

УДК 004.93

Г. М. Новіцький; С. М. Злепко, д. т. н., проф.; Л. Г. Коваль, к. т. н., доц.;  
І. О. Криворучко

## АНАЛІЗ ПОМИЛОК ІДЕНТИФІКАЦІЇ Й ШЛЯХИ ПІДВИЩЕННЯ ТОЧНОСТІ СИСТЕМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

*Ідентифікація та аутентифікація забезпечують якісне зберігання персональних даних, що забезпечує надійний доступ до об'єктів чи таємної інформації, наукових розробок тощо. Особливо важливим стає поєднання паролів із біометричними характеристиками людини, завдяки чому надійність системи доступу зростає в тисячі разів.*

*У статті розглянуто основні властивості й принципи біометричних ідентифікаційних систем, проаналізовано й класифіковано помилки основних методів біометричної ідентифікації: статичних методів (за відбитками пальців, за райдужною оболонкою ока, за геометрією обличчя або кисті руки, за венозним рисунком руки, за сітківкою ока) та динамічних (ідентифікація за голосом, за набором на клавіатурі, за підписом).*

*Обґрунтовано принцип отримання рисунку вен долоні, який полягає у поглинанні ІЧ випромінювання гемоглобіном крові, за якою необхідний венозний рисунок долоні визначається ступенем відбиття випромінювання та рівнем візуалізації судинного русла. Здійснено порівняльний аналіз кількох методів ідентифікації людини за рисунком вен долоні й обрано метод із найкращими характеристиками. Проведено аналіз контрольних точок венозного рисунка (мінуцій). Для оптимального зняття даних упроваджено нову методику сканування руки із використанням фіксаторів, що дозволяє до скоротити мінімуму зсув рисунка вен досліджуваної особи й полегшує його порівняння із шаблонним. Обґрунтовано вибір промислового зразка зчитувача вен – сканера, який найбільш швидко та якісно адаптується до загальної структури системи ідентифікації. Для скелетизації бінарного зображення обрано метод шаблонів, який дозволяє швидше обробити дані й отримати матрицю даних – координати мінуцій та їхній тип. Удосконалюючи функціональну модель процесу ідентифікації особистості за венозним рисунком долоні руки до структури процесу ідентифікації введено ідентифікаційний протокол, виконання якого зумовлює адекватне прийняття рішення “ідентифіковано / не ідентифіковано”.*

**Ключові слова:** біометрична ідентифікація, профілі біометричні, розпізнавання, рисунок вен, біометрична система, сканер, точність ідентифікації, біометрія.

### Вступ

Традиційні методи й засоби аутентифікації вимагають від користувача різних рівнів підготовленості, фінансових витрат, безпекових та інших заходів щодо забезпечення точної й достовірної ідентифікації особи. Найбільшу популярність сьогодні здобули: сканування відбитків пальців (використовують 57% компаній); розпізнавання обличчя (14%); геометрії руки (5%); аналіз райдужної оболонки ока (3%); розпізнавання голосу й сканування долонь – по 2%. [1]. За даними Biometrics Research Group, витрати світового ринку на методи та засоби ідентифікації у 2020 році перевищили 50 млрд. доларів [1].

На жаль, усі сучасні методи ідентифікації особи мають недолі, що й зумовлює необхідність пошуку рішень, направлених на забезпечення високої точності персоніфікованої біометричної ідентифікації.

### Аналіз літературного контенту

Методи біометричної ідентифікації мають низку недоліків: від можливості обійти алгоритм ідентифікації до повної неможливості аутентифікації за зміни відповідних частин тіла людини. Найдосконаліший сканер обличчя може не розрізнити близнюків, як і не зможе ідентифікувати людину після заміни кришталика ока або протезування його рогівки, тому використовують ідентифікацію за сітківкою або райдужною оболонкою ока [1]. Щорічно у світі фірми виробляють близько 75 млн. засобів біометричної ідентифікації, точність визначення яких лише 80% [1].

