УДК 004.056.52
DOI: https://doi.org/ 10.17721/3041-2323.2025.243-265

Євген РІМЕК, директор
ORCID ID: 0009-0008-1934-7625
e-mail: e.rimek@biosol.ua
Товариство з обмеженою відповідальністю
“Біосол Україна”, Київ, Україна

Артем РІМЕК, магістр
ORCID ID: 0009-0007-7500-4267
e-mail: a.rimek@biosol.ua
Київський національний університет
імені Тараса Шевченка, Київ, Україна

В’ячеслав КОЛОМИЦЕВ, дир. департаменту
ORCID ID 0009-0003-9739-2636
e-mail: v.kolomycev@biosol.ua
Товариство з обмеженою відповідальністю
“Біосол Україна”, Київ, Україна

ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ СТАТИЧНИХ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ В ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті узагальнено практичні засади впровадження біометричних технологій у прикладних інформаційних системах. Розкрито ключові критерії добору методів: точність і надійність за показниками FAR/FRR, стійкість до підробок (PAD/Liveness), швидкодія, інтеграційні вимоги та сумарні витрати (CAPEX/OPEX). Окреслено основні сфери застосування – від аутентифікації в ОС, мережах і веб-ресурсах до контролю доступу, обліку робочого часу, клієнтських сервісів і державних або міжнародних проектів. Також у цій роботі було проведено порівняльні вимірювання FAR та FRR і часу ідентифікації для різних біометричних систем, оцінено типові атаки та ефективність засобів PAD/Liveness. Також досліджено інтеграційні сценарії з IAM/SSO і рольовими політиками доступу, та підготовлено практичні рекомендації й матрицю критеріїв, що можна використовувати для впровадження у державних, корпоративних, особистих та IoT системах безпеки та контролю.

Ключові слова: ***прикладні інформаційні системі, біометричні методи, біометричні технології, біометрична***

ідентифікація особи, захист інформаційних систем, контроль доступу, захист інформації, інформаційна безпека.

Вступ

Сьогоденна безпекова ситуація як в Україні, так і у всьому світі, характеризується великими ризиками, нестабільністю, гібридними та прямими військовими атаками як безпосередньо на людей, так і на інфраструктуру, екологічне середовище, економіку тощо. Тобто практично на всі сфери життєдіяльності суспільства як в Україні, так і за кордоном. Звісно, повномасштабна агресія, здійснена Російською Федерацією в Україні, особливо додає вищезгадані ризики не тільки для всього суспільства в Україні, але і для країн всієї Європи і не тільки.

Гібридні та диверсійні атаки та дії сьогодні також особливо направлені на інформаційні системи та інфраструктуру, яку використовує суспільство для своєї життєдіяльності, особливо на критичну інфраструктуру. Ми бачимо це майже щодня по різним кейсам кібератак, а також по тим наслідкам, до яких ці атаки призводять. На жаль наслідки таких гібридних кібератак можуть (а деякі з них вже призвели) до великої кількості людських жертв. Тому сьогодення вимагає особливо приділити увагу до кіберзахисту, інформаційному та технологічному захисту прикладних інформаційних систем (ПІС).

Однією з компонент для кіберзахисту інформаційних систем може бути біометрична ідентифікація особи-користувача для доступу як до технічних засобів, які використовує прикладна інформаційна система, так і до інформаційних ресурсів, підтвердження та виконання операцій, тощо. Головна вимога до використання біометричних технологій ідентифікації особи-користувача прикладної інформаційної системи (відносно до прав, які надаються користувачеві при використанні ПІС) – це мінімізація ризиків дискредитації облікових записів та підробки біометричних даних користувача ПІС, особливо з правами верхнього рівня, які можуть нанести велику шкоду, або навіть знищити ПІС і за рахунок цього мати великий негативний вплив на інфраструктуру підприємства чи сервіси, на які має вплив ця ПІС, або нею надаються.

У цій статті ми розглянемо які біометричні методи і технології існують, які з них вже активно використовуються на практиці, які з цих методів доцільно використовувати для доступу до ПІС і які з них найбільш поширено сьогодні використовуються. Особливо зупинимося на практичних особливостях використання біометрії для різних задач для доступу та використанню ПІС, а також плюси та мінуси використання деяких статичних біометричних технологій для ідентифікації користувача ПІС, використовуючи досвід практичної реалізації в різних кейсах.

Також у статті будуть надані практичні рекомендації щодо впровадження та використовування біометричних методів та технологій в різних категоріях ПІС (інфраструктурні, сервісні, IoT та інші) по критеріям економічної доцільності, зменшення або зняття ризиків, екологічності, простоті використання, тощо.

Основна частина і результати

Методи та технології біометричної ідентифікації особи

Використання біометричних технологій сприяє досягненню відповідності нормативним вимогам, забезпечує надійний захист внаслідок однозначної автентифікації та авторизації, забезпечує життєво важливі гарантії та спокій для всіх зацікавлених сторін.

Біометричні технології ідентифікації та автентифікації, у порівнянні з традиційними методами, демонструють численні переваги та знаходять все ширше застосування у комп'ютерних системах.

Нагадаємо, що біометрична ідентифікація – це процес визначення особистості за винятковими біологічними характеристиками, які є унікальними для кожної особи. Використовують більше десяти різних унікальних біометричних ознак, притаманних конкретній особі.

