УДК 004.056.52

Ших Н. В., к.пед.н., доцент, Шаклеіна І. О., к.ф.-м.н., доцент
(Дрогобицький державний педагогічний університет імені Івана Франка, м. Дрогобич)

АНАЛІЗ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА В СИСТЕМАХ З КЕРОВАНИМ ДОСТУПОМ

В умовах сьогодення біометричні технології активно застосовуються в системах пов'язаних із забезпеченням керованого доступу до інформації та матеріальних об'єктів на основі унікальної ідентифікації особи. З огляду на це виникає потреба аналізу методів та технологій біометричної ідентифікації з метою їх оптимального практичного впровадження. В статті розглянуто та проаналізовано основні методи біометрично ідентифікації користувача; розглянуто основні характеристики систем та їх вплив на ефективність роботи системи; визначено особливості використання біометричних систем для захисту і контролю виробничих об'єктів.
***Ключові слова*: біометрична система, ідентифікація, характеристики біометричних систем.**

Вступ. Інтеграція України в європейський та світовий простір потребує інноваційних підходів до організації захисту інформації в системах з керованим доступом. Поряд з правовими [1] та криптографічними методами захисту все більшої важливості набувають інженерно-технічні методи. Перспективним напрямком забезпечення захисту інформації є використання методів біометричної ідентифікації користувача, які включають в себе автоматичні або автоматизовані методи ідентифікації особи за її біологічними чи поведінковими ознаками [3].

В широкому значенні біометрія є сукупністю математичних методів, які застосовуються до біологічних організмів з метою отримання результатів спостережень, і статистичної обробки цих результатів. В контексті сучасних інформаційних технологій захисту інформації біометрика [2, С. 6] має наступне трактування – це прикладна галузь знань, яка використовує при створенні автоматизованих систем розмежування доступу унікальні ознаки людини – біометричні характеристики.

Під біометричними технологіями розуміють автоматичні або ав-

томатизовані методи ідентифікації особи за її біологічними чи поведінковими ознаками [2].

о-

би. Біометричні технології активно застосовуються в системах пов'язаних із забезпеченням керованого доступу до інформації та матеріальних об'єктів шляхом розмежування прав, а також в задачах унікальної ідентифікації особи, з метою:

- контролю доступу;
- захисту інформації;
- ідентифікації клієнтів.

Результати аналізу розподілу біометричних систем за сферами використання представлено на рис. 1:

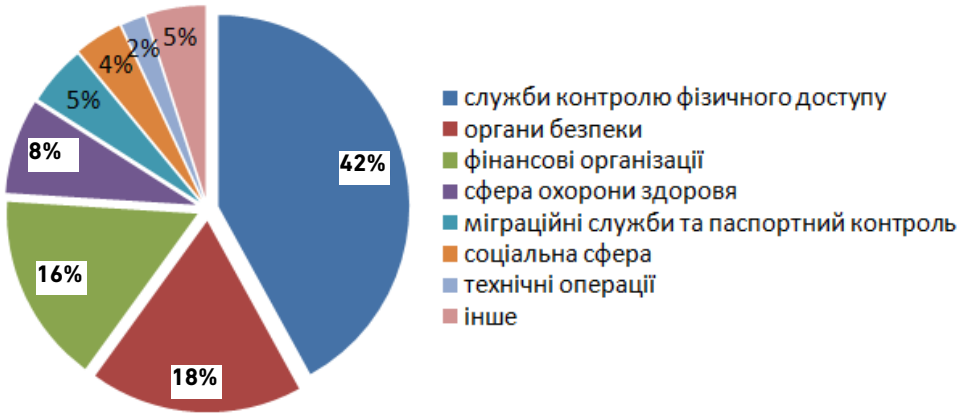

Рис. 1. Розподіл біометричних систем за сферами використання

Найбільша частка систем біометричної ідентифікації припадає на виробничу сферу, зокрема, служби контролю фізичного доступу до об'єктів. На основі аналізу предметної області було визначено основні напрямки використання біометричних систем на виробництві (табл. 1):