Головним завданням безпомилкової ідентифікації є мінімізація хибних невідповідностей і відповідностей. У першому випадку зчитування даних особи треба здійснювати згідно з

переліком відповідних вимог (правильне положення пальця під час дактилоскопії, обличчя особи під час ідентифікації за геометрією обличчя, положення ока під час сканування райдужної оболонки тощо). У другому випадку певна особа має дуже близькі чи подібні параметри із тією, дані якої зберігаються у базі даних, і тоді система спрацює помилково, визнавши цю особу за істинну. виправити помилку можна лише, якщо дослідити іншу біометричну характеристику цієї людини [2].

Оскільки первинним пристроєм зняття інформації для ідентифікації особи є сканер, то якість його роботи істотно впливатиме на подальшу обробку інформації. Це зумовлює необхідність оснащення систем біометричної ідентифікації більш точними сканувальними пристроями, насамперед, із високою роздільною здатністю.

У напівпровідникових сканерах зображення поверхні пальця або рисунка вен долоні отримують шляхом використання властивостей напівпровідників, що змінюються в місцях контакту гребенів папілярного візерунка (для дактилоскопії) чи гемоглобіну в кровотоці (рисунок вен) із поверхнею сканера [3].

Робота ємнісних сканерів ґрунтується на зміні ємності р-п-переходу напівпровідника під час дотику гребеня папілярного візерунка з елементом напівпровідникової матриці. Сканери недорогі й надійні, проте неефективні в боротьбі з муляжами.

Радіочастотні сканери працюють із використанням мініатюрних антен. На поверхню руки, яку сканують, спрямовують сигнал низької інтенсивності, а відбитий від поверхні сигнал приймає чутлива матриця. Однак робота сканера нестійка, що зумовлює високу вірогідність помилки під час ідентифікації.

Чутливі до контакту зі шкірою сканери використовують матрицю п'єзоелектричних елементів, чутливих до ступеня натискання. Недоліками методу є низька чутливість, неефективний захист від муляжів, можливість пошкодження у випадку надміру докладених зусиль.

Термосканери побудовані на піроелектричних елементах, які дозволяють фіксувати різницю температури. Під час сканування будують температурну карту, яку формують рівнями температури на гребенях і западинах папілярного візерунка. Система стійка до електростатичного розряду, ефективно захищена від муляжів, проте головним недоліком є швидке зникнення зображення відбитка.

Ультразвуковий метод ґрунтується на фіксації відстані між джерелом хвиль і впадинами папілярного візерунка. Зображення об'єкту якісне, захист від муляжів високий, водночас можна отримати дані про пульс людини. Головний недолік – висока вартість обладнання [3].

Як уже зазначалося раніше, для сканування малюнка вен використовують і напівпровідниковий сканер, що працює в інфрачервоному діапазоні хвиль. Це сприяє тому, що отримане зображення буде чітким і захищеним від муляжів. Єдина вимога до особи, яку ідентифікують, полягає в тому, щоб вона правильно розмістила долоню у вікні сканера.

Узагальнювальний аналіз розглянутих методів і засобів біометричної ідентифікації дозволив визначити їхні переваги й недоліки, згрупувати відповідним чином і представити у вигляді таблиці 1.

Дані таблиці 1 дають уявлення про наявність як спільних переваг і недоліків, так і властивих тільки одному методу або засобу, завдяки чому зацентровано увагу на актуальності й важливості наявної проблеми, що мотивуватиме фахівців до пошуку ефективних та адекватних шляхів її розв'язання.

Проблема полягає у складності і неоднозначності вибору високоточного методу або засобу для персоніфікованої ідентифікації особистості.

Мета статті – виявити причини недостатнього рівня безпомилкової ідентифікації й визначити шляхи їх усунення.

Основний текст статті

Одним із способів підвищення точності систем біометричної ідентифікації є інтеграція різних методів ідентифікації особи. І хоча це призводить до зростання матеріальних затрат на ідентифікацію, результат стає більш достовірним і набагато ближчим до бажаного.

На відміну від методу ідентифікації за геометрією обличчя, ідентифікація за венами долоні більш точна й надійна, й наближається за точністю до ідентифікації за райдужною оболонкою для одного ока. Стабільність отримуваних результатів ідентифікації пояснюється тим, що русла кровоносних судин не змінюються з віком, а їхня форма й розташування мало залежать від різних захворювань, наприклад, варикозу або тромбозу. Це забезпечує стабільні результати ідентифікації протягом багатьох років. На результати сканування вен практично не впливають зовнішні умови, що дозволяє використовувати метод для ідентифікації на виробництві.

