

Біометричні технології ідентифікації:

кордони, контроль доступу, FinTech та інші кейси



Розберімо разом, яка існує біометрія, яке вона має історичне підґрунтя, як вона працює та яку користь приносить замовникам і користувачам різноманітних сервісів.

Що таке біометрія і коли вона виникла

Міжнародний стандарт ISO/IEC 2382-37:2022 Information technology — Vocabulary — Part 37: Biometrics визначає термін «біометрія» (biometrics) як «автоматизоване розпізнавання індивідуумів на основі їхніх біологічних і поведінкових характеристик». Термін «біометрична характеристика» (biometric characteristic) — це «біологічна та поведінкова характеристика особи, з якої можна виділити відмітні повторювані біометричні ознаки з метою біометричного розпізнавання». Прикладами біометричних характеристик є «структура хребта Гальтона, топографія обличчя, текстура шкіри обличчя, топографія кисті, топографія пальців, структура райдужної оболонки, структура вен кисті, структура валика долоні, малюнок сітківки, динаміка рукописного підпису тощо». Ці характеристики часто називають модальностями (modes), а використання кількох (принаймні двох із трьох) біометричних характеристик в одній біометричній системі називається мультимодальним (multimodal).

Як часто буває із складними технічними системами, історія біометрії починається значно раніше, ніж

технології, які її використовують та стандартів, які її описують. Автоматизовані біометричні системи існують лише кілька десятиліть, але вони базуються на ідеях, яким сотні й тисячі років.

Стародавні єгиптяни розпізнавали надійних торговців за їхніми фізичними підписами (відбиток пальців на документах). У Вавилоні відбитки пальців використовувалися для ідентифікації купцями, які записували ділові операції на глиняних табличках, датованих 500 роком до нашої ери. У другому столітті до н. е. китайський імператор Цинь Ши Хуан вже засвідчував справжність певних печаток за допомогою відбитків пальців. Китайські купці також використовували відбитки пальців як ідентифікатори для ділових операцій у 14 столітті. Про унікальність малюнку шкіри на внутрішній стороні долоні людини було відомо за 3000 років до нашої ери, коли з'явилися перші згадки про хіромантію в давньоіндійських текстах, а пізніше і в Китаї, і в Греції. Хоча у сучасному світі хіромантію вважають псевдонаукою, проте підтверджено, що відбитки пальців та структура вен є реальними та унікальними біометричними характеристиками кожної людини.

Перша біометрія: відбитки пальців (Fingerprints)

У середині 1800-х років швидка урбанізація під час промислової революції збільшила потребу у формальних методах ідентифікації людей. Британці, французи і аргентинці досі сперечаються, хто ж був першою особою, яка впровадила першу ідентифікацію. Але точно відомо, що перші методи ідентифікації мали на меті допомогти правоохоронним структурам боротися зі злочинністю.

Деякі джерела повідомляють, що у 1891 році аргентинський поліцейський Хуан Вучетич (Juan Vucetich) почав збирати відбитки пальців злочинців, що стало одним з перших систематичних застосувань біометрії для ідентифікації особи.

Достеменно відомо, що у 1879 році офіцер французької поліції Альфонс Бертильон (Alphonse Bertillon) розробив антропометричну систему, а саме — систему ідентифікації Bertillonage, яка передбачала вимірювання різних фізичних характеристик, таких як зріст, вага, розміри голови, рук і ніг, щоб ідентифікувати злочинців. Система також враховувала татуювання, шрами та риси обличчя. Інформацію записували на картки, які містили фотографії людей у фас і профіль. Паризька поліція прийняла цю систему на початку 1880-х років. Ця система широко використовувалася поліцейськими департаментами по всьому світі і вважалася золотим стандартом ідентифікації до початку 20 століття.

Британці почали використовувати відбитки пальців випадково, у липні 1858 року, коли сер Вільям Гершель (William Herschel), головний суддя округу Хуглі в Джунгипурі, Індія, досяг межі свого розчарування через нечесність місцевих жителів. Гершель наказав місцевому бізнесмену Раджадхару Конаї зробити відбиток своєї руки на звороті контракту. Ідея Гершеля полягала лише в тому, щоб «налякати його від усякої думки про відмову від свого підпису». Раджадхар Конаї був вражений, і Гершель взяв за звичку вимагати відбитки долоні, а пізніше просто вказівного та середнього пальців правої руки, на кожному контракті, укладеному з місцевими жителями. На думку Гершеля, особистий контакт місцевих жителів з документом робив контракт більш обов'язковим, ніж якби вони просто підписали його.