За способом взаємодії з біометричними ознаками, біометричні методи ідентифікації розділяються на статичні (використання ознак, що не змінюються протягом життя), динамічні (використання ознак, що змінюються або генеруються під час дії) та комбіновані (використання комбінації обох типів).

Статичні методи використовують спеціальне обладнання (біометричні сканери) для зняття біометричної інформації і в подальшому, використовуючи спеціалізовані математичні

алгоритми, обробляють біометричну інформацію, записуючи її у вигляді цифрового унікального коду, що зберігається в базі даних. В подальшому отриманий еталонний біометричний шаблон людини використовуються для порівняння з іншими біометричними даними цієї ж людини для її аутентифікації, використовуючи ту ж саму біометричну технологію, за допомогою якої формувався біометричний шаблон.

Динамічні методи використовують алгоритми, які в першу чергу аналізують динамічні процеси і також шифрують цю інформацію в вигляді деякого цифрового коду для подальшого зрівняння з аналогічними процесами.

Комбіновані методи біометричної ідентифікації (так звана багатофакторна автентифікація) поєднують декілька методів ідентифікації (як правило статичний + динамічний метод, або декілька) для того, щоб збільшити достовірність ідентифікації та прискорити процес пошуку і обробки результатів.

До основних статичних біометричних методів відносяться:

– ідентифікація по відбиткам пальців;
– ідентифікація по обличчю;
– ідентифікація по радужній оболонці ока;
– ідентифікація по геометрії долоні;
– ідентифікація, що використовує термограму обличчя;
– ідентифікація по ДНК;
– ідентифікація на основі характеристик уха;
– ідентифікація по малюнку венозної сітки долоні.

До основних динамічних біометричних методів відносяться:

– ідентифікація за голосом;
– ідентифікація за рукописним почерком;
– ідентифікація за механікою роботи на клавіатурі;
– ідентифікація за ходою особи.

Критерії використання деяких технологій біометричної ідентифікації наведені в табл. 1.

Таблиця 1

Порівняння основних статичних біометричних методів

Біометричні методи	FAR, %	FRR, %	Фальсифікація	Сувора аутентифікація	Сталість	Швидкість аутентифікації	Вартість реалізації
Відбиток пальця	0,001	0,6	Можлива	Можлива	Низька	Висока	Низька
Розпізнавання обличчя 2D	0,1	2,5	Можлива	Ні	Низька	Середня	Середня
Розпізнавання обличчя 3D	0,0005	0,1	Проблематична	Ні	Висока	Низька	Висока
Райдужна оболонка ока	0,00001	0,016	Неможлива	Можлива	Висока	Висока	Висока
Сітківка ока	0,0001	0,4	Неможлива	Можлива	Середня	Низька	Висока
Венозний малюнок долоні	0,00008	0,01	Неможлива	Можлива	Середня	Висока	Середня

Найбільш важливими з цих критеріїв є 2, які використовують для порівняння якості методів та технологій біометричної ідентифікації – це FAR (False Acceptence Rate, або частота помилкових спрацювань) та FRR (False Rejection Rate, або частота відмов у спрацьовуванні).

FAR та FRR одержують розрахунковим шляхом на основі методів математичної статистики.

Чим нижчі ці показники, тим точніше розпізнавання об'єкта.

Саме ці критерії є ключовими для визначення доцільності використання того чи іншого статичного біометричного методу для тої чи іншої задачі.

Процес формування біометричного контрольного шаблону особи на прикладі використання технології венозної сітки долоні наведено на рис. 1.

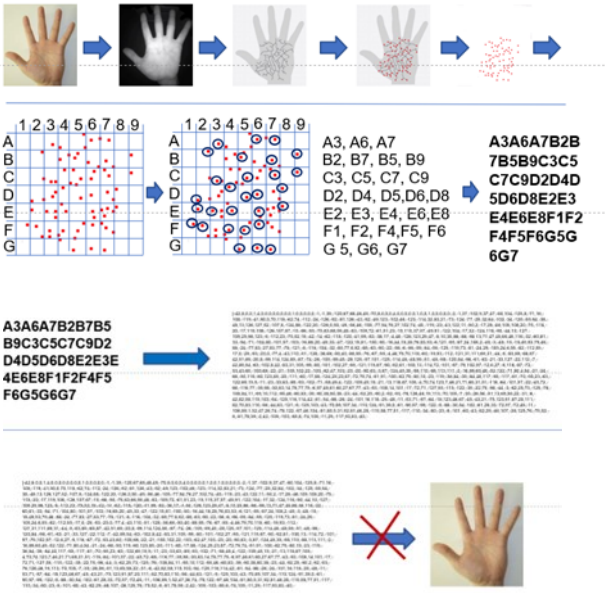

Рис. 1. *Процес формування біометричного контрольного шаблону особи на прикладі використання технології венозної сітки долоні*

Фактичний процес перетворення біометричних даних особи набагато складніший, детальніший хоча й займає небагато часу. Але результатом завжди є біометричний контрольний шаблон, який не містить в собі реальних біометричних даних особи і відповідно не може перетворити контрольний шаблон зворотно в біометричні дані особи. Відповідно питання збереження та використання біометричного шаблону не ставить під загрозу персональні дані особи, бо вони не зберігаються в базі даних.

