужна оболонка захищена від пошкоджень рогівкою;

4) стійка протидія підробкам.

Недоліки методу:

1) вартість системи для захоплення райдужної оболонки вища за вартість сканера відбитків пальця і камери для захоплення 2D зображення обличчя [11].

Напрям біометричної ідентифікації за сітківкою ока розвивається з 1976 р., коли у США була утворена компанія Eyedentify, яка досі зберігає монополію на виробництво комерційних систем ідентифікації за ретиною [11].

До останнього часу вважалося, що найнадійніший метод біометричної ідентифікації – це метод, що базується на скануванні сітківки ока. Він поєднує в собі кращі риси ідентифікації за райдужною оболонкою і за рисунком вен руки. Сканер зчитує малюнок капілярів на поверхні сітківки ока. Сітківка має нерухому структуру, що незмінна в часі, окрім як у результаті очної хвороби, наприклад катаракти.

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судин на задній стінці ока. Сканери сітківки ока отримали широке поширення в системах контролю доступу на особливо секретні об’єкти, тому що в них один з найнижчих відсотків відмови в доступі зареєстрованих користувачів і практично не буває помилкового дозволу доступу [7].

На жаль, низка труднощів виникає під час використання цього методу біометрії. Під час ідентифікації за сітківкою ока вимірюється кутовий розподіл кровоносних судин на поверхні сітківки щодо сліпої плями ока та інші ознаки. Капілярний малюнок сітківки очей відрізняється навіть у близнюків і може бути з великим успіхом використаний для ідентифікації особистості. Усього нараховують близько 250 ознак. Подібні біометричні термінали забезпечують високу вірогідність ідентифікації на рівні з дактилоскопією, але вимагають від особи, що перевіряється, значний час не рухатися і фіксувати погляд на об’єктиві сканера [7].

Переваги методу:

1) високий рівень статистичної надійності;

2) завдяки невеликому поширенню систем імовірність розроблення засобів їх «обману» досить низька;

3) безконтактний метод реєстрації даних.

Недоліки методу:

1) складна у користуванні система і досить довгий час оброблення;

2) висока вартість системи;

3) відсутність широкого ринку пропозиції і, як наслідок, недостатня інтенсивність розвитку методу [11].

Біометрична ідентифікація за геометрією обличчя, кисті руки та венозним рисунком долоні. Існує безліч методів розпізнавання за геометрією обличчя. Всі вони базуються на тому, що риси обличчя і форма черепа кожної людини індивідуальні.

Технічна реалізація методу – більш складна (з математичної точки зору), ніж розпізнавання відбитків пальців, що вимагає дорогої апаратури (необхідна цифрова відео- або фотокамера і плата захоплення відео-зображення). Але метод має один істотний плюс: для зберігання даних одного зразку ідентифікаційного шаблону потрібно небагато пам'яті, оскільки людське обличчя можна «розкласти» на відносно невелику кількість ділянок, незмінних у всіх людей. Наприклад, для обчислення унікального шаблону, відповідного конкретній людині, необхідно всього 12…36 характерних ділянок. Розпізнавання людини за зображенням обличчя відрізняється від інших біометричних систем тим, що, по-перше, не вимагає спец-устаткування, по-друге, відсутній фізичний контакт людини із пристроями. Не треба очікувати дотику або зупинки для спрацьовування системи.

У наш час існують чотири основних методи розпізнавання обличчя, які відрізняються складністю реалізації і метою застосування [13]:

1) "Eigenface" або «власне обличчя»;

2) аналіз «відмітних рис»;

3) «нейронна мережа»;

4) автоматичне оброблення зображення обличчя.

Технологія Eigenface використовує двовимірні зображення в градаціях сірого, які представляють характеристики зображення особи, відмінні від інших. Метод Eigenface є основою для інших методів розпізнавання обличчя. Комбінуючи характеристики 100–120 Eigenface, можна відновити велику кількість облич. В момент реєстрації Eigenface кожної конкретної людини представляється у вигляді ряду коефіцієнтів. Для режиму встановлення особистості, у якому зображення використовується для перевірки ідентичності, «живий» шаблон порівнюється із вже зареєстрованим з метою визначення коефіцієнта відмінності. Ступінь відмінності між шаблонами визначає факт ідентифікації. Технологія Eigenface оптимальна при використанні в освітлених приміщеннях, коли є можливість сканування особи у фас [13].