Таким чином, перше широкомасштабне сучасне використання відбитків пальців не ґрунтувалося на наукових доказах, а мало психологічний ефект. Проте, у міру того як його колекція відбитків пальців зростала, Гершель почав помічати, що нанесені чорнилом відбитки можуть довести або спростувати особу. Наукове підґрунтя ідентифікації відбитків пальців заклали два інші британці. Британський хірург-керівник лікарні Цукідзі в Токіо, Японія, у 1870-х роках доктор Генрі Фолдс (Henry Faulds) зайнявся вивченням «шкірних борозен» після того, як помітив сліди пальців на зразках «доісторичної» кераміки. Доктор Фолдс не тільки визнав важливість відбитків пальців як засобу ідентифікації, але й розробив метод їх

класифікації. У 1880 році Фолдс надіслав серу Чарльзу Дарвіну пояснення своєї системи класифікації та зразок розроблених ним бланків для запису відбитків. Дарвін, який був у похилому віці та хворий, повідомив доктора Фолдса, що він нічим йому не допоможе, але пообіцяв передати матеріали своєму двоюрідному братові Френсісу Галтону (Francis Galton). У 1892 році останній опублікував книгу про розроблену ним систему класифікації відбитків пальців на основі трьох основних типів візерунків: петель, завитків та дуг. Хоча його початковою метою було виявити відмінності у відбитках пальців між різними расами (міркування, які не витримали експериментальної перевірки), його система показала, що немає двох однакових відбитків пальців і що ці відбитки залишаються незмінними протягом усього життя людини. Для вивчення відбитків Галтон використав численну колекцію відбитків пальців, яку зберігав вищезгаданий суддя Вільям Гершель.

У 1894 році британський Скотленд-Ярд, штаб-квартира міської поліції Лондона, прийняв систему відбитків пальців Галтона як допоміжну до системи Бертильона.

У 1896 році генеральний інспектор бенгальської поліції Едвард Генрі (Edward Henry) запровадив систему зняття відбитків пальців. Система класифікації відбитків пальців Генрі (Henry Classification System) виявилася настільки успішною в Індії, що 1901 року сам Едвард Генрі був переведений до Англії, де він почав створювати Центральне бюро відбитків пальців Скотленд-Ярду та навчати обраних офіцерів мистецтву класифікації і остаточно замінив систему Бертильона.

У 1903 році перевірку відбитків пальців запровадили в тюрмах штату Нью-Йорк, а система Генрі протягом багатьох років використовувалася Федеральним бюро розслідувань (ФБР) та іншими правоохоронними органами по всьому світі. Наразі поліція та правоохоронні органи широко застосовують ідентифікацію людини за відбитками пальців.

Розпізнавання райдужної оболонки ока (Iris Recognition)

Розпізнавання райдужної оболонки ока — це процес ідентифікації людини шляхом аналізу візерунка райдужної оболонки ока. Ця технологія має чітке наукове підґрунтя.

У 1936 році офтальмолог Френк Берч (Frank Burch) запропонував концепцію використання візерунка райдужної оболонки ока, але на той час технології не дозволяли її перевірити та підтвердити. Лише у 1985 році лікарі-офтальмологи Леонард Флам (Leonard Flam) і Аран Сафір (Aran Safir) встановили, а у 1987 році отримали патент на концепцію, що немає двох однакових райдужних оболонок, навіть якщо люди близнюки.

Доктор Флам звернувся до професора Кембриджського університету Джона Даугмана (John Daugman) з проханням розробити алгоритм для автоматизованої ідентифікації райдужної оболонки ока людини. У 1994 році доктор

Даугман досяг мети та отримав патент, який охоплював алгоритм IrisCode, що перетворював візерунки райдужки в унікальне математичне представлення для біометричної ідентифікації.

Точність розпізнавання райдужної оболонки ока стала широко відомою через десять років, коли в червні 2005 року комп'ютерна лабораторія Кембриджського університету оприлюднила результати 200 мільярдів перехресних порівнянь оболонок.

В 2005 році завершився термін дії широкого патенту, який охоплював базову концепцію розпізнавання райдужної оболонки ока, що надало маркетингові можливості для інших компаній, які розробили власні алгоритми розпізнавання. Термін дії патенту Даугмана закінчився в 2011 році, що дозволило різним компаніям розробляти та впроваджувати власні технології.

Розпізнавання райдужної оболонки ока не використовують у криміналістиці чи у системах відеоспостереження, але активно застосовують як засіб надійної ідентифікації людини у платіжних системах та національних системах ідентифікації. Адже рівень помилкових спрацювань дуже низький: райдужні оболонки ока майже не змінюються протягом життя людини, на них не впливають зміни погоди чи фізичного стану організму людини, а також їх можна визначити, навіть якщо людина носить окуляри або контактні лінзи.

Розпізнавання обличчя (Face Recognition)

Між 1964 і 1966 роками дослідницька група під керівництвом Вудро В. Бледсо (Woodrow W. Bledsoe) проводила експерименти, щоб побачити, чи можуть «програмні комп'ютери» розпізнавати людські обличчя. Команда використовувала сканер, щоб відображати лінію росту волосся, очей і носа людини. Завданням комп'ютера було знайти збіги. Через те, що проект фінансувало розвідувальне агентство, більшість їхніх робіт так і не було опубліковано. Однак пізніше виявилось, що їхня початкова робота включала ручне позначення різних «орієнтирів» на обличчі, таких як центри очей, рот тощо. Відстані між орієнтирами автоматично обчислювалися та порівнювалися між зображеннями для визначення ідентичності. Досліди були цікавими, але їх навряд чи можна назвати вдалими через те, що проблема розпізнавання обличчя була ускладнена змінами даних при повороті чи нахилі голови, зміною інтенсивності та кута освітлення, змінами виразу обличчя, старінням тощо. Проте ці перші експерименти залишаються важливим першим кроком у доведенні того, що розпізнавання облич є можливим.