Водночас для статистично залежних біометричних характеристик можна використовувати методи оцінювання щільностей розподілів, які оперують із багатомірним простором результатів порівнянь, залежно від рівня інтеграції біометричних технологій. Статистичні залежності біометричних тестів на рівні характеристик пояснюються тим, що одна біометрика містить іншу біометрику (форма й термограма обличчя, відбитки пальців і відбиток долоні), або парний орган (рисунок вен правої та лівої долонь, райдужні оболонки очей). За наявності залежності на рівні зразків біометричної характеристики якість розпізнавання можна покращити збільшенням числа зразків, узятих під час навчання, тому що при цьому компенсується вплив чинників, які спотворюють результат.

Таблиця 1

**Переваги й недоліки біометричних методів ідентифікації**

Метод	Переваги	Недоліки
2D-розпізнавання	<ol style="list-style-type: none"> <li>1) під час 2D-розпізнавання, на відміну від більшості біометричних методів, не потрібно коштовне обладнання;</li> <li>2) можливість розпізнавання на значних відстанях від камери.</li> </ol>	<ol style="list-style-type: none"> <li>1) вимоги до освітлення (наприклад, не вдається реєструвати обличчя людей, які входять з вулиці, у сонячний день);</li> <li>2) для багатьох алгоритмів неприйнятність якихось зовнішніх завад, наприклад, окуляри, борода, деякі елементи зачіски;</li> <li>3) обов'язкове фронтальне зображення обличчя з незначними відхиленнями;</li> <li>4) багато алгоритмів не враховують можливі зміни міміки обличчя, тобто вираз повинен бути нейтральним [4].</li> </ol>
За відбитками пальців	<ol style="list-style-type: none"> <li>1) висока достовірність (статистичні показники методу вищі за показники способів ідентифікації за обличчям, голосом, підписом);</li> <li>2) низька вартість пристроїв, які сканують зображення відбитка пальця;</li> <li>3) доволі проста процедура сканування відбитка.</li> </ol>	<ol style="list-style-type: none"> <li>1) папілярний візерунок відбитка пальця дуже легко пошкодити дрібними подряпинами, порізами;</li> <li>2) недостатня захищеність від підробки зображення відбитка, зумовлена широким поширенням методу [5; 6].</li> </ol>
3D-розпізнавання	<ol style="list-style-type: none"> <li>1) відсутність необхідності контактувати із пристроєм, що здійснює сканування;</li> <li>2) низька чутливість до зовнішніх факторів як на самій людині, так і в її оточенні (освітленість, поворот голови);</li> <li>3) високий рівень надійності, який можна порівняти з методом ідентифікації за відбитками пальців.</li> </ol>	<ol style="list-style-type: none"> <li>1) дороге обладнання;</li> <li>2) зміна міміки обличчя й завади на обличчі погіршують надійність методу;</li> <li>3) метод ще недостатньо розроблений, особливо порівняно з дактилоскопією, що утруднює його широке застосування [6; 7].</li> </ol>

За райдужною оболонкою	1) захоплення зображення райдужної оболонки можна здійснювати на відстані від кількох сантиметрів до кількох метрів, під час цього фізичний контакт людини з пристроями не відбувається; 2) райдужна оболонка захищена від пошкоджень рогівкою; 3) стійка протидія підробкам.	1) вартість системи для захоплення райдужної оболонки вища за вартість сканера відбитків пальця і камери для захоплення 2D-зображення обличчя. [11]
За сітківкою ока	1) високий рівень статистичної надійності; 2) через низьке поширення систем низька ймовірність розробки способу їх “обману”; 3) безконтактний метод зняття даних.	1) складна в користуванні система з тривалим часом обробки; 2) висока вартість системи; 3) відсутність великої кількості пропозицій і, як наслідок, недостатня інтенсивність розвитку методу [6].
За рисунком вен долоні	1) унікальність рисунка вен у кожної людини, який на долоні не змінюється з дворічного віку; 2) відсутність необхідності контактувати із пристроєм, що здійснює сканування, унаслідок чого питання гігієни вважають вичерпані; 3) високий ступінь захищеності: характеристику неможливо отримати від людини “на вулиці”, у випадку муляжу кисті рисунок вен не буде знятий інфрачервоною камерою; 4) можливість широкого використання за рахунок мінімізації впливу зовнішніх факторів; 5) простота: інтерфейс користувача сприяє максимальній простоті сприйняття; 6) висока вірогідність: статистичні показники методу можна порівняти із показами сканування райдужної оболонки.	1) недопустиме засвічення сканера сонячними променями й променями галогенних ламп; 2) деякі вікові захворювання, наприклад, артрит, сильно погіршують помилкове схвалення й помилкову відмову [4; 6].