Таблиця 1

Використання біометричних систем на виробництві

Вид біометричної системи	Потенційні переваги за рахунок біометрики	Необхідні прилади
Системи контролю і управління доступом на територію, що охороняється	Підвищення рівня безпеки та зручності отримання допуску	Біометричні термінали; автономні замки зі сканерами відбитків пальця

продовження табл.1

Системи обходу периметра для ідентифікації працівників служби охорони	Підвищення дисципліни при обході периметра згідно визначеного маршруту в заданий час	Біометричні термінали
Системи обліку робочого часу для підтвердження персоналом часу знаходження на робочому місці	Підвищення надійності даних обліку робочого часу на виробництві; підвищення дисципліни	Біометричні термінали; біометричний сканер; автономні системи обліку робочого часу
Індивідуальні сейфи для отриманням допуску за біометричними характеристиками	Підвищення безпеки і зручності користування сейфом на підприємствах стратегічного значення	Автономний біометричний замок, вбудований в сейф
Системи відеоспостереження з функцією розпізнавання за базою даних	Зниження загрози заворушень та терористичних актів на підприємствах стратегічного значення	Програмні модулі розпізнавання осіб в даних відеопотоку
Інформаційні термінали для видачі захищеної інформації	Підвищення захисту інформації і зручності отримання доступу	Вбудовані сканери

Основними перевагами систем з біометричним контролем доступу є простота використання, значна швидкодія і зручність для користувача, оскільки вирішується ряд проблем, пов'язаних із «людським фактором», таких як втрата засобів персоналізованого доступу, необхідність збереження паролів та кодів ідентифікації тощо. А унікальність біометричних характеристик людини практично унеможливлює їх використання зловмисниками.

Недоліками систем з біометричним контролем доступу є ймовірність виникнення помилок розпізнавання, необхідність використання спеціалізованого обладнання, проблема обслуговування та супроводу і, як наслідок, доволі висока вартість.

Функціонування системи біометричної аутентифікації. В основі роботи систем з керованим доступом на основі використання біомет-

ричних характеристик мають місце два механізми: верифікація та ідентифікація. Верифікація, як порівняння «один до одного», є засобом підтвердження конкретної особи на основі визначення ступеня схожості заявлених для неї характеристик.

Ідентифікація передбачає порівняння типу «один до багатьох». В даному випадку показники відповідної біометричної характеристики співставляються з усіма наявними в базі даних зразками, а в якості результату беруться ті дані, для яких ступінь схожості є найвищим (при цьому він не є нижчим від деякого визначеного граничного порогу).

Незалежно від використовуваного механізму і опрацьовуваних біометричних характеристик у системах керування доступом відбуваються наступні процеси: реєстрація і автентифікація (рис. 2).

Дані надходять у систему із біометричних датчиків і проходять первинну обробку й оцифровування. Після цього на етапі реєстрації за допомогою вейвлет-перетворень створюється шаблон або вектор ознак, який записується у базу даних шаблонів. На етапі автентифікації формується вектор ознак отриманого зразка, який порівнюється з одним чи усіма шаблонами, наявними у базі даних, обчислюється міра подібності (відповідності шаблону) і, на основі аналізу результатів порівняння цієї міри з деяким граничним значенням розпізнавання, ухвалюється рішення про надання чи заборону доступу до деякого об'єкта.