У 1970-х роках Голдштейн (Goldstein), Гармон (Harmon) і Леск (Lesk) вдосконалили роботу Бледсо, додавши 21 маркер на кшталт кольору волосся та товщини губ. Хоча точність підвищилася, вимірювання відстаней та позначення деталей все ще потрібно було робити вручну, що виявилось надзвичайно трудомістким.

Наприкінці 1980-х Сирович (Sirovich) і Кірбі (Kirby) застосували лінійну алгебру до розпізнавання облич. Система, яка стала відома як Eigenface, показала, що аналіз функцій на серії зображень обличчя може сформувати набір основних ознак. Вони також змогли показати, що для точного кодування нормалізованого зображення обличчя потрібно менше ста значень. У 1991 році Турк (Turk) і Пентланд (Pentland) удосконалили цей метод, навчивши систему автоматично виявляти обличчя на зображеннях, що стало проривом у розвитку технології розпізнавання.

На початку 1990-х років Агентство передових оборонних дослідницьких проєктів (The Defence Advanced Research Projects Agency, DARPA) і Національний інститут стандартів і технологій (The National Institute of Standards and Technology, NIST) США запровадили програму створення технології розпізнавання облич (Face Recognition Technology, FERET), щоб заохотити комерційний ринок. Проєкт передбачав створення бази даних зображень облич. До тестового набору було включено 2413 нерухомих зображень, які представляли 856 людей. Сподівалися, що велика база даних тестових зображень надихне на інновації та зможе призвести до появи більш потужної технології розпізнавання облич.

На початку 2000-х років NIST розпочав тестування постачальників технологій розпізнавання облич (Face Recognition Vendor Test, FRVT). FERET та FRVT фактично забезпечили незалежне державне тестування комерційних систем розпізнавання облич та їх прототипів. Результати тестів були дуже корисними для правоохоронних органів і уряду США допомігши визначити найкращі технології та способи їх використання. Розробники алгоритмів розпізнавання облич з усього світу і по сьогодні намагаються потрапити до переліку FRVT від NIST, щоб довести свою якість та конкурентоспроможність.

У 2006 році за підтримки уряду США був започаткований конкурс Face Recognition Grand Challenge (FRGC) задля оцінки професійних технологій та алгоритмів розпізнавання облич. У тестах використовувалися зображення облич високої роздільної здатності, 3D-сканування облич та зображення райдужної оболонки ока. Результати показали, що нові алгоритми вдсятеро точніші, ніж алгоритми розпізнавання облич 2002 року, і в 100 разів точніші за алгоритми 1995-го, що свідчило про потужний прогрес технологій.

Фактично технології розпізнавання облич були готові для державного та комерційного використання. Відповідні рішення були впроваджені на кордонах та в аеропортах багатьох країн як засіб ідентифікації людей, що відвідують ці країни.

Біометричні характеристики та технології

Для збирання доказової наукової бази про біометричні характеристики людству знадобилося близько 2300 років. Для створення автоматизованих біометричних

технологій — близько 60 років. Модернізація біометричних технологій за рахунок впровадження штучного інтелекту (AI) відбувається зараз майже кожного дня, а кількість реалізованих проєктів експоненційно зростає з кожним роком.

Біометричні технології базуються на біометричних характеристиках, які поділяються на два основних типи: фізіологічні та поведінкові (рис. 1).



Рис. 1. Класифікація біометричних характеристик

Біометричні фізіологічні характеристики (Physiological Biometrics) пов'язані з будовою тіла людини, це: відбитки пальців, риси обличчя, райдужна оболонка ока, сітківка ока, геометрія кисті руки, венозна сітка пальців або руки, форма вушної раковини, ДНК, кров, інше. В свою чергу, фізіологічні характеристики поділяються на морфологічні (видимі та вимірювані фізичні риси, унікальні для кожної людини) та біологічні (ДНК, кров, слина та інші). З біологічними характеристиками переважно працюють медичні служби, також їх використовують судово-медичні експерти для ідентифікації особи.

Біометричні поведінкові характеристики (Behavioral Biometrics) базуються на унікальних діях або навичках людини: манера ходи, голос, підпис, рукописний текст тощо.

Біометричні технології вперше були розроблені у другій половині 20 століття окремими вченими та науковими групами в різних країнах (переважно США, Велика Британія і Франція) на замовлення державних структур, правоохоронних агенцій та відповідних державних спеціальних служб з метою забезпечити можливість пошуку особи та її надійну ідентифікацію.

Більшість технологій були запатентованими і потребували значних обчислювальних потужностей і тому не могли бути використані на широкий загал. У 2010-х роках ці технології в різних країнах (США, Велика Британія, ЄС та інші) отримали нормативну базу, державне законодавче регулювання, а завдяки новому поколінню обчислювальних засобів стали комерційно життєздатними і почали активно використовуватися.

Біометричними технологіями, які впроваджуються на державній та комерційній основі у різних країнах світу, є:

- розпізнавання відбитків пальців (Fingerprint Recognition);
- розпізнавання обличчя (Face Recognition);
- розпізнавання райдужної оболонки ока (Iris Recognition);
- розпізнавання сітківки ока (Retina Recognition);
- розпізнавання відбитків долоні (Palm Print Recognition);
- розпізнавання судинних малюнків пальців або руки (Finger/Palm Vein Recognition);
- розпізнавання форми вуха (Ear Shape Recognition);
- розпізнавання голосу/мовлення/мови (Voice/Speech/Language Recognition);
- розпізнавання підпису/динаміки підпису (Digital signature/signature dynamics) та інші.