Замість них зберігається зашифрований за допомогою спеціальних алгоритмів набір символів.

Подальша ідентифікація особи відбувається шляхом порівняння збереженого біометричного контрольного шаблону з реальними біометричними даними особи під час її ідентифікації для надання доступу для тих чи інших ресурсів (рис. 2).

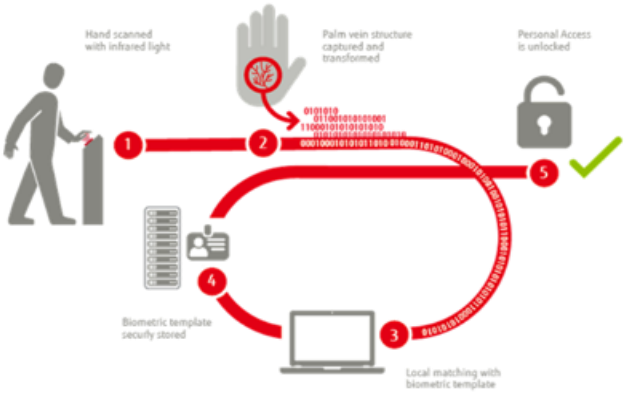

Рис. 2. *Схема процесу ідентифікації особи через порівняння збереженого біометричного контрольного шаблону з реальними біометричними даними*

Сфери та задачі, в яких використовуються статичні методи біометрії

Останні 10-15 років у світі поступово розповсюджується використання біометричних методів у різноманітних сферах суспільного життя і в прикладних інформаційних системах, які обслуговують ці сфери (Jain, Nandakumar & Ross, 2016), зокрема:

– персоніфікована ідентифікація для доступу до операційних систем і локальних мереж, при підтвердженні особи та повноважень користувачів прикладних інформаційних систем, де необхідно пройти процедуру авторизації;

– аутентифікація при доступі до веб-ресурсів;

– визначення конкретної фізичної особи в системах контролю доступом;

– облік робочого часу персоналу підприємств і установ;

– реєстрація та ідентифікація клієнтів;

– підтвердження особистості клієнтів під час здійснення електронних платежів;

– впровадження соціальних проектів, що вимагають ідентифікаційних процедур (електронне урядування, біометричні системи голосування, благодійні акції тощо);

– забезпечення надання персоніфікованих послуг (фінансових, медичних, соціальних, адміністративних);

– забезпечення контролю обмежень доступу до інформації (конфіденційна інформація, закриті реєстри, персональні дані, медичні дані).

– точна ідентифікація особи для управління процесами та прийняття рішень (фінансові установи, органи державної влади, силові відомства, енергетика).

Це знайшло своє відображення у розробці відповідних міжнародних стандартів. Зокрема, в Стандарті ISO/IEC-19795-1-2021 було продемонстровано потік інформації в загальній (незалежно від конкретного біометричного методу) біометричній системі, від збору даних, обробки сигналів та зберігання даних до порівняння, процесу перевірки/ідентифікації та прийняття рішення про доступ або відмову в доступі для користувача.

Загальний процес сканування біометричних даних, їх обробки, зберігання і прийняття рішення описаний в стандарті ISO/IEC-19795-1-2021 (International Organization for Standardization, 2021) та представлений на рис. 3.

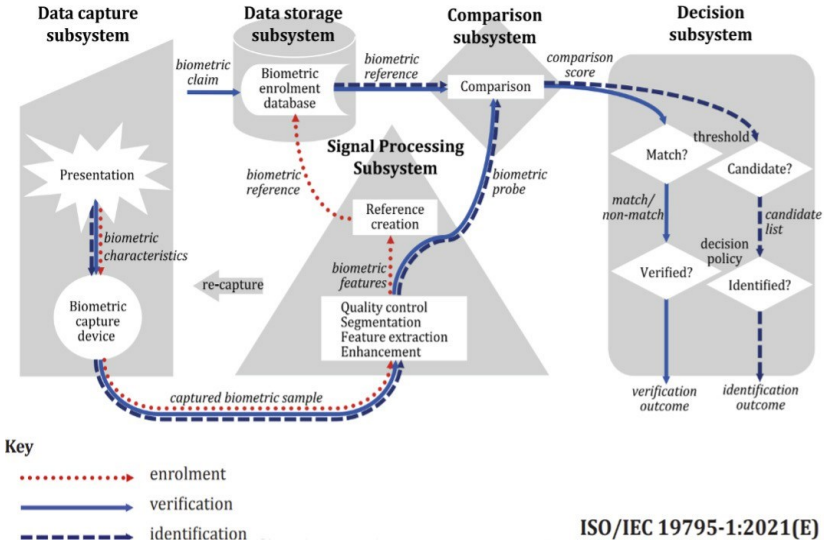

Рис. 3. *Схема загального процесу сканування біометричних даних та їх оброблення*

Не всі технологічні рішення виробників конкретних продуктів біометричної ідентифікації використовують всі компоненти цього стандарту, але загалом всі концептуальні блоки тут відображені.

Сучасні підприємці мають захищати мережі без кордонів, надаючи користувачам доступ у будь-який час і будь-де, щоб вони були продуктивними. Досягнення правильного балансу між безпекою та зручністю залежить від того, щоб користувачі були тими, ким вони себе визнають, – надання доступу лише до ресурсів, якими вони уповноважені користуватися.