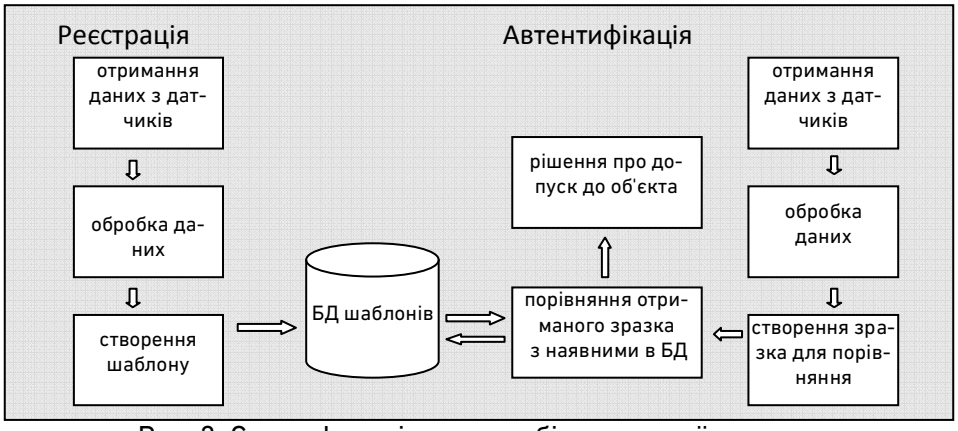

Рис. 2. Схема функціонування біометричної системи

Математичні характеристики біометричних систем. Для математичного опису процесу автентифікації може використовуватись відстань Евкліда, через яку виражається міра відмінностей між двома векторами ознак [4]:

$$D = \sqrt{\sum_{k=1}^{m} (FV_{i,k} - FV_{j,k})^2}\ , \qquad (1)$$

де $FV_{i,k}$ і $FV_{i,k}$ – вектори ознак деякої довжини m. Якщо значення відстані Евкліда рівне нулю чи наближене до 0, то обидва вектори ознак належать одній особі. Відповідність векторів ознак, а, отже, відповідність зразка еталону визначається на основі обраного значення граничного порогу R (допуск має бути надано за умови, що $D \le R$).

Особливістю біометричної ідентифікації є те, що вона являє собою статистичний процес. Вплив певних умов, таких як зашумленість, освітленість, зміна фізичного стану особи, є причинами того, що не може бути досягнута стовідсоткова точність розпізнавання. В той час як в системах, які базуються на точних методах (доступ по паролю, за скетч-картою тощо), тільки 100% відповідність є запорукою надання допуску. В біометричних системах межа між допуском і не допуском не є чітко вираженою, оскільки співпадіння зразка з еталоном ніколи не є 100%.

З огляду на це важливим завданням є вибір значення граничного порогу, оскільки в разі неправильного його завдання в системі можуть виникати помилки хибного допуску або хибної відмови, які знижують ефективність біометричної ідентифікації. Тому математичний апарат, який визначає ефективність біометричної системи керування доступом, ґрунтується на оцінці двох ймовірнісних характеристик (параметрів): *FAR* (False Accept Rate), що відповідає помилкам хибного допуску, і *FRR* (False Reject Rate), що відповідає помилкам хибної відмови.

Помилка хибної відмови виникає, коли система не змогла ідентифікувати біометричний зразок, хоча відповідний шаблон наявний у базі шаблонів, тобто користувач, дані якого зареєстровані у системі, не отримав допуску. Відповідна величина *FRR* обчислюється за формулою

$$FRR = \frac{кількість\ помилок\ недопуску\ особи}{загальна\ кількість\ правильних\ розпізнавань}. \qquad (2)$$

Помилка хибного допуску, яка виникає у випадку, коли біометричний зразок було ідентифіковано невірно, тобто йому було поставлено у відповідність не той шаблон, визначається згідно співвідношення

$$FAR = \frac{кількість\ помилок\ допуску\ особи}{загальна\ кількість\ неправильних\ розпізнавань}. \qquad (3)$$

З точки зору безпеки, така помилка є більш суттєвою, ніж помилка хибної відмови, яка впливає лише на зручність користування системою.

В комерційних реалізаціях систем з біометричною ідентифікацією, гранично допустиме значення *FAR* коливається в межах 10^{-3} до 10^{-6}, а системах із великою кількістю користувачів і високим ступенем захищеності – до 10^{-9}. Водночас значення FRR може коливатись у межах 0,025-0,01, а для систем з великою кількістю користувачів цей показник не повинен перевищувати 0,001-0,0001 [3].