Біометричні технології використовуються для боротьби зі злочинністю, перевірки людей на кордонах, протидії шахрайству, забезпечення доступу до об'єктів та приміщень, забезпечення доступу до комп'ютерних мереж, у національних системах охорони здоров'я, для ідентифікації військовослужбовців тощо.

Біометрична авторизація та ідентифікація

Біометрична авторизація (Biometric Authentication) та біометрична ідентифікація (Biometric Identification) — це дві різних технології, що використовують біометричні дані для підтвердження особи.

Біометрична авторизація/автентифікація/верифікація відповідає на запитання «Чи точно це ви?» і встановлює особу шляхом порівняння її біометричних даних з раніше збереженими еталонними даними у форматі «один до одного» (1:1). Наприклад, сучасні смартфони проводять вашу авторизацію за допомогою відбитку пальця чи розпізнавання обличчя. Біометрична авторизація активно використовуються банківськими та фінансовими установами (доступ до банківських застосунків тощо). Задля підвищення безпеки авторизація може бути багатфакторною: сканування обличчя на вашому телефоні + одноразовий код від банку. Біометричні технології можуть доповнювати автентифікацію працівників, що дозволяє створити політики ідентифікації та керування доступом для організації.

Біометрична ідентифікація відповідає на запитання «Хто ви?» і встановлює особу шляхом порівняння її біометричних даних із великою базою даних у форматі «один до багатьох» (1:N). Можливість ідентифікації особи у більшості країн регулюється відповідним законодавством, тому такими технологіями переважно користуються державні структури та служби. Біометричну ідентифікацію активно використовують:

- правоохоронні органи та державні служби безпеки (ідентифікація злочинців/підозрюваних);
- військові (ідентифікація противника/союзника);
- прикордонний, патрульний та міграційний контроль (ідентифікація мандрівника/мігранта/пасажира);
- державні сервіси (ідентифікація громадянина/резидента/виборця);

- заклади охорони здоров'я (ідентифікація пацієнта/медичного працівника/пільговика);
- фізичний і логічний доступ (ідентифікація власника/користувача/працівника/підрядника/партнера);
- комерційні організації (ідентифікація споживача/клієнта).

Також технології біометричної ідентифікації активно впроваджують безпечні міста.

Біометричні технології, якими ми всі користуємося

Всі власники сучасних смартфонів є користувачами біометричних технологій.

Першою біометричною технологією, впровадженою у смартфонах, було розпізнавання голосу. Першим виробником, який це впровадив, стала Motorola. У 2003 році компанія випустила смартфони V-серії, які мали функцію розпізнавання голосових команд без необхідності попереднього навчання. Першим інтелектуальним голосовим асистентом став Siri в iPhone 4S (2011 рік).

Другою біометричною технологією стало розпізнавання відбитків пальців. Першим у світі мобільним телефоном, який містив зчитувач відбитків пальців, був південнокорейський Pantech Gi100, випущений у 2004 році. Наступними сканери відбитків пальців додали японська компанія Toshiba та американська HTC, пізніше Motorola. Першим масовим телефоном, у якому для авторизації використовувалась технологія розпізнавання відбитків пальців під назвою Touch ID, у 2013 році став iPhone 5s. Компанія Samsung у 2014 році представила смартфон Galaxy S5, який дозволяв розблокувати телефон за допомогою Swipe Fingerprint Scanner (проведення пальцем по екрану). Компанії Samsung вдалося значно покращити авторизацію користувачів після початку співпраці з південнокорейською компанією Suprema Inc., яка з 2019 року стала постачальником алгоритму розпізнавання відбитків пальців для Samsung Galaxy S-серії.

У 2011 році з'явився Samsung Galaxy Nexus — перший смартфон з технологією Face Unlock, заснованій на фронтальній камері, але реальну популярність ця технологія отримала у 2017-му під назвою Face ID з запуском iPhone X.

У 2011 році запустили першу систему мобільних платежів Google Wallet, у 2014-му — Apple Pay з використанням Touch ID, у 2015-му — Samsung Pay, а у 2017-му — Google Pay.

Впровадження біометрії змінило ринок смартфонів та засоби авторизації/верифікації користувачів. Розпізнавання відбитків пальців, облич та голосу використовують розробники операційних систем (Windows Hello), виробники ноутбуків (MacBook Touch ID тощо) та різноманітних пристроїв (підтримка голосових помічників Siri, Google Assistant, Alexa).

Біометричні технології в FinTech

Біометрія у фінансових технологіях (FinTech) стає все більш важливою складовою частиною сучасних платіжних систем завдяки здатності покращувати безпеку транзакцій і спрощувати процеси авторизації для користувачів.

Apple Pay, Google Pay та Samsung Pay дозволяють користувачам здійснювати швидкі оплати за допомогою розпізнавання облич або відбитків пальців на смартфонах. Розпізнавання обличчя активно використовується у складі MFA (мультифакторна авторизація) користувачів мобільних застосунків різних банків для доступу до фінансових рахунків та здійснення фінансових транзакцій.