Відповідно стратегія безпеки не має бути зосереджена тільки на захисті периметра – вона зосереджена на захисті особистості (Yeoh, et al., 2023). Це користувач з обліковими даними, якому за

замовчуванням не дозволено переглядати або робити що-небудь у мережі організації чи за її межами. Всі користувачі незалежно від посад повинні пройти автентифікацію, авторизацію та безперервну перевірку, перш ніж отримати доступ до прикладних програм, інформаційних систем і даних. Такий підхід ліг в основу концепції ZeroTrust – стратегії безпеки з нульовою довірою.

Люди віддають перевагу зручності, а не безпеці – це поняття називається тертям безпеки. Вони чують «безпеку» і думають про «розчарування», оскільки інструменти, призначені для захисту систем і додатків, часто заважають виконувати їхню роботу.

Архітектура інформаційних систем з нульовою довірою вимагає цифрової ідентифікації в основі своєї основи, створення контрольних точок, які вимагають авторизації та аутентифікації, щоб не допустити зловмисників і запобігти кібератакам і злому даних.

Одним з прикладів практичного використання біометричних методів для ідентифікації особи користувача є рішення, розроблене спеціально для ERP SAP, яке дозволяє, використовуючи внутрішню мову програмування ABAP, ефективно захищати конфіденційні дані, критичні функції з одночасним зниженням внутрішніх витрат на IT та адміністрування.

Єдиний вхід до інформаційної системи за допомогою біометричної аутентифікації дозволяє використання цифрових підписів для узгодження фінансових, організаційних, транспортних або адміністративних трансакцій з документуванням всіх дій ідентифікованих користувачів.

Забезпечення принципу подвійного контролю (за допомогою використання біометричного підтвердження повноважень користувачів на здійснення тих чи інших операцій в інформаційній системі) мінімізує ризики крадіжки, зловживання своїми повноваженнями та захист від маніпуляцій.

Іншим прикладом є використання біометричних методів в різних галузях економіки за допомогою спеціалізованого програмного забезпечення.

Спеціалізоване програмне забезпечення завдяки легкій інтеграції з розробниками відповідних біометричних програмних

продуктів підтримує широкий спектр методів та пристроїв аутентифікації, включаючи біометричні дані, які можуть миттєво ідентифікувати користувачів для доступу до робочого простору (прикладних програм, додатків, медичного та іншого обладнання, тощо) без порушення робочих процесів.

До ключових особливостей таких рішень відносяться забезпечення єдиного входу на робочому столі ПК для всіх програм та швидке перемикання користувачів на одному ПК.

Підпис та узгодження того чи іншого рішення на кожному етапі робочого процесу потребує повторної біометричної аутентифікації, яка займає декілька секунд. Відповідно не призводить до додаткових часових витрат і не створює ускладнення робочого процесу.

Навпаки, використання біометричних методів автентифікації забезпечує безпечний та зручний доступ до корпоративних даних, що дозволяє оптимізувати робочі процеси та скоротити витрати робочого часу до 20% на введення логінів та паролів. Подібні рішення дозволяють компаніям повною мірою використовувати переваги своїх інвестицій у технології, вбудовуючи прозору, безшовну та зручну систему безпеки у робочі процеси та оптимізувати свою роботу.

Однією дією користувач отримує доступ до всіх корпоративних програм, не вводячи кожного разу свої ім’я користувача та паролі. Технологія дозволяє захищати дані згідно з груповою політикою безпеки підприємства.

Використання комплексних рішень з точним контролем доступу на основі ролей, автоматизованою ініціалізацією та деініціалізацією, оптимізованими процесами аудиту та аналітики, дозволяє швидше оцінити загрози та усунути їх.

Наприклад, до ключових переваг використання біометричних рішень у медичній сфері можна віднести:

– скорочення витрат на ІТ, шляхом автоматизації адміністрування облікових записів користувачів;

– встановлення більш детального контролю за дотриманням політики безпеки та нормативних вимог;

– розширення можливостей для надання високоякісної медичної допомоги при одночасному підвищенні продуктивності;

– надійний та безпечний доступ до медичного обладнання провідних європейських та американських виробників.

– ідентифікація пацієнтів за допомогою безконтактної біометричної аутентифікації в прикладній медичній інформаційній системі дозволяє:

– підвищувати фізичну безпеку пацієнтів й зменшувати кількість медичних помилок; покращувати якість сервісу роботи з пацієнтом;

– усувати дублікати в медичних записах;

– зменшувати кількість медичних претензій та покращувати фінансові результати медичних установ.

Прикладом універсального програмного рішення, що не залежить від конкретної прикладної інформаційної системи чи галузі використання може бути біометричне програмно-апаратне рішення єдиного входу (SSO – Single Sign-On), що дозволяє користувачам входити в мережу та до всіх прикладних програм, які вони мають право використовувати, використовуючи один надійний пароль. Єдиний вхід позбавляє користувачів тягаря запам'ятовування кількох паролів, підвищує продуктивність, допомагаючи користувачам уникнути блокування систем, та знижує витрати ресурсів, зменшуючи кількість дзвінків до служби підтримки для скидання нового або тимчасового пароля.