FAR і *FRR* пов'язані між собою обернено-пропорційною залежністю. Як приклад наведемо статистичні дані VeriFinger SDK, отримані за допомогою сканера відбитків пальців DP U.are.U. [3]:

Таблиця 2

Зв'язок між FAR і FRR

FAR,%	FRR,%
0,10	0,30
0,01	0,40
0,001	0,60
0,0001	0,90

Розглянемо особливості розрахунку та практичної значимості основних характеристик біометричних систем. Розподіли допусків і відмов в системах представляються кривими Гауса. Зміщуючи порогове значення вздовж *OX*, можемо відслідковувати його вплив на ефективність роботи біометричної системи [4].

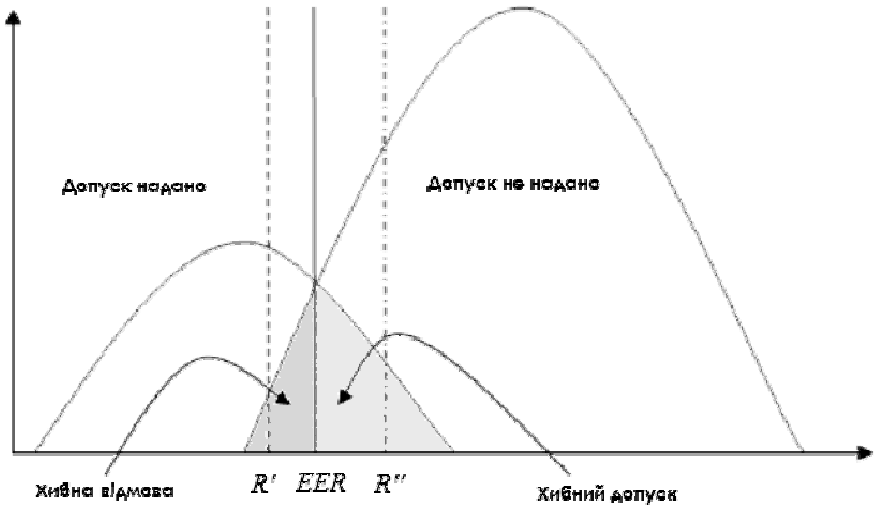

Рис. 3. Взаємозалежність показників FAR та FRR

Як видно з рис. 3, зменшення значення граничного порогу (*R'*)

призводить до того, що особа, яка раніше отримувала допуск, отримує відмову у доступі при тому, що її шаблон зареєстрований у базі – показник *FRR* збільшується. Відповідно збільшення значення граничного порогу (*R''*) сприяє зменшенню кількості помилок хибної відмови *FRR*, але збільшує ймовірність помилок несанкціонованого допуску.

Точка перетину кривих *EER* (Equal Error Rates) визначає якість того чи іншого біометричного методу (чи пристрою) і називається коефіцієнтом рівної ймовірності помилок. Точність системи аутентифікації *T* визначається за формулою [4]

$$T(\%)=(100 - (FAR(\%)+FRR(\%)/2)). \quad (4)$$

Інтерес також становлять додаткові показники: *FER* (Failture to Entroll Rate) – виражає ймовірність того, що система не зможе зареєструвати особу, і *ATV* (Ability To Verify) – ймовірність успішної перевірки особи, що обчислюється за формулою [2]

$$ATV(\%)= (1 - FAR)*(1 - FRR)*100\%. \quad (5)$$

Важливою характеристикою, що визначає власне вибір типу системи, є її пропускна здатність. Під пропускною здатністю будемо розуміти таку чисельність осіб, що потребують автентифікації, за якої робота системи із заданим показником *FAR* буде стабільною протягом деякого проміжку часу.