Аналіз рис, відмінних від інших, – ще одна із широко використовуваних технологій ідентифікації, яка подібна до технології Eigenface, але в більшому ступені адаптована до зміни зовнішності або міміки людини (усміхнене або насуплене обличчя). В зазначеній технології використовуються десятки характерних рис різних областей обличчя, причому враховується їхнє відносне місце розташування [11]. Індивідуальна комбінація цих параметрів визначає особливості кожного конкретного обличчя людини, яке є унікальним і досить динамічним.

Метод автоматичного оброблення зображення особи – найпростіша технологія, що використовує відстані та їх відношення між точками обличчя, такими як очі, кінець носа, куточки рота. Хоча даний метод і не настільки потужний, як Eigenface або «нейронна мережа», але він досить ефективний в умовах слабкого освітлення [7].

Біометрична ідентифікація за геометрією кисті руки за своєю технологічною структурою і рівнем надійності повністю аналогічна методу ідентифікації особистості за відбитком пальця. Статистична ймовірність існування двох кистей рук з однаковою геометрією надзвичайно мала [7].

Математична модель ідентифікації за даним параметром вимагає небагато інформації – усього 9 байт, що дозволяє зберігати великий обсяг записів і швидко здійснювати пошук. Пристрої ідентифікації особистості за геометрією руки знаходять широке застосування. Так, у США пристрої для зчитування відбитків долонь встановлені більш ніж на 8 000 об'єктах. Пристрій Handkey сканує як внутрішню, так і бічну сторону долоні, використовуючи для цього вбудовану відеокамеру та алгоритми стиску [7].

Ідентифікація користувачів за геометрією руки використовується в законодавчих органах, міжнародних аеропортах, лікарнях, імміграційних службах тощо. Переваги ідентифікації за геометрією долоні адекватні перевагам ідентифікації за відбитком пальця з погляду надійності, хоча пристрій для зчитування відбитків долонь займає більше місця.

Біометрична ідентифікація за малюнком вен руки – нова технологія у сфері біометрії, яка базується на інфрачервоному скануванні вен із подальшим цифровим обробленням. Дана технологія була розроблена для використання в системі охорони здоров'я, щоб допомогти лікарям знайти у пацієнтів вени для ін'єкцій. Але враховуючи те, що струк-

тура вен у кожної людини індивідуальна, ця технологія викликала інтерес фахівців з ідентифікації, як більш надійна відносно технології ідентифікації за відбитком пальця, оскільки відтворити модель кровоносної системи неможливо [7].

Малюнок вен зчитується із зовнішнього боку долоні або кисті руки за допомогою інфрачервоної камери і дозволяє отримати достатньо чітке зображення кровоносних судин, таке, що навіть відносно невеликі порізи чи бруд на поверхні шкіри не перешкоджають успішній реєстрації особи. Поглинаючи випромінювання, відновлений гемоглобін переносить кисень по венах і скорочує ступінь відбиття та відображення малюнка вени у вигляді чорного унікального візерунка. Далі отримане зображення обробляється, і залежно від розташування вен на руці формується цифрова згортка [15].

Переваги методу:

1) висока достовірність отриманих результатів;

2) відсутність необхідності прямого контакту з пристроєм, що здійснює сканування;

3) висока ступінь захищеності – рисунок неможливо отримати від людини «на вулиці», а у випадку використання муляжу кисті малюнок вен не буде зчитаний інфрачервоною камерою;

Недоліки методу:

1) недопустиме засвічення сканера сонячними променями і променями галогенних ламп;

2) вплив деяких захворювань, наприклад артриту, на прийняття рішення [7; 11]

Біометрична ідентифікація за голосом досить зручна та інформативна, але за умови, що вона здійснюється не людиною, а технічними засобами, до яких належать програмні комплекси, автоматизовані системи, комп'ютеризовані пристрої тощо.