Понад усе, рішення єдиного входу посилює IT-безпеку, оскільки користувачі більше не вдаються до записування паролів на папірцях та не залишають їх там, де їх можуть вкрасти та використати неавторизовані (сторонні або ті, що не мають відповідних повноважень) особи.

Створення рішення для надійної автентифікації за допомогою біометричного програмно-апаратне рішення єдиного входу надає ефективний та доступний спосіб впровадження заходів інформаційної безпеки, що рекомендуються або зобов'язані регуляторними органами, галузевими аналітиками, галузевими асоціаціями та державними установами.

Водночас, використання подібного рішення надає підприємствам гнучкість у виборі правильної комбінації методів надійної автентифікації, яка найкраще відповідає специфіці бізнесу, встановленим робочим бізнес-процесам та різним ролям і обов'язкам співробітників – незалежно від того, наскільки велике або географічно розосереджене підприємство його використовує.

Ще одним прикладом використання біометричних методів є застосування їх у інформаційних системах та компонентах сумісності з метою підвищення ефективності управління зовнішніми кордонами ЄС, візової та міграційної політики, боротьби зі злочинністю та тероризмом.

Багато з цих систем використовують біометричні дані для встановлення або перевірки особи. Наприклад, Шенгенська інформаційна система (SIS) працює з 2023 року. Система в'їзду/виїзду (EES) починає функціонувати у 2025 році.

Європейська інформаційна система кримінальних записів громадян третіх країн (ECRIS-TCN) почала працювати у 2025 році, а давно існуючі Візова інформаційна система (VIS) та Європейська дактилоскопія (EURODAC) зазнають оновлення та розширення у 2026 році.

Ці масштабні ІТ-системи ЄС впроваджує, забезпечуючи сумісність, точність, якість біометричних даних, надійність і зручність використання, що є необхідним для забезпечення різних установ держав-членів ЄС взаємопов’язаними посиланнями, зробленими в той чи іншій інформаційній системи, через забезпечення правильної ідентифікації осіб та захист чутливої персональної інформації найвищим рівнем безпеки даних та усіма необхідними запобіжними заходами.

Прийняття моделі безпеки з нульовою довірою може бути складним, але, маючи міцну основу біометричних технологій, організації можуть знизити ризики, не жертвуючи продуктивністю та користувацьким досвідом.

Уніфіковані рішення для доступу та аутентифікації забезпечують безпечний, спрощений доступ до локальних і хмарних програм з будь-якого пристрою та в будь-якому місці.

Централізований доступ до ідентифікації та аутентифікація по всьому підприємству за допомогою швидкої біометричної автентифікації для локального або віддаленого доступу до прикладних інформаційних систем, хмарних додатків, спеціалізованої апаратури, пристроїв та інших важливих елементів робочих процесів дозволяє успішно використовувати підхід нульової довіри.

Одним з прикладів використання концепції нульової довіри є впровадження комплексної інформаційної системи з використанням біометричних даних клієнтів в мережі Korea Airports Corporation (KAC) для прискорення реєстрації пасажирів забезпечуючи високий рівень точності, зручності при гарантовано високому рівні безпеки.

Використання біометричних методів ідентифікації особи при наданні соціальних послуг дозволило Раді соціального забезпечення Белізу (SSB) суттєво підвищити ефективність роботи корпоративної інформаційної системи Microsoft Dynamics з одночасним скороченням рівня зловживань з боку користувачів соціальних послуг.

Впровадження біометричних технологій у фінансовому секторі Японії свого часу забезпечило як підвищення ефективності роботи фінансових установ, так і дозволило шляхом мінімальної модернізації перетворити прикладні інформаційні системи фінансових установ в високонадійні та безпечні системи, що гарантують як комфортність користування так і високу надійність конфіденційності та безпеки даних.

Досвід впровадження статичних біометричних рішень. Практичні вимоги та ризики

Треба зазначити, що на практиці нівелювання (або зменшення) загроз дискредитації біометричної компоненти функціонування ПІС тісно пов’язане з правильними організаційними діями на підприємстві (построєні бізнес-процеси, організаційні дії), ефективним кіберзахистом технологічної і інформаційної інфраструктури, резервуванням як інформації, так і апаратної інфраструктури, протоколами дій як підрозділів фізичної безпеки, так і інформаційної безпеки (в т.ч. так звана інсайдерська загроза, тобто можливість колаборантних або саботажних дій

співробітників компанії). Але в цій статті ми не будемо детально зупинятися на цих всіх аспектах.

Що стосується самої біометричної компоненти ПІС, для неї розглядається 9 точок загроз, як вказано в стандарті ISO/IEC 30107-1:2023 (International Organization for Standardization, 2023), і відображено на рис. 4.