Нехай через біометричну систему протягом доби проходять *N* осіб. Якщо вважати допустимою одну помилку системи протягом доби, то пропускну здатність можна обчислити за формулою [2]:

$$N \approx \sqrt{\frac{1}{FAR}}. \quad (6)$$

Очевидно, що оптимізація біометричної системи передбачає зменшення як *FAR*, так і *FRR*. Є кілька основних чинників, які впливають на зазначені характеристики систем біометричної ідентифікації [4] (табл. 3).

Таблиця 3

Оптимізація FAR і FRR

Чинники	Оптимізація	
	Вплив на FAR	Вплив на FRR
Вибір біометричної функції чи біометричної характеристики	Унікальність біометрики	Сталість і вимірюваність
Якість датчиків (сенсорів)		Висока якість отриманого зображення зменшує FRR

продовження табл. 3

Поведінка користувача	Знижує FAR	Знижує FRR
Зменшення граничного порогу розпізнавання	Знижує FAR	Збільшує FRR

Показники ефективності різних типів біометричних систем. Для біометричної ідентифікації використовуються два типи біометричних характеристик: статичні (пов'язані з фізичними чи фізіологічними параметрами) і динамічні (пов'язані із особливостями виконання певних дій чи з біоритмами людського організму).

У системах керування доступом, що працюють із статичними біологічними характеристиками, ідентифікація може здійснюватися:

1) за відбитками пальців (капілярним рисунком шкіри);
2) за геометрією обличчя (2D і 3D моделі, термограма);
3) за геометрією руки (параметрами долоні, рисунком вен, формою долоні);
4) за райдужною оболонкою та/або сітківкою ока;
5) за формою вушної раковини;
6) за рентгенограмою зубів;
7) за антропометричними показниками;
8) за хімічним складом ДНК.

До динамічних біометричних характеристик, придатних до використання в системах керування доступом належать:

1) голос (спектральний склад, окремі частоти);
2) почерк (динаміка, особливості написання, особистий підпис);
3) динаміка роботи з клавіатурою та маніпулятором миші;
4) хода (динаміка рухів);
5) динаміка сердечного ритму, динаміка мозкового ритму тощо.

Такі характеристики зазнають впливу керованих і некерованих психічних факторів, що зумовлює потребу в їх періодичному оновленні. Це є однією з причин незначного розповсюдження систем, у яких доступ визначається за динамічним показниками.

При виборі системи біометричної ідентифікації зазвичай беруться до уваги такі показники, як пропускна здатність; надійність; вартість; зручність користування; захищеність даних, точність та продуктивність системи.

Аналіз показує, що найбільш поширеними є системи, у яких розпізнавання здійснюється за відбитками пальців, геометрією об-

личчя та райдужною оболонкою ока. За даними досліджень [2], їхня частка становить понад 80% від загальної кількості систем біометричної ідентифікації. В таблиці 4 наведено результати розрахунку параметрів систем на основі середніх показників *FAR* і *FRR* [2]:

Таблиця 4

Характеристики біометричних систем

Характеристики біометричних систем	Відбитки пальців	2D розпізнавання обличчя	3D розпізнавання обличчя	Райдужна оболонка ока
помилки хибного допуску (*FAR*, %)	0,001%	0,1%	0,005%	0,00001 %
помилки хибної відмови (*FRR*, %)	0,6%	7%	0,1%	0,1%
ймовірність успішної перевірки особи (*ATV*, %)	99,39%	92,91%	99,895%	99,899%
точність (*T*, %)	99,69%	96,45%	99,948%	99,949%
оптимальна пропускна здатність (*N*, чол.)	316	35	141	3162
захищеність (за рейтинговою шкалою 1-10)	6	4	9	10
стійкість до зовнішніх умов (за рейтинговою шкалою 1-10)	10	6	8	9
простота (зручність) використання (за рейтинговою шкалою 1-10)	9	6	10	8
вартість (за рейтинговою шкалою 1-10)	10	10	5	7
швидкодія (за рейтинговою шкалою 1-10)	10	10	7	10
стабільність ознаки в часі (за рейтинговою шкалою 1-10)	9	8	10	10