Новим трендом FinTech є впровадження банківських карток з біометричними сенсорами (сканування відбитків пальців), які дозволяють здійснювати безпечні платежі за допомогою сканування пальця замість введення коду (**рис. 2**).



Рис. 2. Банківські картки з біометричними сенсорами (джерело: Mastercard)

Розпізнавання голосу активно використовується банками для ідентифікації клієнтів, підвищення безпеки транзакцій та спрощення обслуговування в контакт-центрах. Серед реалізованих проєктів — HSBC, Barclays (Велика Британія), CitiBank (США) та інші банки. В Україні голосову ідентифікацію клієнтів впровадив ПриватБанк.



Рис. 3. Біометричний термінал з розпізнаванням облич та зчитуванням RFID-карток

У банківській сфері біометричні технології в системах контролю доступу стають дедалі більш популярними. Вони дозволяють одночасно керувати доступом співробітників та відвідувачів у різні зони банку за різними принципами. Для входу/виходу в банки використовують безконтактний прохід співробітників як складову системи контролю доступу за допомогою біометричних терміналів, встановлених на турнікетах (рис. 3).

Другою за популярністю в сучасних банках є технологія мобільного доступу співробітників за допомогою смартфонів та згенерованої адміністратором банку віртуальної карти доступу. Це дозволяє замінити традиційні RFID-картки доступу чи RFID-брелоки, які співробітники часто гублять чи забувають. Для особливо важливих зон використовують мультифакторну автентифікацію з біометрією, а для відвідувачів використовують тимчасові RFID-картки чи QR-коди (рис. 4).

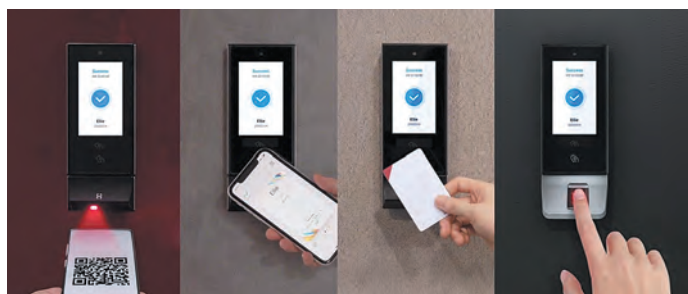


Рис. 4. Різні типи ідентифікації: QR-коди, мобільний доступ, RFID-картки, розпізнавання відбитків пальців

Новим трендом у FinTech є впровадження оплати за допомогою розпізнавання обличчя (Face Payment). У США це PopID, у Китаї — Smile-to-Pay та WeChatFacePay, у Польщі — PayEye та інші. Amazon One в США використовує оплату за допомогою зчитування відбитків долонь користувачів.

Біометрична ідентифікація для прикордонного та міграційного контролю

Біометрична ідентифікація відіграє ключову роль у прикордонному та міграційному контролі, забезпечуючи швидко, точно та надійно перевірку особи.

США були першою країною, яка впровадила біометричний контроль на кордонах. У 2004 році Міністерство внутрішньої безпеки США запустило програму US-VISIT, яка забезпечила пункти видачі віз біометричною технологією (сканування відбитків пальців і фотографування), що давало змогу встановити та підтвердити особу кожного іноземного громадянина, який в'їжджав або виїжджав зі США. На програму US-VISIT у 2003 році було виділено \$380 млн, а загальна вартість проекту склала декілька мільярдів доларів і включала вартість інфраструктури, впровадження біометричних технологій (сканери відбитків пальців, системи розпізнавання обличчя), а також підтримку баз даних для обробки інформації про мільйони подорожуючих. У 2013 році US-VISIT стала частиною державної структури «Офіс управління біометричною ідентифікацією» (Office of Biometric Identity Management, OBIM) Міністерства внутрішньої безпеки США та продовжує працювати.

Впровадження біометричного контролю на кордонах дозволило створити єдину базу ідентифікації осіб, які в'їжджають та виїжджають зі США, виявити тисячі візових шахраїв та заблокувати в'їзд особам, пов'язаним з кримінальною діяльністю, тероризмом або імміграційними порушеннями. Біометрична система скоротила час на перевірку особи до кількох секунд, що значно прискорило роботу прикордонних служб, а для відвідувачів США з'явилася можливість онлайн побачити свою історію в'їздів/виїздів (Form I-94).

Згодом відповідну законодавчу базу та біометричний контроль на своїх кордонах впровадили Велика Британія, країни ЄС, ОАЕ, Китай, Індія та інші держави.

Наразі в США, Великій Британії, Сінгапурі та деяких інших країнах працюють автоматичні пункти контролю eGates. Наприклад, у Великій Британії встановлено понад 270 eGates у 15 повітряних і залізничних портах (рис. 5).



Рис. 5. eGates, аеропорт Лондон Хітроу (джерело: The Telegraph)

Це дозволяє громадянам країн ЄС, Австралії, Канади, Ісландії, Японії, Ліхтенштейну, Нової Зеландії, Норвегії, Сінгапуру, Південної Кореї, Швейцарії та США, також громадянам Великої Британії швидко проходити прикордонний контроль шляхом сканування паспорта й автоматичного розпізнавання обличчя. Для всіх інших резидентів Великої Британії чи відвідувачів передбачено проходження паспортного та міграційного контролю з особистим спілкуванням із офіцерами UK BorderForce, скануванням паспорта й відбитків пальців (рис. 6).