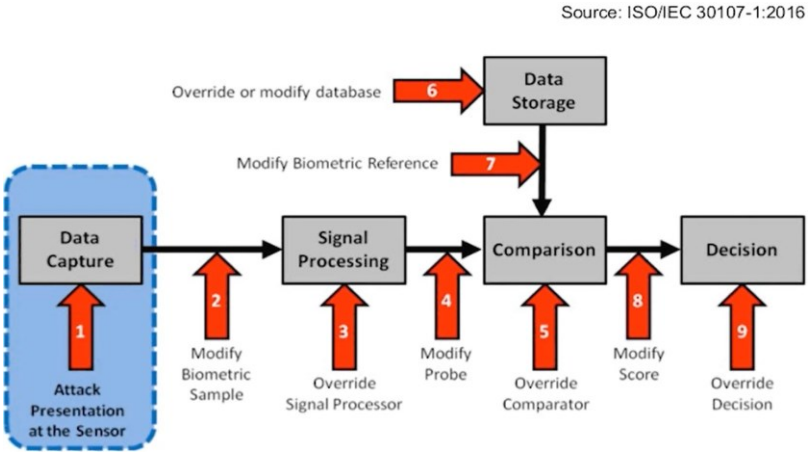

Рис. 4. *Схема 9 точок загроз для біометричної системи*

На представленому рис. 4 загроза 1 – це пряма атака на біометричний сенсор; 2, 4, 7, 8 – непрямі атаки на канали передачі даних (як фізичні, так і логічні); 3, 5 – це атаки на модулі біометричної підсистеми ПІС з ціллю або їх виключення, або дискредитації; 6 – втручання в базу даних з ціллю дискредитації, або несанкційного копіювання інформації; 9 – вплив на рішення біометричної компоненти ПІС (Biometric vulnerabilities, 2025).

Атаки 2-9 мають бути нівельовані системою кіберзахисту та організаційними заходами, які унеможливлюють фізичне втручання в мережеву інфраструктуру.

Що стосується вибору та практичного використання того чи іншого методу біометричної ідентифікації особи-користувача ПІС, тут треба зважити по-перше на параметри FAR і FRR цього методу біометрії, по-друге можливість підробки як самих

біометричних даних, так і процесу сканування особи. Можливості підробки деяких технологій сканування статичних біометричних параметрів людини описані в новітньому звіті Європол «Біометричні вразливості. Забезпечення майбутньої готовності правоохоронних органів» (Biometric vulnerabilities, 2025).

Характеристики FAR, FRR отримують розрахунковим шляхом на основі методів математичної статистики. Чим нижче ці показники, тим точніше розпізнавання об'єкта (див. табл. 1).

В Україні серед статичних методів ідентифікації особи найбільш використовуються наступні методи: сканування пальця (копія поверхні та використання оптичних датчиків) FingerPrint, ідентифікація по обличчю (2D та 3D) FaceID/FaceRecognition та сканування долоні (по відбитку або безконтактне інфрачервоне сканування (PalmVein/PalmSecure)).

Серед динамічних методів на практиці найбільш використовується голосова ідентифікація.

Ці методи часто поєднуються з багатофакторною ідентифікацією (2MFA) за допомогою пін-кодів, смарт-карт, токенів, тощо.

Також біометричні пристрої статичної аутентифікації часто поєднують з датчиками тепла та руху. Пристрої для сканування обличчя часто використовують дві-три камери для алгоритмічного моделювання 3D голови, в різних частотних діапазонах, алгоритми розпізнавання руху, тощо. Все це робиться для того, щоб зменшити вірогідність підробки сканування.

Але на практиці це підвищує вірогідність видачі системою рішення FALSE там, де має бути TRUE (параметр FRR), значно подовжує час на процес сканування і ідентифікації, значно підвищує вимоги до технічних засобів ПІС та розміру сховищ даних, вимоги та надійність телекомунікаційної інфраструктури та каналів зв’язку. Особливо це критично, коли основні бази даних знаходяться в віддаленій хмарі, для аналізу даних використовується штучний інтелект (AI), а також в IoT-системах.

У середовищі IoT біометрія дає змогу ефективно та швидко керувати доступом до важливих об’єктів та приміщень.

У розумних будівлях та офісах біометрія дозволяє безключового та безпарольного входу через двері, турнікети, виклику ліфта з автоматичним призначенням поверху, доступу до переговорних, серверних і комірок. Події ідентифікації синхронізуються з контролером біометричних датчиків та загальної системи безпеки. Наприклад при вході співробітника вмикається робочий профіль, тобто світло у офісі, клімат чи доступ до робочого місця, а в аварійних режимах пожежі чи евакуацій, то правила доступу миттєво змінюються. Для відвідувачів біометрія спрощує реєстрацію чи введення обліку входу у вхідні пункти одночасно майже миттєво створює тимчасовий профіль із правами, дієвими лише у потрібних зонах і в заданий час.

У промислових середовищах біометрія виконує важливішу функцію «ключа безпеки» до небезпечних об'єктів чи обладнання доступ до яких має бути лише у авторизованих працівників (станки з ЧПК, преси, конвеєри чи роботизовані клітки). З огляду на рукавички та ЗІЗ, у таких зонах частіше застосовують безконтактні біометричні сенсори (обличчя, райдужна оболонка ока, долонна/венозна біометрія PalmVein).

У логістиці й на складах біометрія з'єднує фізичні об'єкти з цифровим ланцюжком доставки та перевезень (видача й повернення інструментів, ТМЦ, сканерів, ТСД і ключів до навантажувачів). Також біометрія фіксує хто знаходиться та кому передавався вантаж разом із роллю та зміною. Доступ до докових воріт, рамп та окремих зон (цінні вантажі, «клітки») може також контролюватися чебрез біометричні пристрої, як наприклад кур'єри отримують тимчасові права для відкриття поштових шаф і модульних сейфів.