Для побудови моделі венозного рисунка долоні руки, яка враховує координати контрольних точок, їх взаємне розміщення й кути сформуємо,  $N$ -множину біометричних зразків та  $H$ -кінцеву множину рішень, для якої можливі два варіанти ідентифікації

$$H = \{-1; +1\},$$

де  $\{-1\}$  – біометричний зразок визначають як «чужий», а  $\{+1\}$  – як «свій». Результатом ідентифікації є відображення  $h * N - H$ , отримане в результаті роботи системи

$$h(n) = \text{sign}[f(n, w) - w_0],$$

де  $h(n) \in H$  – рішення щодо ідентифікації системи;  $n \in N$  – вхідний біометричний зразок;  $f(n, w)$  – дискримінанта функція;  $w$  – вектор параметрів;  $w_0$  – поріг відсічення [8].

Кожна окрема мінучія векторного рисунка, як правило, описана її координатами, кутами й напрямками

$$M_i = (x_i, y_i, \alpha_i, \theta_i),$$

де  $x_i, y_i$  – координати мінучії;  $\alpha$  – напрям мінучії;  $\theta$  – тип мінучії (поле в бітах): роз'єднання – «0», закінчення – «-1», вигин – «-2».

Тоді модель рисунку вен долоні руки може бути представлена

$$M = \{(x_i, y_i, \alpha_i, \theta_i), \dots, (x_k, y_k, \alpha_k, \theta_k)\}, i=1, k.$$

Більш зручною формою опису мінучії є представлення її координат, кутів і типів у вигляді матриці  $M$  за аналогією з [9]

$$M = \begin{pmatrix} x_1 & y_1 & \alpha_1 & \theta_1 \\ x_2 & y_2 & \alpha_2 & \theta_2 \\ \dots & \dots & \dots & \dots \\ x_k & y_k & \alpha_k & \theta_k \end{pmatrix},$$

де  $x_i, y_i$  – координати мінучії відносно початку системи координат – центру сілуєтного зображення кисті руки;  $\alpha_i$  – напрям можливого продовження судин у точки «закінчення» й напрям «змикання» – у точки роздвоєння;  $\theta_i$  – тип контрольної точки.

У реальних умовах під час зчитування біометричного зразка (венозного рисунка долоні руки) для усунення можливих неоднозначностей і помилок, зумовлених зміненням або поворотом зображення венозного рисунка в зареєстрованому шаблоні відносно контрольного, використовують процедуру перетворення абсолютних значень параметрів мінучій у відносні за такими формулами [9]

$$\begin{cases} d_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \\ \alpha - 1_{ij} = \alpha_j - \alpha_i \\ \alpha - 2_{ij} = \alpha_j - \alpha_i \\ \alpha - 3_{ij} = \alpha_j - (\alpha_i + \alpha_j) \end{cases},$$

де  $i, j$  – мінучії;  $d_{ij}$  – відстань між точками  $i$  та  $j$ ;  $\alpha - 1_{ij}$  – кут між напрямом точки  $i$  та напрямом на точку  $j$ ;  $\alpha - 2_{ij}$  – кут роздвоєння між напрямом точки  $i$  та напрямом точки  $j$ ;  $\alpha - 3_{ij}$  – кут збігу напрямів точки  $i$  та напрямом точки  $j$  у дугу;

Автори розробили систему, у якій використано сканер рисунка вен BioSmart PV-WM з такими параметрами й функціями: тип сканера – оптичний, інфрачервоний; наявність вбудованого зчитувача RFID-міток – так; інтерфейс зв'язку з контролером - Ethernet (IEEE 802.3, 100BASE-TX); максимальна довжина кабелю Ethernet – 100м; підтримка PoE - IEEE 802.3af class 3; живлення – 12В, DC, 400mA; розміри 185x160x134 мм; маса нетто 532 г.; вартість – 18240 грн.