Рис. 6. Паспортний та міграційний контроль на кордонах Великої Британії (джерело: Thales)

Як відомо, Європейський Союз вже впроваджує на своїх кордонах нову біометричну систему в'їзду/виїзду EES (Entry/Exit System). Ця система замінить традиційне

проставлення штампів у паспортах на цифрову реєстрацію, що включатиме збір та зберігання біометричних даних, таких як відбитки пальців та фотографії обличчя, а також інформацію про час та місце перетину кордону. EES має запрацювати у жовтні 2025 року.

Об'єднані Арабські Емірати активно впроваджують біометричні технології для підвищення ефективності та безпеки прикордонного контролю. В міжнародному аеропорту Дубая та інших великих аеропортах ОАЕ встановлені SmartGates, які дозволяють пасажиром самостійно проходити паспортний контроль. Для ідентифікації мандрівників використовується розпізнавання обличчя та відбитків пальців. Використання біометричних технологій допомагає виявляти осіб з підробленими документами, розшукуваних злочинців та інших небажаних осіб, підвищуючи загальну безпеку країни. Авіакомпанія Emirates впровадила інтегрований біометричний маршрут в міжнародному аеропорту Дубая, а саме розпізнавання обличчя та райдужної оболонки ока. Пасажири можуть пройти реєстрацію на рейс, митний контроль, вхід до лаунжу Emirates та посадку на борт, просто пересуваючись через аеропорт без необхідності пред'являти документи на кожному етапі. ОАЕ планує розширити використання біометричних технологій.

У реалізації цих амбітних проєктів біометричного контролю кордонів вищезгаданих країн з метою безпеки не було використано жодного китайського вендора. В цих проєктах брали участь лише авторитетні та професійні компанії, такі як Thales та IDEMIA/Safran (France), NEC Corporation (Японія) та інші.

Біометрична ідентифікація у системах контролю доступу

У більшості замовників в Україні системи контролю доступу працюють переважно з використанням карт захищеного формату EM Marlin, які дуже легко можна скопіювати та отримати доступ до об'єкта (докладно про це у статті «СКД на шляху до IoT», МтБ №4—5/2023).

На відміну від кодів, паролів або карток доступу, які можна забути або втратити, біометрична ідентифікація базується на тому, ким є люди, а не на тому, що вони мають із собою.

Це робить біометричні технології дуже привабливими для впровадження як складову систем контролю доступу для об'єктів критичної інфраструктури (електростанції, енергетична інфраструктура, водопостачання), промислових об'єктів (нафтопереробні заводи, металургійні підприємства), військових об'єктів, банків, аеропортів, логістичних комплексів тощо.

Біометричні технології допомагають автоматизувати доступ до серверних приміщень та ЦОДів, забезпечують авторизований прохід людей в банки та бізнес-центри, дозволяють покращити процеси в логістичних компаніях, забезпечують керування відвідувачами, автоматизують прохід людей в метро та багато іншого.

Біометрична ідентифікація використовується для забезпечення контрольованого входу/виходу людей на територію, доступу до певних зон та обмеження доступу до зон підвищеної важливості.

Це завдання вирішують мультимедійні біометричні термінали або біометричні зчитувачі, які забезпечують надійну ідентифікацію особи за однією чи декількома біометричними характеристиками, а також є відносно доступними по ціні. Основними біометричними технологіями, які використовують для доступу, є ідентифікація за відбитками пальців та розпізнавання обличчя в комбінації з використанням RFID-карт та сценаріями доступу для кожної зони. Біометрична ідентифікація забезпечує зручність, швидкість та автоматизацію процесів, але для забезпечення високого рівня безпеки об'єктів біометричні термінали/зчитувачі мають бути складовою системи контролю доступу, а не окремо встановленим рішенням (рис. 7).



Рис. 7. Біометрія на промислових підприємствах: ліворуч — розпізнавання облич/карта доступу; праворуч — розпізнавання облич/карта доступу та алкотестери

Розпізнавання райдужної оболонки ока, розпізнавання венозного малюнка та голосова ідентифікація є більш дорогими та складними технологіями, тому їх використовують в поєднанні з RFID-картами чи з набором коду для забезпечення багаторівневої безпеки на військових об'єктах, де кожен елемент безпеки має критичне значення для запобігання несанкціонованого доступу.

Біометричні технології змінили навіть організацію доступу на будівельний майданчик (рис. 8). У Великій Британії вже використовують біометричні термінали з розпізнаванням обличчя, які встановлені на турнікетах та дозволяють уповноваженому персоналу проходити на місце проведення робіт у засобах індивідуального захисту.



Рис. 8. Біометрія для доступу на будівельний майданчик

Біометрична ідентифікація у державних сервісах та послугах

Технології біометричної ідентифікації стають дедалі більш популярними у державних сервісах та послугах різних країн.