Автомати позбавлені впливу «людського фактору». Вони розрізняють голос і здійснюють ідентифікацію об'єктивно, на основі жорстко детермінованих і заданих наперед ознак. Для підвищення якості ідентифікації за голосом в деяких системах використовують додатково верифікацію голосу, а іноді – аутентифікацію.

Технологія біометричної ідентифікації добре зарекомендувала себе в системах верифікації особистості за голосом в окремих каналах зв'язку, підтвердила більш високу надійність порівняно із частотним набором особистого номера.

В останні роки набуває все більшого розповсюдження біометрична ідентифікація за клавіатурним «почерком» користувача як таким, що за наявності високої стабільності дозволяє ідентифікувати з високим рівнем достовірності особу користувача.

При цьому застосовуються статистичні методи обробки вихідних даних і формування вихідного вектора, що є ідентифікатором даного користувача. Як вихідні дані використовують часові інтервали між натисканням клавіш на клавіатурі і часом їх утримання. При цьому інтервали між натисканням клавіш характеризують темп роботи, а час утримання клавіш характеризує стиль роботи із клавіатурою – різкий удар або плавне натискання [7].

Принципова відмінність цих двох способів полягає в тому, що у першому випадку використовується ключова фраза, яка задається користувачем у момент реєстрації його в системі (пароль), а в другому – використовуються ключові фрази, які генеруються системою щоразу в момент ідентифікації користувача [7].

Застосування способу ідентифікації за клавіатурним почерком доцільне тільки стосовно користувачів з досить тривалим досвідом роботи з комп'ютером і почерком роботи на клавіатурі, що сформувався, тобто до програмістів, секретарів тощо. Еталонні характеристики користувача, отримані на етапі навчання системи, дозволяють зробити висновки про ступінь стабільності клавіатурного почерку користувача і визначити довірчий інтервал розкиду параметрів для наступної ідентифікації користувача.

Нові методи біометричної ідентифікації. Перелік технологій, які можуть бути використані в системах безпеки, постійно розширюється, і більшість з них вважаються досить перспективними:

1) аналіз термограми обличчя в інфрачервоному діапазоні випромінювання;

2) оцінювання характеристики ДНК;

3) аналіз структури шкіри та епітелію на пальцях з використанням цифрової ультразвукової спектроскопії шкіри;

4) аналіз форми вушної раковини;

5) аналіз характеристик ходи людини;

6) аналіз індивідуальних антропометричних особливостей людини;

7) розпізнавання за рівнем солоності шкіри [20].

Технологія побудови та аналізу термограм з використанням інфрачервоних камер є одним з останніх досягнень в області біометрії, оскільки дає унікальну картину об'єктів, що знаходяться під шкірою людини. Термограма особи є суворо індивідуальною, завдяки чому можна впевнено

розрізняти навіть близнюків. З інших властивостей цього підходу можна відмітити його інваріантність стосовно будь-яких косметичних змін та прихованість процедури реєстрації.

Технологія, що побудована на аналізі характеристик ДНК (метод геномної ідентифікації), є хоча і найбільш тривалою, але й найбільш перспективною із відомих систем ідентифікації. Метод базується на тому, що в ДНК людини є поліморфні локуси (локус – положення хромосоми в гені або аллелі), які часто мають 8–10 аллелей. Визначення набору цих аллелей для декількох поліморфних локусів в конкретного індивіда дозволяє отримати геномну карту, характерну тільки для цієї людини. Точність даного методу визначається характером і кількістю проаналізованих поліморфних локусів сьогодні дозволяє досягти рівня 1 помилки на 1 млн осіб.

Технологія аналізу відбитків долонь стала розвиватися порівняно недавно, але вже має певні досягнення. Ряд компаній-розробників (наприклад у Великобританії) зосередилися на технології, що аналізує не малюнок ліній на шкірі, а обрис долоні, який також має індивідуальний характер. Аналогічна система, що працює з відбитками пальців, успішно використовується британськими поліцейськими вже 5 років. Але одних лише відбитків пальців, як стверджують криміналісти, часто виявляється недостатньо. До 20% слідів, що залишаються на місці злочину, – це відбитки долонь. Комп'ютеризація цього процесу дозволить використовувати відбитки долонь більш широко й приведе до істотного збільшення розкривання злочинів. Слід відмітити, що пристрої сканування долоні зазвичай мають високу вартість, тому оснастити ними велику кількість робочих місць не так уже й просто [7, с. 20].