У медицині біометрія зменшує ризики помилок і зловживань, та дає тільки авторизований та захищений доступ до медичних холодильників, сейфів з наркотичними або сильнодіючими препаратами, анестезіологічні візки й аптеки-комірки. Усі дії з препаратами відстежуються до персони. На робочих станціях у відділеннях використовується швидка біометрична автентифікація для входу та підпису дій у медичних IoT-системах,

а в телемедичних кіосках біометрія дозволяє дистанційну ідентифікацію пацієнта перед наданням послуги.

Для державного сектору та критичної інфраструктури біометрія дає захищений доступ до серверних ресурсів та дата-центрів. Доступ до кімнат де зберігаються зброї, архівів доказів, сховищ ключових документів або до кризових та штабних центрів робиться записи в цифрових журналаг через біометричних пристроїв з миттєвим відкликанням прав.

Спільним знаменником для всіх цих сценаріїв є те, що біометрія в IoT системах, спрощує та підвищує загальну ефективність роботи та захисту інформації або обьектів.

Як ми зазначали вище, так як досліджено в звіті Європолу (Biometric vulnerabilities, 2025), технології сканування пальців та розпізнавання обличчя нажаль достатньо легко підробити. Особливо це стосується сканування відбитка пальця (як на смартфонах або планшетах) або сканування відбитка долоні (без глибинного сканування венозної сітки пальця або долоні). І навпаки безконтактне сканування венозної сітки долоні (PalmVein) надає майже 100% достовірність ідентифікації і неможливість підробки (див. табл. 1 з FAR і FRR).

Тому при плануванні та реалізації практичних проектів порівнюють – технологія біометрії (FAR і FRR) / простота реалізації / швидкість ідентифікації / ризики підробки або атаки / необхідні технічні та інформаційні ресурси / можливість інтеграції з існуючими іншими ПІС та технологічними процесами / Ціна.

Для складання оптимального рішення аналізуються можливі компроміси між вимогами з урахуванням важливості (ранжування, в тому числу за допомогою вагових коефіцієнтів) параметрів проекту для кожної практичної реалізації. І звісно практична експлуатація може вносити свої корективи в це ранжування.

Таким чином, важливо, щоб вибрана технологія і проектне рішення в цілому мали можливість змінюватись, якщо потрібно внести корективи в діючий проект.

Окремо треба підкреслити питання дискредитації облікових записів користувачів ПІС, особливо з великими правами, які

можуть мати величезний вплив як на функціювання ПІС, так і на роботу підприємства в цілому. І нажаль сьогоденному середовищі гібридної війни ми вже маємо достатньо багато кейсів, як дискредитація облікових записів вплинула на роботу великих компаній, як в Україні так і в світі.

Тому впровадження протоколів SSO та IAM за допомогою заміни паролів та пін-кодів на біометричні методи ідентифікації особи-користувача ПІС мають дуже велике значення. І тут постає питання важливості ролей та прав користувачів ПІС! В практичних проектах ми та наші партнери рекомендують проектувати ПІС, використовуючи різні біометричні технології для різних ролей користувачів, згідно з ризиками і доцільністю впроваджувати той чи інший метод біометрії, в тому числі враховуючи вартість обладнання, програмного забезпечення, процесу ліцензування, вартість CAPEX і OPEX, простота експлуатації системи. Але різні технології в проекті мають бути сумісні і цілостні в рамках всього рішення.

Впровадження біометричної ідентифікації користувача ПІС також важливо і для задач доступу до документації та цифрового підпису, виконання різних процесів в компанії або за допомогою ПІС назовні.

Ми будемо розглядати 5 основних блоків ролей користувачів:

– адміністратори ПІС (глобальні та локальні);

– ТОП-персонал компанії з високими правами прийняття рішень;

– користувачі ПІС з правами вносити або коригувати якісь дані;

– користувачі тільки з правами моніторингу;

– зовнішні користувачі (наприклад, клієнти).

Реальних ролей користувача ПІС може бути і більше, але вони блокуються в ці 5 категорій. Для перших двох або трьох блоків користувачів дуже важливо надати технології з мінімальними ризиками дискредитації (наприклад, PalmVein).

Інші види користувачів не мають впливу на працездатність ПІС і тому для них можуть використовуватись більш дешеві, але менш захищені технології біометричної ідентифікації (наприклад, FingerPrint або FaceID). Але звісно в межах кожного

проєкту компромісні рішення формуються на основі аналізу вимог замовника та проходять узгодження з ним.

Дискусія і висновки

У наші часи сучасні прикладні інформаційні системи (ПІС) потребують надійних механізмів керування доступом, тому біометрія в наші часи дуже має дуже інтенсивний розвиток що дозволяє використовувати біометричні методи у різноманітних сферах суспільного життя і в прикладних інформаційних системах, які обслуговують ці сфери. Біометрія може адаптивно вписуватися в загальну архітектуру системи, при цьому вона зменшує залежність від паролів і підвищує зручність без втрат для безпеки.

Біометрія доказує свою ефективність у широкому спектрі ПІС, починаючи від контролю доступу, обліку робочого часу, IoT-систем та клієнтських сервісів закінчуючи критичними для державних та міжнародних систем ідентифікації (SIS, EES, ECRIS-TCN тощо). Наприклад, для підприємств найбільший ефект саме мають поєднання SSO/IAM з біометричною автентифікацією та рольова диференціація методів за ризиком і повноваженнями.