Представлені дані дають підстави стверджувати, що для середніх і великих виробничих об'єктів, а також для об'єктів стратегічного значення, які вимагають підвищеного рівня безпеки, доцільно використовувати системи біометричного доступу на основі ідентифікації за райдужною оболонкою ока. Для об'єктів з кількістю персоналу до декількох сотень чоловік оптимальним буде доступ за відбитками

пальців. Системи розпізнавання за геометрією обличчя можуть використовуватись у випадках, коли розпізнавання вимагає відсутності фізичного контакту, але поставити систему контролю за райдужною оболонкою неможливо. Наприклад, при необхідності ідентифікації людини прихованою камерою або камерою зовнішнього стеження. Але такі системи є ефективними лише при малій кількості суб'єктів в базі і невеликому потоці людей, що знімаються камерою.

Висновки. Таким чином, аналіз особливостей та основних характеристик біометричних систем ідентифікації показує, що застосування такого типу систем як засобу захисту інформації в системах з керованим доступом є перспективним, не зважаючи на той факт, що дані системи не гарантують стовідсоткової точності розпізнавання. Підвищення достовірності аутентифікації користувачів може досягатися за рахунок підбору оптимальних значень розглянутих характеристик систем біометричної ідентифікації особи.

1. Авраменко В. Ф. Правові основи охорони інформації / В. Ф. Авраменко, Г. О. Брудний, С. І. Жлобін; за ред. проф. В. О. Хорошка. – К. : ТОВ «Поліграф Консалтинг», 2003. – 176 с. **2**. Лебеденко Ю. И. Биометрические системы безопасности / Ю. И. Лебеденко. – Тула : ТулГУ, 2012. – 160 с. **3.** Харитонов А. В. Обзор биометрических методов идентификации личности / А. В. Харитонов // NB: Кибернетика и программирование. – 2015. – № 2. – С. 12–19. **4.** Jyoti Malik. Reference Threshold Calculation for Biometric Authentication / Jyoti Malik, Dhiraj Girdhar, Ratna Dahiya, G. Sainarayanan // Image, Graphics and Signal Processing – 2014. – Vol. 6, № 2. – P. 46–53.

Рецензент: д.т.н., професор Бомба А. Я. (НУВГП)

Shykh N. V., Candidate of Pedagogical Sciences, Associate Professor, Shakleina I. O., Candidate of Physical and Mathematical Sciences, Associate Professor (Drohobych State Pedagogical Univercity)

ANALYSIS OF METHODS OF BIOMETRICAL USER IDENTIFICATION IN SYSTEMS WITH THE GUIDED ACCESS

In the conditions of present time in the systems related to providing of the guided access to information and material objects on the basis of unique authentication of person biometrical technologies are actively used. That's why there is a necessity of analysis of methods and technologies of biometrical authentication with an aim them optimal

practical introduction. In the article the basic methods of biometrical user identification are considered and analyzed; basic descriptions of the systems and their influence on efficiency of work of the system are considered; the features of the use of the biometrical systems for defence and control of productive objects are certain.
***Keywords*: biometric system, authentication, descriptions of the biometric systems.**

Ших Н. В., к.пед.н., доцент, Шаклеина И. А., к.ф.-м.н., доцент
(Дрогобычский государственный педагогический университет имени Ивана Франка)

АНАЛИЗ МЕТОДОВ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В СИСТЕМАХ С УПРАВЛЯЕМЫМ ДОСТУПОМ

В сегодняшних условиях биометрические технологии активно применяются в системах, связанных с обеспечением управляемого доступа к информации и материальных объектов на основе уникальной идентификации личности. В связи с этим возникает потребность анализа методов и технологий биометрической идентификации с целью их оптимального практического внедрения. В статье рассмотрены и проанализированы основные методы биометрической идентификации пользователя; рассмотрены основные характеристики систем и их влияние на эффективность работы системы; определены особенности использования биометрических систем для защиты производственных объектов.
***Ключевые слова*: биометрическая система, идентификация, характеристики биометрических систем.**