Технологія аналізу форми вушної раковини є однією з найбільш останніх розробок у біометричній ідентифікації людини. За допомогою недорогої Web-камери можна отримувати досить надійні зразки для порівняння й ідентифікації. Цей спосіб поки що недостатньо вивчений, тому у науково-технічній літературі достовірна інформація про поточний стан практично відсутня.

До перспективних слід віднести системи «електронний ніс», що реалізують процес розпізнавання за запахом. Наявність генетичного впливу на запах тіла дозволяє вважати цю характеристику можливого для використання з метою біометричної ідентифікації особистості. Цій технології, як і технології аналізу форми вушної раковини, ще треба буде пройти довгий шлях розвитку, перш ніж вона стане задовольняти біометричним вимогам [11].

Висновки. Проведений аналіз літературного контенту, присвяченого методам біометричної ідентифікації та технологіям їх реалізації, підтвердив актуальність існуючої проблеми ідентифікації і аутентифікації особистості і визначив її як одну з пріоритетних, вирішення якої сприяє якісному збереженню персональних даних, забезпечує надійний доступ до об'єктів таємної інформації, наукових розробок тощо. Показано, що поєднання паролів із біометричними характеристиками людини підвищує надійність системи доступу в сотні і тисячі разів.

Наведені переваги, недоліки та основні характеристики біометричних ідентифікаційних технологій методів біометричної ідентифікації дозволили класифікувати їх на статичні (за відбитками пальців, за райдужною оболонкою ока, за геометрією обличчя або кисті руки, за венозним малюнком руки, за сітківкою ока) та динамічні (ідентифікація за голосом, за набором на клавіатурі, за підписом).

Серед нових методів біометричної ідентифікації варто зазначити про такі: за термограмою обличчя, за характеристиками ДНК, за спектроскопією шкіри, за формою вушної раковини, за ходою людини; за індивідуальними антропометричними особливостями людини, за рівнем солоності шкіри. Критичний аналіз цих методів підтвердив їхню життєздатність і перспективи розвитку.

Список літератури:

1. Голубев Г.А., Габриелян Б.А. Современное состояние и перспективы развития биометрических технологий. *Нейрокомпьютеры. Разработка. Применение.* № 10. 2004. 40 с.

2. Мороз А.О. Биометрические технологии идентификации человека. Обзор систем. *Математические машины и системы*. 2011. № 1. С. 39–45.

3. Горбань А.Н. Обучение нейронных сетей. Москва : СП ПараГраф, 1990. 156 с.

4. В. Моржаков, А. Мальцев. Современные биометрические методы идентификации. URL: http://www.polyset.ru.

5. Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности. Москва : Радиотехника, 2004. 144 с.

6. Современные биометрические методы идентификации. URL: http://www.habrahabr.ru/post/126144/.

7. Царьов Р.Ю., Лемеха Т.М. Біометричні технології: навч. посіб. [для вищих навчальних закладів]. Одеса : ОНАЗ ім. О.С. Попова, 2016. 140 с.

8. Идентификация по отпечаткам пальцев. Часть 1. / Институт экономической безопасности. Электрон. дан., ред. В. Задорожный. URL: http://www.bre.ru/security/20994.html.

9. Maltoni D. Handbook of fingerprint recognition [et al.]. N.Y. : Springer-Verlag, 2009. 494 p.

10. Кухарев Г.А. Биометрические системы: Методы и средства идентификации личности человека. Санкт-Петербург : Политехника, 2004. 204 с.

11. Обзор существующих методов биометрической идентификации. URL: http://www.sec4all.net/modules/myarticles/article.php?storyid=1265.

12. Руководство по биометрии / Р.М. Болл Джонатан, Х Коннел., Шарат Панканти и др.; пер. с англ. Н.Е. Агапова. Москва : Техносфера, 2007. 367 с.

13. Belhumeur, P. & Hespanha, J. & Kriegman, D. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1997. Vol. 19(7), P. 711–721.