До прикладу, ОАЕ активно впроваджують біометричні технології в державних сервісах через програму «UAE PASS», яка є цифровим аналогом фізичного паспорта та ідентифікаційного документа. В Австралії для надання послуг громадянам використовується система біометричних даних, яка дозволяє здійснювати реєстрацію особи для отримання австралійських паспортів, а також для доступу до соціальних послуг. У Бразилії біометричні технології впроваджені у виборчий процес для підвищення безпеки та достовірності виборів.

Найбільш вражаючим реалізованим проектом у світі є національна **система ідентифікації Aadhaar** в Індії. Вона забезпечує біометричну ідентифікацію понад 1,3 мільярда громадян за допомогою відбитків пальців, райдужної оболонки ока та фотографій обличчя. Aadhaar була створена Unique Identification Authority of India (UIDAI) і запущена у 2009 році. Це найбільша у світі біометрична система ідентифікації, яка побудована на декількох модальностях, адже рівень хибного спрацювання не повинен був перевищувати 1 на 100 мільярдів (тобто 0,000000001%).

З метою створення єдиної достовірної бази даних населення Індії кожному жителю видається 12-значний ідентифікаційний номер. Кожна особа проходить процес реєстрації, під час якого записуються фотографія обличчя, десять відбитків пальців і скани двох райдужних оболонок, а також демографічна інформація про мешканця (ім'я, адреса, стать і дата народження). Після завершення реєстрації та перевірки біометричних даних видається номер Aadhaar. Постачальники послуг можуть підтвердити особу, надавши номер Aadhaar заявника разом з біометричними даними (наприклад, відбитками пальців) до UIDAI, що миттєво підтвердить особу людини — або ні. У 2017 році програма охопила понад 1,1 мільярда номерів Aadhaar.

Унікальні номери Aadhaar використовуються також у індійському секторі мобільних телекомунікацій. Кожного разу, коли абонент отримує нову SIM-карту, його особа перевіряється завдяки поєднанню біометричних даних (сканування райдужної оболонки ока/відбитків пальців) і номера Aadhaar. Біометричні дані користувача, а саме відбиток пальця, порівнюються з базою даних UIDAI, і результат миттєво доставляється оператору та в точку продажу. Завдяки цьому підписка активується відразу. Реєстрація клієнтів з цифровим ідентифікатором Aadhaar надає операторам в Індії ефективний засіб для задоволення вимог уряду щодо автентифікації абонентів. Біометрія дозволяє унікально ідентифікувати кожного жителя країни, що допомагає у боротьбі з шахрайством та для ефективного розподілу соціальної допомоги. Ця система є основою для багатьох державних послуг, таких як отримання соціальних виплат, медичне обслуговування та фінансові послуги.

Гравці ринку біометричних технологій

Відомі ринку виробники рішень з контролю доступу Honeywell (США), JohnsonControls (Ірландія), Nedap (Нідерланди) та Bosch (Німеччина) не мають своєї власної біометрії та використовують термінали інших виробників.

На масовому ринку можна зустріти китайських виробників Hikvision, Dahua, Huawei, ZKTeco, Anviz, але жоден з них не здатен забезпечити дійсне дотримання міжнародних стандартів кібербезпеки та захисту даних. Отже, обираючи, купуючи та впроваджуючи рішення від китайських виробників, замовники «дають свою добровільну згоду» на передачу всіх своїх персональних даних китайському комуністичному уряду.

На ринку серйозних біометричних систем домінують визнані та надійні виробники з великим досвідом роботи в галузі та з підтвердженою здатністю забезпечити належне зберігання персональних даних: Thales (Франція), IDEMIA (Франція), NEC Corporation (Японія), Fujitsu (Японія) та Suprema (Південна Корея). Ці виробники дотримуються етичних принципів, підтримують протоколи HTTPS, AES-256, TLS 1.2 та відповідають світовим стандартам NIS2, GDPR, PSTI, NDAA, а також міжнародно визаним сертифікатам кібербезпеки ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 30107—3 PAD та іншим.

Ризики впровадження біометричних технологій та гравці ринку

Незважаючи на ефективність та зручність, біометричні технології мають певні ризики, тому їх вибором, тестуванням та впровадженням мають займатися ІТ-фахівці та фахівці з інформаційної безпеки, або спеціалісти з ринку систем безпеки, які мають підтверджену компетенцію та сертифікацію з інформаційної безпеки.

Існує ризик помилкової ідентифікації особи. Система може не розпізнати особу або, навпаки, ідентифікувати звичайну людину як порушника. Такі помилки можуть призвести до неправомірних дій та юридичних проблем. Над зменшенням таких ризиків працюють виробники біометричних терміналів, саме тому вони багатофакторні: біометрія + код/картка. Для національних систем з великою базою даних необхідно впроваджувати мультимодальні рішення: біометрія1 + біометрія2 + інші дані, щоб уникнути помилкової ідентифікації особи.

Ключовим є питання конфіденційності та захисту персональних даних, адже біометрична інформація є унікальною для кожної особи, а її компрометація може мати серйозні наслідки. На відміну від паролів, біометричні дані неможливо змінити, якщо вони були вкрадені. Це створює ризик для особистої безпеки та приватності, тому збирання та зберігання біометричної інформації потребує високого рівня безпеки, щоб уникнути несанкціонованого доступу та використання. Саме тому у країнах, які впроваджують біометричні технології на рівні держави, цей процес регулюється міжнародними стандартами та відповідним

національним законодавством. А фахівці з інформаційної безпеки постійно працюють над тестуванням систем на стійкість до зламу та запобіганню витоку даних і в жодному випадку не використовують обладнання та технології китайських виробників.