Наявними аналогами було обрано: 1. Біометричний мережевий термінал за відбитком пальців ZKTECO MA300 з такими основними параметрами й функціями: пам'ять відбитків пальців – 1500; пам'ять безконтактних карт – 10000; кількість записів – 50000; порт Wiegand: вхід і вихід; інтерфейс – RS485, TCP/IP, USB – host; сенсор – ZK оптичний; версія алгоритму ZK Finger v10.0; інтерфейси контролю доступу – електронний замок, геркон, кнопка «Вихід», сирена; функції контролю доступу – 50 часових зон, 5 груп доступу, 10 комбінацій розблокування; живлення 12В, DC, 500mA; розміри 73x148x34,5мм; вартість – 5145грн (без комп'ютера).

2. Біометричний термінал контролю доступу з розпізнаванням райдужної оболонки ока ANVIZ ULtraMath S2000 з такими основними параметрами та функціями: модель Iris 2000 на два ока; процесор ARM cortex; операційна система WinCE/Linux; відстань сканування – 180-240см; час сканування – 1сек.; кількість користувачів – 1000; кількість подій у пам'яті пристрою – 100000; FAR<1/1 000 000 000 000; Стандарти безпеки для здоров'я ока – ISO/IEC 19794-6(2005&2011) / IEC62471: 22006-07; мережевий інтерфейс – TCP/IP; живлення 12В, DC, 2A; розміри - 180 x 141 x 70; вимоги до навколишнього середовища – не допускається попадання прямих сонячних променів; вартість – 61434грн.

В експерименті взяли участь 160 осіб (80 чоловіків і 80 жінок), із них з абсолютно непошкодженими долонями 152 особи; із долонями, що мали зміни, зумовлені хворобою – 8 осіб (5 чоловіків і 3 жінки). У процесі експерименту спроба зареєструвати венозний рисунок долоні за наявності сонячної засвітки була змодельована для 10 осіб з неушкодженими долонями (5 чоловіків і 5 жінок), а за наявності засвітки від галогенних ламп освітлення – для 12 – осіб, також із неушкодженими долонями.

Узагальнена схема експерименту показана на рис 1: БД1 – база даних контрольних шаблонів; БД2 – база даних осіб, яким відмовлено в дозволі на доступ; БД3 – база даних зареєстрованих (поточних) шаблонів.

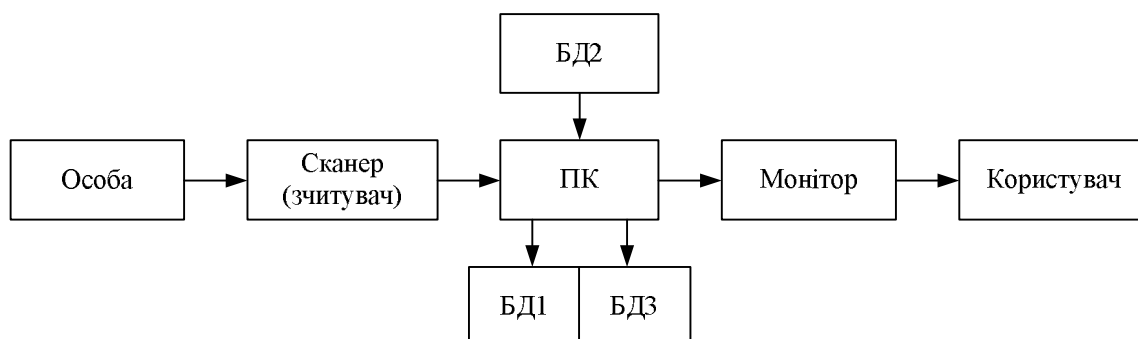


Рис. 1. Схема експерименту з оцінювання якості ідентифікації особистості

Послідовність проведення експерименту.