14. Кухарев Г.А., Каменская Е.И, Матвеев Ю.Н., Щеголева Н.Л. Методы обработки и распознавания изображений лиц в задачах биометрии. Москва : Политехника, 2013. 416 с.

15. Тихонов И.А. Информативные параметры биометрической аутентификации пользователей информационных систем по инфракрасному изображению сосудистого русла. *Безопасность информационных технологий.* 2011. № 4. С. 61–68

16. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в современных компьютерных системах. 2-е издание. Москва : Радио и связь, 2001. 376 с.

17. Татарченко Н.В., Тимошенко С.В. Биометрическая идентификация в интегрированных системах безопасности. *Специальная техника*. 2002. № 2. 7 с.

18. Рабинер Л.Р., Шафер Р.В. Цифровая обработка речевых сигналов: пер. с англ. / под ред. М.В. Назарова, Ю.Н. Прохорова. Москва : Радио и связь, 1981. 495 с.

19. Широчин В.П., Кулик А.В., Марченко В.В. Динамическая аутентификация на основе анализа клавиатурного почерка URL: http://www.masters.donntu.edu.ua/2002/fvti/aslamov/files/bio_autentification.htm.

20. Технологии биометрической идентификации. URL: http://www.tadviser.ru/index.php.

21. Синицын И.Н., Новиков С.О., Ушмаев О.С. Развитие технологий интеграции биометрической информации. *Системы и средства информатики.* 2004. Вып. 14. С. 4–35**.**

22. Сесин Е.М., Белов В.М. Построение моделей идентификации личности, основанных на сравнении множества физических или поведенческих характеристик человека. *Вестник Сибгути.* 2011. № 4(16). 7 с**.**

23. Ворона В.А., Костенко В.О. Биометрические технологии идентификации в системах контроля и управления доступом. *Comp. nanotechnol.* 2016. Вып. 3. С. 224–241.

24. Введение в криптографию / В.В. Ященко, Н.П. Варнавский, Ю.В. Нестеренко и др.; под редакцией В.В. Ященко. Москва : МЦНМО ЧеРо. 1998. 276 с.

25. Вилле Й. Новые пути биометрии. *Журнал сетевых решений LAN*. 2005. № 1. С. 15–18

26. Безик О.В., Басараб М.А. Разработка и анализ алгоритма биометрической аутентификации по рисунку кровеносных сосудов пользователя. *Молодой ученый*. 2016. № 8. С. 116–119. URL https://www.moluch.ru/archive/112/28527/.

27. Тихонов И.А. Модели качества инфракрасных изображений сосудистого русла для целей биометрической аутентификации пользователей информационных систем. *Техническая защита информации*. 2013. № 3.

28. Биометрическая идентификация по рисунку вен ладони (mini How To). 2012. URL: https://habrahabr.ru/post/149424.

29. Огнев А.В., Типикин А.П. Центрирование отпечатков при инвариантном распознавании на основе метрики Хаусдорфа. Курск : КурскГТУ : *Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации*, 2008. С. 34–35.

30. Sherlock B., Monro D. A model for interpreting fingerprint topology. *Pattern Recognition*. 1993. Vol. 26, Number 7. P. 1047–1055.

МЕТОДЫ И ТЕХНОЛОГИИ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПО РЕЗУЛЬТАТАМ ЛИТЕРАТУРНЫХ ИСТОЧНИКОВ

В статье проведен анализ методов биометрической идентификации и технологий их реализации. Подтверждена актуальность существующей проблемы идентификации и аутентификации личности, которая определена как одна из приоритетных. Приведены преимущества, недостатки и основные характеристики биометрических идентификационных технологий методов биометрической идентификации, что позволило классифицировать их.

Ключевые слова: *ДНК, отпечаток пальца, радужная оболочка, биометрическая идентификация.*

METHODS AND TECHNOLOGIES OF BIOMETRIC IDENTIFICATION BY RESULTS OF LITERARY SOURCES

The article analyzes the methods of biometric identification and the technologies of their implementation, confirmed the relevance of the existing problem of identification and authentication of the individual and identified it as one of the priority. The advantages, disadvantages and basic characteristics of biometric identification technologies of biometric identification methods, which allowed to classify them, are presented.

Key words: *DNA, fingerprint, iris, biometric identification.*