Зазвичай загрози для біометрії охоплюють як спроби підробки (спуфінгу) на рівні сенсора, так і маніпуляції каналами зв'язку та програмно-апаратними рішеннями. Водночас біометрія вже широко застосовується у різних сферах суспільного життя: для персоніфікованої ідентифікації під час входу в операційні системи та локальні мережі й підтвердження особи в прикладних програмах; для аутентифікації при доступі до веб-ресурсів; для ідентифікації та верифікації у системах контролю доступу; ведення обліку робочого часу персоналу; реєстрації та ідентифікації клієнтів; підтвердження особи під час електронних (зокрема дистанційних) платежів; у соціальних і державних сервісах, що потребують ідентифікації (електронне урядування, голосування, гуманітарні та благодійні програми); а також у державних та міжнародних проектах – для оперативної перевірки осіб, контролю кордонів, візових процедур тощо.

Також використання кількох біометричних рішень у межах MFA додатково підвищує надійність і зменшує ризики

компрометації, але може впливати на час процесу ідентифікації та вартість системи.

Таким чином, при практичному впровадженню/проектуванню системи біометричної ідентифікації особи для різних категорій ПІС вкрай важливо аналізувати все в комплексі, разом з організаційними процесами користування ПІС, заходами кібербезпеки від загроз мережевої та інформаційної інфраструктури, а також знаходження достатніх компромісів між ризиками дискредитації, простотою використання, вартістю та іншими критеріями, вказаними в цій статті.

Список використаних джерел

Europol. (2025). *Biometric vulnerabilities: Ensuring future law enforcement preparedness* (Report No. QL-01-25-000-EN-N). https://www.europol.europa.eu/publication-events/main-reports/biometric-vulnerabilities-ensuring-future-law-enforcement-preparedness.

International Organization for Standardization. (2021). *ISO/IEC 19795-1:2021. Conceptual representation of general biometric system* (Section 6.1).

International Organization for Standardization. (2023). *ISO/IEC 30107-1:2023. Information technology – Biometric presentation attack detection – Part 1: Framework*. https://www.iso.org/standard/83828.html.

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges and opportunities. *Pattern Recognition Letters, 79*, 80–105. https://doi.org/10.1016/j.patrec.2015.12.013.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14(1),* 4–20. https://doi.org/10.1109/TCSVT.2003.818349.

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security, 133*, 103412. https://www.sciencedirect.com/science/article/pii/S016740482300322X.

References

Europol. (2025). *Biometric vulnerabilities: Ensuring future law enforcement preparedness* (Report No. QL-01-25-000-EN-N). https://www.europol.europa.eu/publication-events/main-reports/biometric-vulnerabilities-ensuring-future-law-enforcement-preparedness.

International Organization for Standardization. (2021). *ISO/IEC 19795-1:2021. Conceptual representation of general biometric system* (Section 6.1).

International Organization for Standardization. (2023). *ISO/IEC 30107-1:2023. Information technology – Biometric presentation attack detection – Part 1: Framework*. https://www.iso.org/standard/83828.html.

Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges and opportunities. *Pattern Recognition Letters, 79*, 80–105. https://doi.org/10.1016/j.patrec.2015.12.013.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14(1),* 4–20. https://doi.org/10.1109/TCSVT.2003.818349.

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security, 133*, 103412. https://www.sciencedirect.com/science/article/pii/S016740482300322X.

Отримано редакцією журналу / Received: 24.09.25
Прорецензовано / Revised: 29.09.25
Схвалено до друку / Accepted: 01.10.25

Ievgen RIMEK, Director
ORCID ID: 0009-0008-1934-7625
e-mail: e.rimek@biosol.ua
Limited Liability Company "Biosol Ukraine", Kyiv, Ukraine

Artem RIMEK, Master
ORCID ID: 0009-0007-7500-4267
e-mail: a.rimek@biosol.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Viacheslav KOLOMYTSEV, Deputy Director
ORCID ID 0009-0003-9739-2636
e-mail: v.kolomycev@biosol.ua
Limited Liability Company "Biosol Ukraine", Kyiv, Ukraine

PRACTICAL ASPECTS OF USING STATIC BIOMETRIC TECHNOLOGIES IN APPLIED INFORMATION SYSTEMS

The paper generalizes the practical foundations for deploying biometric technologies in applied information systems. It outlines the key criteria for selecting methods: accuracy and reliability by FAR/FRR indicators, resistance to spoofing (PAD/Liveness), performance, integration requirements, and total cost (CAPEX/OPEX). The principal application areas are defined – from authentication in operating systems, networks, and web resources to access control, time and attendance, customer services, and governmental or international projects. The study also reports comparative measurements of FAR/FRR and identification time for different biometric systems, assesses common attacks and the effectiveness of PAD/Liveness tools, examines integration scenarios with IAM/SSO and role-based access policies, and provides practical recommendations and a criteria matrix that

can be used for deployments in government, corporate, personal, and IoT security and access-control systems.

Keywords: ***applied information systems, biometric methods, biometric technologies, biometric identification of individuals, protection of information systems, access control, information protection, information security.***

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.