1. Формують бази даних контрольних шаблонів БД1-1, БД2-2, БД3-3 для кожного із трьох наявних ідентифікаторів.

2. Формують бази даних БД2-1, БД2-2, БД2-3 осіб, яким відмовлено в дозволі на доступ, знову ж таки для кожного з трьох наявних ідентифікаторів.

3. Через 30 днів після пп.1 і 2 була проведена процедура ідентифікації 160 осіб окремо для кожного із трьох наявних ідентифікаторів: 1 – зчитувач BioSmart PV-WM – для рисунка вен долоні руки; 2 – терміналу ZKTECO MA300 – для відбитків пальців; 3 – терміналу ANVIZ ULtraMath S2000 – для розпізнавання райдужної оболонки ока. Апаратний складник системи є однаковим для всіх трьох варіантів ідентифікації. У цій частині експерименту розроблена біометрична система ідентифікації особи представлена в повній конфігурації, тобто з удосконаленою підсистемою захоплення даних, до складу якої додатково ввійшли термографічна інфрачервона камера HY-18 MLX90640 в комплектації з інфрачервоним давачем температури; давач тремору на основі веб-камери iSlim32IR (потребує наявності на ПК операційної системи Windows XP\Vista) і точковий нагрівач долоні власного виробництва.

4. Проводять заміну вдосконаленої підсистеми захоплення даних на звичайну, стандартну, після чого знову здійснюють процедуру ідентифікації для 160 осіб.

Отримані в результаті експерименту дані систематизують, за необхідності додатково обробляють і групують у відповідні таблиці.

Таблиця 2

### Розподіл ідентифікованих осіб за типами сканера

Тип сканера (зчитувача)	Кількість осіб до ідентифікації		Ідентифіковано осіб		Не ідентифіковано осіб
	Без будь-яких пошкоджень	Зі змінами, зумовленими хворобою (в анамнезі)	Без будь-яких пошкоджень	Зі змінами, зумовленими хворобою	
BioSmart PV-WM (удосконалена система)	152	8	152	4	4
ioSmart PV-WM (стандартна система)	152	8	151	2	7
KTECO MA300 (аналог)	152	8	151	1	8
NVIZ ULtraMath S2000 (аналог)	152	8	150	3	7

Таблиця 3

**Порівняльна таблиця біометричних систем за базовими критеріями**

Емпіричні характеристики	Стійкість до підробки	Стійкість до впливу зовнішнього середовища	Комфортність користування	Швидкість роботи	Стабільність біометричної ознаки в часі	Критерій вартість/якість
Венозний рисунок долоні рук (удосконалений)	12	10	10	9 – 10	10	10
Венозний рисунок долоні рук (стандартний)	10	10	9 – 10	8 – 9	10	9 – 10
Папілярний рисунок пальця (аналог)	6	9	8 – 9	9 – 10	9	9
Райдужна оболонка ока (аналог)	10	9	7 – 8	8 – 9	10	9 – 10

Оцінювання проводили за 10-тибальною шкалою.

Проведений аналіз показав, що розроблена система біометричної ідентифікації за венозним рисунком долоні має показники, не нижчі за наведені для аналогів, а за деякими з показників, перевищує наявні аналоги.

Водночас аналіз ідентифікації в таблицях 2 і 3 виявив і підтвердив наявність проблеми забезпечення достовірності біометричної ідентифікації особистості. Тут має сенс навести інформацію, опубліковану в [9] й представлену дослівно: «Почати варто з того, що сам по собі папілярний рисунок шкіри пальців і долоней вважають унікальним і незмінним протягом всього життя людини, хоча строгого наукового обґрунтування й підтвердження наведена гіпотеза, незважаючи на її широке практичне використання, як не дивно, досі ще не має. Більше того, ніхто й ніколи не проводив серйозного оцінювання достовірності ідентифікації особистості за відбитками пальців, а тим більше долоней рук. За замовчуванням цю гіпотезу приймають за 100%, однак є підтвержені дані науковців, що фактично вона – не перевищує 98%»

Одним із перспективних напрямів зниження помилковості й підвищення точності й достовірності методів і засобів біометричної ідентифікації є технологія SABI (система ефективною біометричної ідентифікації) [1].