У демократичних країнах активно обговорюють обмеження використання розпізнавання облич. Наприклад, ЄС розглядає заборону цієї технології в громадських місцях. Водночас авторитарні країни активно впроваджують технології розпізнавання облич та інші біометричні системи для масового стеження, контролю та затримання громадян. У Китаї система розпізнавання облич активно використовувалась для масового спостереження за уйгурами та іншими мусульманськими меншинами. За інформацією Human Rights Watch, з кінця 2016 року китайський уряд піддав 13 мільйонів етнічних уйгурів та інших тюркських мусульман у Сінцзяні масовим довільним затриманням та репресіям, близько мільйона людей утримуються в таборах «політичного виховання». BBC, The Guardian, Reuters та інші джерела детально описували у своїх численних матеріалах, як уряд Китаю активно використовує мережу камер для масового спостереження, а також технології розпізнавання облич на державних заходах і публічних місцях. Через порушення прав людей китайські компанії Hikvision, Dahua, ZTE та інші потрапили під міжнародні санкції: з 2019 року їм заборонено брати участь у державних проєктах багатьох демократичних країн.

Успішний приклад Китаю з біометричного відстеження громадян надихнув дві інші авторитарні країни. У 2018 році в Росії з'явилась «Единая биометрическая система», призначена для збору, зберігання та обробки біометричних даних громадян, таких як зображення облич та голосові дані. Метою системи було нібито покращення процесу ідентифікації осіб в різних сферах, таких як банки та державні послуги, але фактично ця система стала новим ефективним засобом контролю населення через впровадження зручних сервісів на кшталт «оплата улыбкой» в громадському транспорті чи ритейлі.

Технології розпізнавання облич російських розробників NTechLab, VisionLabs активно використовуються для моніторингу громадян на вулицях та в громадських місцях, зокрема в московському метро для моніторингу пасажирів (джерела: BBC, The New York Times, Reuters), а правозахисні організації Human Rights Watch і Freedom House відзначали, що в окупованому Криму камери та технології розпізнавання облич активно використовуються для стеження за місцевим населенням. У 2023 році NTechLab потрапила під санкції Євросоюзу, а у 2024-му і США за порушення прав людей, зокрема арешти та затримання. Технології розпізнавання облич та іншої відеоаналітики також використовувалися в 2020 році в Білорусі для придушення протестів.

Біометрія в Україні

За останні десять років Україна активно впроваджує біометричні технології та має великий потенціал для покращення безпеки, зручності та ефективності в різних сферах життя.

У 2010 році в Україні був прийнятий та постійно доповнюється закон «Про захист персональних даних».

У 2015 році почався процес впровадження біометричних паспортів, які містять електронний чіп з біометричними даними (фото обличчя та відбитки пальців). Цей крок дозволив отримати безвізовий режим з Європейським союзом.

У 2017 році було затверджено «Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства». У 2018-му МВС України ініціювало проєкт створення єдиної біометричної бази даних для використання правоохоронними органами.

Було розпочато розроблення нормативної бази для регулювання використання біометричних технологій і у 2020 році офіційно запущено мобільний застосунок «Дія». Для підтвердження особи користувача в застосунку використовується технологія розпізнавання обличчя. В «Дії» також зберігаються біометричні дані, такі як фотографії обличчя, що дозволяє використовувати цифрові копії паспортів для підтвердження особи в різних ситуаціях, зокрема перевірку в органах влади або при відвідуванні державних установ. Для забезпечення юридичної сили цифрових документів в додатку використовується електронний підпис. «Дія» інтегрується з різними державними реєстрами та системами.

Протягом останніх п'яти років біометричні технології стали активно застосовуватися в українському FinTech. Багато українських банків впровадили технології розпізнавання обличчя чи відбитків пальців для входу в застосунки, але не всі використовують біометрію для підтвердження транзакцій. Monobank заявляє про найкращий рівень захисту своїх клієнтів, відповідність стандарту PCI-DSS та підтримку підтвердження транзакцій за допомогою біометричних даних, що підвищує безпеку операцій.

Зважаючи на глобальні тренди та швидкість технологічного розвитку, можна очікувати, що в найближчі роки біометричні технології в Україні та інших країнах набудуть ще більшого поширення, відкриваючи нові можливості для цифрової трансформації, а також посилюючи заходи безпеки на державному рівні. Водночас важливими залишаються питання всебічного законодавчого врегулювання, захисту персональних даних, кібербезпеки та етичного використання біометрії.

Альона ШВЕЦОВА,
незалежний експерт
з систем безпеки, [cctvmadonna](#)

Джерела: сайти компаній NEC, IDEMIA, Thales, Suprema Inc., ISO Global Standards, The United States Department of Homeland Security, New York State Division of Criminal Justice Services, The National Institute of Standards and Technology, Biometrics Institute, British Standards Institution, The UK's National Cyber Security Centre, GOV.UK, Britannica, EN-CENELEC, Biometrics Research Group та інші.