В основу технології покладено ефект, сутність якого полягає в тому, що комбіноване випромінювання в деяких діапазонах НВЧ і КВЧ може аномально глибоко просякати в тканини організму. Це дозволяє отримати за результатами аналізу відбитих від об'єкта сигналів унікальний електромагнітний профіль біооб'єкта, у якому міститься відбиток електрофізіологічних, клітинних і молекулярних процесів у певних тканинах [1].



## Висновки

1. Отже, проаналізувавши наявні методи біометричної ідентифікації та технологію їх реалізації, можна підсумувати таке.

Проблема ідентифікації та аутентифікації особи разом з актуальністю є одним із головних завдань, розв'язання яких сприяє якісному збереженню персональних даних, забезпечує надійний доступ до об'єктів чи таємної інформації, наукових розробок тощо. Особливо важливим стає поєднання паролів із біометричними характеристиками людини, завдяки чому надійність системи доступу зростає в тисячі разів.

2. Розглянуто основні властивості й принципи біометричних ідентифікаційних систем, проаналізовано й класифіковано помилки основних методів біометричної ідентифікації: статичних методів (за відбитками пальців, за райдужною оболонкою ока, за геометрією обличчя або кисті руки, за венозним рисунком руки, за сітківкою ока) та динамічних (ідентифікація за голосом, за набором на клавіатурі, за підписом).

3. Запропоновано застосовувати інтеграцію біометричних технологій за принципами комбінування інформації й технології SAbi в якості базових напрямів розв'язання проблеми підвищення точності персоніфікованої біометричної ідентифікації особистості.

## СПИСОК ЛІТЕРАТУРИ

1. SAbi – биометрическая идентификация нового поколения [Електронний ресурс] / Режим доступу : <https://hacker.ru/2018/10/10/sabi>.
2. Ворона В. А. Биометрические технологии идентификации в системах контроля и управления доступом / В. А. Ворона, В. О. Костенко // Computational nanotechnology. – 2016. – Выпуск 3. – С. 224 – 241.
3. Руководство по биометрии / [Р. М. Болл, Дж. Х. Коннел., Ш. Панканти и др.] ; пер. с англ. Н. Е. Агапова. – М. : Техносфера, 2007. – 367 с.
4. Царьов Р. Ю. Біометричні технології: навч. посіб. [для вищих навчальних закладів] / Р. Ю. Царьов, Т. М. Лемеха. – Одеса : ОНАЗ ім. О. С. Попова, 2016. – 140 с.
5. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека / Г. А. Кухарев. – СПб : Политехника, 2004 – 204 с.
6. Обзор существующих методов биометрической идентификации [Електронний ресурс] / Режим доступу : <http://sec4all.net/modules/myarticles/article.php?storyid=1265>.
7. Методы обработки и распознавания изображений лиц в задачах биометрии / [Кухарев Г. А., Каменская Е. И, Матвеев Ю. Н., Щеголева Н. Л.]. – М. : Политехника, 2013. – 416 с.
8. Логистическая регрессия и ROC-анализ – математический аппарат //Basc. Group Labs. Технологии анализа данных [Електронний ресурс] / Режим доступу : <https://loginom.ru/blog/logistic-regression-roc-auc>
9. Маркелов К. С. Идентификация и верификация личности – комплексная биометрическая информационная технология / К. С. Маркелов // International Journal of Open information Technologies. – 2015. – Vol. 3, № 5. – С. 12 – 18.

Стаття надійшла до редакції 04.03.2020 р.

Стаття пройшла рецензування 13.03.2020 р.

**Новіцький Геннадій Михайлович** – аспірант кафедри біомедичної інженерії.

**Зленко Сергій Макарович** – д. т. н., професор, завідувач кафедри біомедичної інженерії.

**Коваль Леонід Григорович** – к. т. н., доцент кафедри біомедичної інженерії.

*Криворучко Іван Олександрович* – аспірант кафедри біомедичної інженерії.  
Вінницький національний технічний університет.